Distributed Routing Software

System Network Architecture Guide

Part Number: AA–QU5SA–TE

January 1996

This manual provides information about SNA interfaces and protocols for the Distributed Routing Software system.

Revision/Update Information:	This is a new manual.
Software Version:	Distributed Routing Software V1.1

This manual was produced by Shared Engineering Services.

Contents

Preface

1 Using the DLSw Protocol

About DLSw 1–1
How DLSw Works 1–1
Problems Inherent in the Bridging Solution 1–2
Protocol Spoofing 1–3
Benefits of DLSw 1–4
Setting Up DLSw 1–4
Configuration Requirements 1–4
Configuring Adaptive Source Route Bridging for DLSw 1–5
Configuring the Internet Protocol for DLSw 1–6
Configuring SDLC Interfaces 1–7
Configuring DLSw 1–8
Sample DLSw Configuration 1–9
Context Diagram 1–9
Configuring Devices and Datalinks 1–10
Configuring Protocols 1–12
Configure IP 1–12
Configuring OSPF or RIP 1–14
Enable OSPF 1–14
Enable Multicast OSPF as Needed 1–14
Define the Interfaces That Use OSPF 1–15

Check the OSPF Configuration 1–15
Configuring ASRT 1–16
Disable Transparent Bridging 1–16
Enable Source Route Bridging 1–17
Assign a Port Segment Number and Enable DLSw 1–17
Implementing Protocol Filtering 1–18
Configuring DLSw 1–19
Configuring DLSw Groups and Static Sessions 1–20
On Demand and Explicitly Configured TCP Sessions 1–22
Using DLSw Groups 1–23
Setting Up DLSw Groups 1–23
Assign OSPF Addresses to Hardware Interfaces 1–23
Issue the DLSw Join-Group Command 1–23
Enable OSPF and Multicast OSPF 1–24
Mixing T2.0 and T2.1 Remote Link Stations on Multipoint Lines 1–24

2 Configuring the DLSw Protocol

About DLSw Configuration and Monitoring Commands 2–1
Accessing the DLSw Configuration Environment 2–1
DLSw Configuration Commands 2–2

3 Monitoring the DLSw Protocol

About DLSw Monitoring Commands 3–1
Accessing the DLSw Monitoring Environment 3–1
DLSw Commands 3–2

4 Configuring SDLC Interfaces

About SDLC Configuration Commands 4–1
Accessing the SDLC Configuration Environment 4–1
SDLC Commands 4–2

5 Monitoring SDLC Interfaces

About SDLC Monitoring Commands 5–1
Accessing the SDLC Monitoring Environment 5–1
Displaying Statistics on SDLC Interfaces 5–2
SDLC Commands 5–4

6 Using Boundary Access Node

About Boundary Access Node 6–1
How BAN Works 6–2
Bridged and DLSw-terminated BAN 6–3
Which Method Do You Use? 6–5
Using BAN 6–6
Configuring Frame Relay 6–6
Configuring the Router for Adaptive Source Route Bridging 6–7
Configuring the Router for BAN 6–8
Opening Service Access Points (SAPs) 6–9
Using Multiple DLCIs for BAN Traffic 6–10
Benefits of Setting Up a Fault-tolerant BAN Connection 6–10
Setting Up Multiple DLCIs 6–10
Checking the BAN Configuration 6–11
Enabling BAN Event Logging System Messages 6–12

7 Configuring Boundary Access Node

BAN Configuration Commands 7–1
Accessing the BAN Configuration Environment 7–1
BAN Command Summary 7–1

8 Monitoring Boundary Access Node

BAN Monitoring Commands 8–1
Accessing the BAN Monitoring Environment 8–1

BAN Command Summary 8–1

9 Using SDLC Relay

About SDLC Relay 9–1
How SDLC Relay Works 9–1
SDLC Primary and Secondary Stations 9–2
When to Use SDLC Relay 9–3
Setting Up SDLC Relay 9–4
Sample SDLC Relay Configuration 9–4
Context Diagram 9–4
Configuring SDLC Relay 9–5
Set Serial Line Parameters 9–6
Configuring the SDLC Relay Protocol 9–6
Assign a Group Number 9–6
Add a Local Port 9–7
Add a Remote Port 9–8
Configure the Neighbor Router 9–8
Set Data Link, Add Group, and Add Port 9–8
Add a Remote Port 9–9

10 Configuring SDLC Relay

About SDLC Relay Configuration Commands 10–1
Accessing the SDLC Relay Configuration Environment 10–1
SDLC Relay Commands 10–2

11 Monitoring SDLC Relay

About SDLC Relay Monitoring Commands 11–1
Accessing the SDLC Relay Monitoring Environment 11–2
SDLC Relay Commands 11–2

A DLSw MIB Support

B Interoperating with the IBM 6611 Router

Glossary

Index

Figures

1–1 Traditional Approach to Bridging Over the Internet 1–2
1–2 Data Link Switching Over the Wide Area 1–3
1–3 Context Diagram for DLSw Configuration 1–10
6–1 Direct Connection of End Nodes to IBM FEP Using BAN 6–2
6–2 BAN Type 1: The Router as an LLC-2 Bridge 6–4
6–3 BAN Type 2: Local DLSw Conversion 6–5
6–4 BAN Configuration with Multiple DLCIs to Different FEPs . . 6–10
9–1 SDLC Primary/Secondary Stations and Local/Remote Ports . . 9–2
9–2 SDLC Relay Configurations 9–3
9–3 Context Diagram for SRLY Configuration 9–5

Tables

2–1 DLSw Command Summary 2–2
3–1 DLSw Command Summary 3–2
4–1 SDLC Command Summary 4–2
5–1 SDLC Command Summary 5–4
7–1 BAN Command Summary 7–2
8–1 BAN Command Summary 8–2
10–1 SDLC Relay Command Summary 10–2

11–1 SDLC Relay Command Summary 11–2
A–1 DLSw MIB Tables Supported A–1
A–2 DLSw MIB Objects Supported A–2

Preface

Objectives

This *System Network Architecture Guide* contains information for configuring and monitoring SNA interfaces and protocols operating with the Bridge Router Software system software.

Audience

This guide is intended for persons who install and operate computer networks. Although experience with computer networking hardware and software is helpful, you do not need programming experience to use the protocol software.

Organization

This manual is organized as follows:

- Chapter 1 describes how to use the DLSw protocol.
- Chapter 2 explains the DLSw protocol configuration commands.
- Chapter 3 explains the DLSw protocol monitoring commands.
- Chapter 4 describes how to configure SDLC interfaces.
- Chapter 5 describes the SDLC monitoring commands.
- Chapter 6 how to use Boundary Access Node.
- Chapter 7 explains Boundary Access Node configuration commands.
- Chapter 8 describes Boundary Access Node monitoring commands.

- Chapter 9 describes how to use SDLC Relay protocol.
- Chapter 10 explains the SDLC Relay configuration commands.
- Chapter 11 describes the SDLC Relay monitoring commands.
- Appendix A lists the DLSw MIB support.
- Appendix B describes considerations for interoperating with the IBM 6611 router.

Associated Digital Documents

The following documents provide additional information about the router hardware and software:

- *Bridging Configuration Guide,* AA–QL29C–TE
- *Event Logging System Messages Guide*, AA–QL2AC–TE
- *Network Interface Operations Guide,* AA–QL2BC–TE
- *Routing Protocols Reference Guide,* AA–QL2CC–TE
- *Routing Protocols User's Guide*, AA–QL2DC–TE
- *System Software Guide,* AA–QL2EC–TE

Conventions Used in This Guide

`Special type`	This special type in examples indicates system output or user input.
`Boldface`	Boldface type in examples indicates user input.
lowercase-italics	Lowercase italics in command syntax or examples indicate variables for which either the user or the system supplies a value.
[ ]	Brackets enclose operands or symbols that are either optional or conditional. Specify the operand and value if you want the condition to apply. Do not type the brackets in the line of code.
key	Indicates that you press the specified key.
Ctrl/x	Indicates that you should hold the CONTROL key down and press the key specified by the x. The server displays the key combination as ^x.
RET	Indicates that you should press the Return key.
underscore	Characters underscored in a command listing represent the least number of characters you must enter to identify that command to the interpreter.

1

Using the DLSw Protocol

This chapter describes Digital's implementation of the Data Link Switching (DLSw) protocol. Digital's DLSw product offers a wide range of functionality designed to integrate SNA (System Network Architecture) into heterogeneous, multi-protocol networks.

The following sections explain how to configure your router for DLSw.

About DLSw

DLSw is a essentially a forwarding mechanism for IBM's LLC2 and SDLC protocols. It relies on the Switch-to-Switch protocol (SSP) running over TCP/IP to provide a reliable transport of SNA traffic over the internet. DLSw does not provide full routing capabilities. Instead, it works by providing switching at the data link layer. Rather than bridging LLC2 frames, DLSw terminates the LLC2 connection locally and encapsulates only the Information (I) and Unnumbered Information (UI) frames in TCP frames. The router ships the TCP frames over the WAN link to a neighbor DLSw router for delivery to their intended end station addresses.

How DLSw Works

LLC2 and SDLC are connection-oriented protocols, designed to function well on LANs and WANS. DLSw gives these protocols the dynamic characteristics of routable protocols. Equally important, DLSw preserves the end-to-end reliability and control features that make LLC2 and SDLC effective for communication on the LAN.

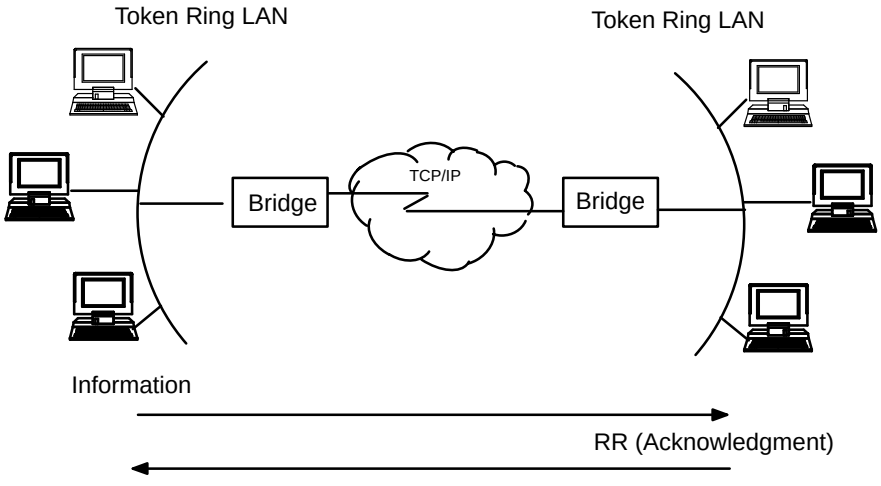
Problems Inherent in the Bridging Solution

Figure 1–1 illustrates the traditional approach to bridging SDLC and LLC2 frames across WAN links. The problem with this approach is that network delays occur much more frequently in the wide area than on a LAN. Such delays can arise from simple network congestion, slower line speeds, or other factors. Each of these factors increases the possibility of a session timing out, and of data failing to arrive at their destination.

In addition, LAN protocols like LLC2 use much shorter retransmit/response times than those designed for use in the wide area. This makes maintaining end-to-end connections across WAN links extremely difficult, causing session timeouts to occur.

The frequency of session timeouts is not the only problem. Another problem arises when data is delayed while crossing the WAN. When a sending station retransmits data that was not lost, but delayed, LLC2 end stations can receive duplicate data. While this seems to safeguard the data, it can lead to confusion of the LLC2 procedures on the receiving side. This may, in turn, lead to inefficient use of the WAN link, as may the added overhead of datalink messages entering the WAN.

Figure 1–1 Traditional Approach to Bridging Over the Internet



Traditional bridging, involving end-to-end data link control.

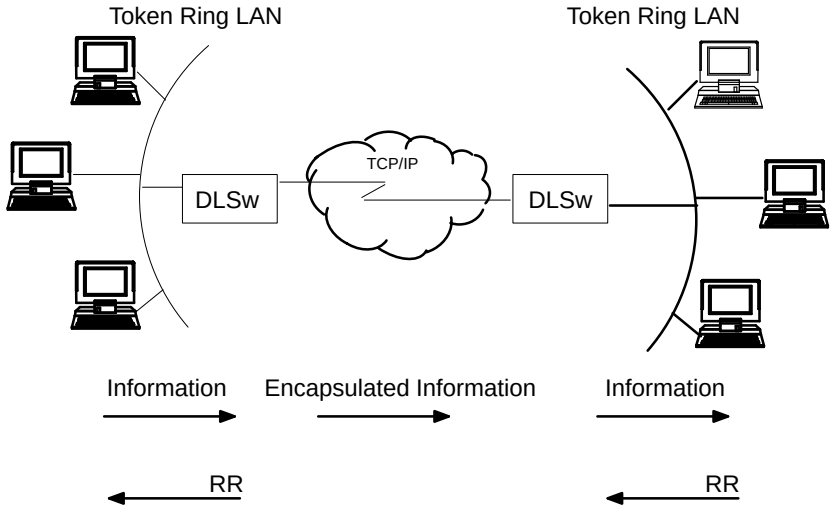
Protocol Spoofing

To reduce the chance of session timeouts, and to maintain the appearance of end-to-end connectivity for sending stations, DLSw works by terminating or spoofing LLC2 connections at the local router. When terminating the connection, the local router sends acknowledgements to the sending station. This acknowledgment tells the sender that data previously transmitted were received.

The acknowledgment prevents the station from retransmitting. From this point forward, assuring that data gets through is the responsibility of the DLSw software. The software accomplishes this by encapsulating the data in routable IP frames, then transporting them (via TCP) to a DLSw peer. The neighbor DLSw router strips away the TCP header, determines the address of data's intended recipient, and establishes a new LLC2 connection with that end station.

Figure 1–2 illustrates this relationship between two DLSw neighbor routers.

Figure 1–2 Data Link Switching Over the Wide Area



DLSw terminates the LLC2 connections at the switch, so that LLC control flows do not cross the wide area network. This reduces the possibility of session timeouts.

Benefits of DLSw

Because DLSw terminates the LLC connection at the local router, it is especially effective at eliminating SNA session timeouts and reducing WAN overhead on shared circuits. The protocol has these main benefits:

- DLSw drastically reduces the possibility of session timeouts by terminating LLC2 and SDLC traffic at the local LAN.
- DLSw reduces WAN network overhead by eliminating the need to transmit acknowledgments (RRs) over the wide area. The RRs are confined to the LANs local to each DLSw router.
- DLSw provides flow and congestion control, and broadcast control of search packets, between DLSw routers and their attached end stations.
- DLSw increases Source Route Bridging (SRB) hop-count limits.
- DLSw allows LLC2 to SDLC protocol conversion.

Setting Up DLSw

The next five sections explain the procedures to follow to set up DLSw. These sections cover the following topics:

- Configuration Requirements
- Configuring ASRT
- Configuring IP
- Configuring SDLC Interfaces
- Configuring DLSw

In addition, a sample DLSw configuration with explanatory notes begins on page 9.

Configuration Requirements

Digital router platforms support DLSw over IEEE 802.5 Token Ring, SDLC, Ethernet, and FDDI . To use DLSw, you must perform the following actions:

- Configure ASRT
- Configure IP
- Configure OSPF and MOSPF, as needed
- Configure SDLC devices, as needed
- Configure DLSw

The sections that follow explain how to complete these actions in a step-by-step fashion. An annotated example of an actual DLSw configuration follows these procedures.

Configuring Adaptive Source Route Bridging for DLSw

Since the DLSw router appears as a bridge to attached end stations, you need to configure source route bridging. Do this by following these steps:

1. Enter the **protocol asrt** command at the `Config>` prompt to enter the ASRT configuration module.
2. Enter the **enable bridge** command to enable bridging on the router. Each bridge must have a unique bridge address.
3. Enter the **add port** command to add a bridge port for each interface used by DLSw. The display prompts you for an interface number and a port number.
4. Configure LAN interfaces.
   - For Token Ring interfaces:

     Enter the **disable transparent** command to disable transparent bridging. Then, enter the **enable source routing** command to turn on source routing for the bridge port. You are prompted for an SRB segment number.
   - For Ethernet or FDDI interfaces:

     Enter the **enable transparent** command to enable transparent bridging on the bridge port.
5. If you are configuring the router for parallel DLSw and bridging paths:
   - Create a protocol filter against the SAPs (Service Access Points) you intend DLSw to use. If the router is performing bridging operations, plus forwarding packets via DLSw, it is essential to do this. If you do not, DLSw both bridges and forwards the packets it receives. See the section “Implementing Protocol Filtering” for further information.

To create a SAP filter, enter this command at the `ASRT config>` prompt:

```
add protocol-filter dsap 4
```

– In addition to this command, you must specify the bridge port to which it applies. The command tells the router to filter all traffic that has a DSAP of 4 on a designated port. (Note that this assumes you have chosen a SAP of 4 for DLSw traffic. Assigning a SAP is something you do during the DLSw configuration.)

6. Next, verify the ASRT configuration. You do not have to do this, but it is a good idea to check the bridge configuration before proceeding. Use the **list bridge** command to verify the configuration of the ASRT protocol.

7. Enable the DLSw protocol using the **enable dls** command.

Configuring the Internet Protocol for DLSw

You need to configure IP so the local DLSw router can form the TCP connection to its DLSw peer. To do this, proceed as follows:

1. Enter the IP configuration process by issuing the **protocol ip** command at the `Config>` prompt.

2. Use the **add address** command to assign the IP address to the hardware interface you are using to connect to the other DLSw peer.

3. Enable dynamic routing:

   If you do not define static routes between DLSw neighbors, you must choose either OSPF or RIP as your routing protocol. Using OSPF is recommended, as it entails less network overhead than RIP.

   – To enable OSPF:

     Enter the **protocol ospf** command from the `Config>` prompt. This brings you to the `OSPF Config>` prompt. To use DLSw group functionality, enable Multicast OSPF.

     For more information on using OSPF, see “The OSPF Routing Protocol” in the *Routing Protocols Reference Guide*.

   – To enable RIP**:**

Enter **enable RIP** at the `Config IP>` prompt.

4. Next, use the **set internal-ip-address** command to set the address that belongs to the router as a whole. The router uses the internal IP address when it connects via TCP with its DLSw peer.

Note: If you are using RIP, the router's Internal IP address must match the physical IP address of the IP port.

Configuring SDLC Interfaces

The SDLC configuration commands allow you to create or modify the SDLC interface configuration as part of the DLSw configuration process.

You must configure SDLC links if you intend to support SDLC over DLSw. This section explains how to access the SDLC configuration process, and describes SDLC-related commands.

1. At the `Config>` prompt, use the **set data-link SDLC** command to configure the data link type for the serial interface. You are prompted for an interface number. Supply the interface number corresponding to the physical synchronous port through which SDLC runs.

2. Use the **`network`** command at the `Config>` prompt to enter the SDLC configuration process. The router prompts you for an interface number. Enter the number you used in Step 1.

3. Set the link clocking source. If your Digital Distributed Router hardware supports internal clocking and you wish to connect directly to an SDLC device without a modem pair or modem eliminator, you can use **set link clocking internal**. If you do use internal clocking, you must supply a synchronous null modem cable interface (not provided by Digital).

4. If you are using internal clocking, use the **set link speed** command to choose the clock speed for this line.

5. Set the line encoding (NRZ/NRZI) to match the attached end station's configuration.

6. Set duplex to full or half to match the attached end station's configuration.

7. When you have finished, use the **list link configuration** command to verify the SDLC interface configuration.

Configuring DLSw

Before you begin configuring DLSw, use the **list device** command at the `Config>` prompt to list the interface numbers of different devices.

To configure the DLSw protocol, follow these steps.

1. At the `Config>` prompt, enter the **protocol dls** command. This brings you to the `DLSw config>` prompt.
2. Use the **enable dls** command to enable DLSw in the router.
3. Use the **set srb** command to designate an SRB (Source Route Bridging) segment number for the DLS router.

   This segment number should be the same for all DLSw routers, and unique in the source route bridge domain. The bridge uses this number in the Routing Information Field (RIF) when the frames are sent on the LAN. The segment number is the key to preventing loops.
4. Enter an **Open SAP** command for each SAP that you wish DLSw to switch. The router prompts for interface numbers.
5. Use the **add tcp** command to add the IP address of each DLSw neighbor. This connection can also be made using multicast OSPF using the **join-group** command.

Note: A router can only participate in a group if its neighbor router is a Digital platform running DLSw. If you configure one DLSw router for a group, you must enable OSPF and MOSPF on all DLSw routers in the group.

6. Set the MAC address used as the default source MAC address when adding SDLC link stations. Do this by issuing the **set mac** command.

   If you configure more than one SDLC link station using this default source MAC address, you must configure each station with different source SAPs to uniquely identify them.

   If no default MAC address is configured, then the first source MAC address configured becomes the default source MAC address used for all subsequently configured SDLC link stations.
7. For your DLSw configuration to support SDLC, you must add an SDLC link station using the **add sdlc** command.

Sample DLSw Configuration

Following is a complete DLSw configuration. The example assumes that the router has not been configured for any other protocols or data links. For this reason, the script begins at the `Config (only)>` prompt, rather than at `Config>`.

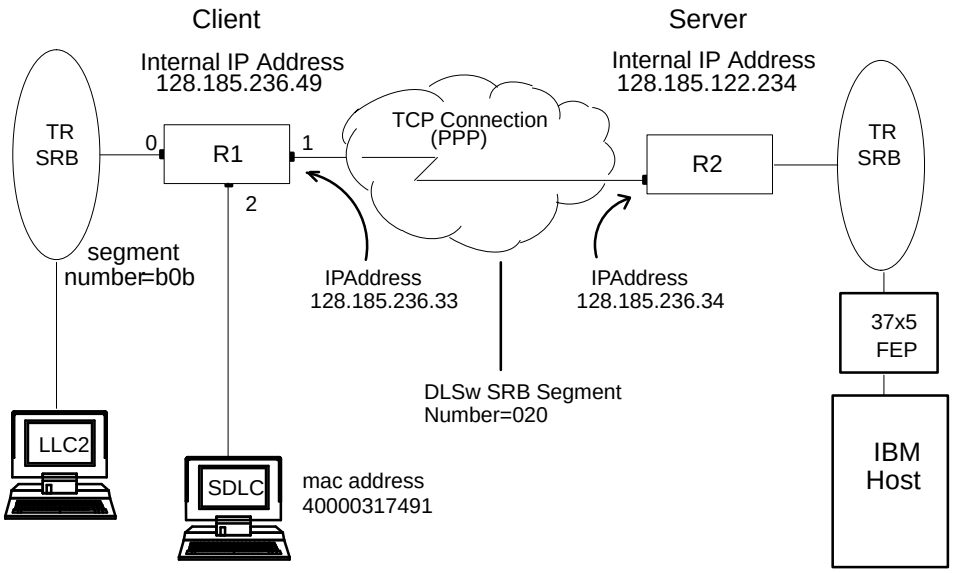
Context Diagram

The example is based on the information shown in Figure 1–3. The DLSw router being configured (R1 in the diagram) supports one LLC and one SDLC connection to its DLSw neighbor (R2). The TCP connection between the two routers is PPP.

Configuring R1 for DLSw requires all of the information shown. This information includes the following:

- The internal IP addresses of R1 and R2.
- The IP address of each port used to maintain the TCP connection between the routers.
- The interface numbers assigned to the Token Ring and SDLC devices, and that used for the TCP connection.
- The source route bridge segment number of the attached Token Ring.

Figure 1–3 Context Diagram for DLSw Configuration



Configuring Devices and Datalinks

Next, configure Token ring. You can use the **list devices** command to determine the interface numbers corresponding to each interface as shown in the following output:

```
Config>list dev
Ifc 0 (Token Ring): CSR D0000000, vector 29
Ifc 1 (WAN PPP): CSR 70001620, CSR2 70000D00, vector 93
Ifc 2 (WAN SDLC): CSR 70001640, CSR2 70000E00, vector 92

TKR config>speed 16

Config (only)>network 0
Token-Ring interface configuration
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    16 Mb/sec
Ring Select:              BackPlane
RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
NetWare IPX encapsulation: TOKEN-RING MSB

TKR config>exit
```

The first port (interface 1) is used for the WAN (TCP/IP) link (See Figure 1–3). The data link selected for the TCP/IP WAN is PPP. An alternative choice is Frame Relay. If the default assignments that are displayed by the **list devices** command are not what you want, change them using the **set data-link** command.

```
Config>network 1
Point-to-Point user configuration
PPP Config>list all

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
--------------
Config Request Tries:               20   Config Nak Tries:             10
Terminate Tries:                    10   Retry Timer:                3000

LCP Options
-----------
Max Receive Unit:                 2048   Magic Number:                 Yes
Password Authentication:            No

PAP Parameters
--------------
Authent Request Tries:              20
Retry Timer:                      3000
Request Timer:                   15000

PAP Ids/Passwords
-----------------
Local ID:                  (None)
Local Password:            (None)

Remote ID:                 (None)
Remote Password:           (None)

NCP Parameters
--------------
Config Request Tries:               20   Config Nak Tries:             10
Terminate Tries:                    10   Retry Timer:                3000

IPCP Options
------------
IPCP Compression:                 None
IP Address:      Don't Send or Request
```

If configuring DLSw to support SDLC, the next step is to configure SDLC devices.

To access the SDLC configuration, use the **network** command and the number of the interface to which an SDLC device is assigned (in this case, 2).

```
Config (only)>network 2
SDLC user configuration
Creating a default configuration for this link
```

This example begins with a **list link** command. The **list** command does not alter the configuration, but shows you the values currently associated with the SDLC link.

```
SDLC 2 Config>list link
Link configuration for: LINK_2   (ENABLED)

Default role: PRIMARY          Type:        POINT-TO-POINT
Duplex:       FULL             Modulo:      8
Idle state:   FLAG             Encoding:    NRZ
Clocking:     EXTERNAL         Frame Size:  2048
Speed:        0

Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
           RTS hold delay:     DISABLED
           Inter-frame delay:  DISABLED

Counters:  XID/TEST retry:  4
           SNRM retry:      6
           Poll retry:      10
```

Configuring Protocols

To run DLSw you must configure IP, OSPF (or RIP), ASRT and the DLSw protocol.

Configure IP

This example begins with the creation of a minimal IP configuration.

To configure IP, begin by entering the **protocol IP** command at the `Config>` prompt:

```
Config (only)>protocol ip
Internet protocol user configuration
```

The **list** command shows the default IP configuration.

```
IP config>list all
Interface addresses
IP addresses for each interface:

Routing
Protocols

BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled
```

Assign an Internet Address to the WAN Link

Add an internet address and assign it to one of the interfaces associated with the WAN link configured earlier:

```
IP config>add address
Which net is this address for [0]? 1
New address [0.0.0.0]? 128.185.236.33
Address mask [255.255.0.0]? 255.255.255.0
```

Set the Internal IP Address

Set the internal IP address. This is the address that remote DLSw routers use to connect to the router you are configuring.

```
IP config>set internal-ip-address 128.185.236.49
```

Enter the **list** command to display the newly added information.

```
IP config>list all
Interface addresses
IP addresses for each interface:
intf 1  128.185.236.33  255.255.255.0 Network broadcast, fill 0
Internal IP address: 128.185.236.49

Routing Protocols

BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: enabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled

IP config>exit
```

Configuring OSPF or RIP

This sample configuration uses OSPF rather than RIP. You can use either of these routing protocols. However, if you choose RIP, you cannot use DLSw group functionality.

The **list** command displays the default OSPF configuration.

```
Config (only)>protocol ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>list all

                --Global configuration--
          OSPF Protocol:          Disabled
          External comparison:    Type 2
          AS boundary capability: Disabled
          Multicast forwarding:   Disabled

               --Area configuration--
Area ID       AuType     Stub?   Default-cost Import-summaries?
0.0.0.0       0=None     No      N/A           N/A
```

Enable OSPF

The first step consists in enabling OSPF, and estimating the number of external routes and OSPF routers.

```
OSPF Config>enable ospf
Estimated # external routes [0]? 100
Estimated # OSPF routers [0]? 25
```

Enable Multicast OSPF as Needed

Since this example implements DLSw Group Functionality, we must enable multicast OSPF, as shown:

```
OSPF Config>enable multicast
Inter-area multicasting enabled? [No]: N
```

Define the Interfaces That Use OSPF

You must issue the **set interface** command for every physical IP interface that uses OSPF. This example assumes that the backbone is the OSPF area (0.0.0.0). At this point, only one IP interface is defined.

```
OSPF Config>set interface 128.185.236.33
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?


Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
Forward multicast datagrams? [Yes]:
Forward as data-link unicasts? [No]:
IGMP polling interval (in seconds) [60]?
IGMP timeout (in seconds) [180]?
OSPF Config>
```

Check the OSPF Configuration

Following is the OSPF display after it is configured. To see what has changed in the configuration, compare this display with the display of the default OSPF configuration shown on page 16.

```
OSPF Config>list all

            --Global configuration--
     OSPF Protocol:          Enabled
     # AS ext. routes:       100
     Estimated # routers:    25
     External comparison:    Type 2
     AS boundary capability: Disabled
     Multicast forwarding:   Enabled
     Inter-area multicast:   Disabled


                          --Area configuration--
Area ID      AuType       Stub? Default-cost Import-summaries?
0.0.0.0      0=None       No         N/A           N/A

                          --Interface configuration--
IP address      Area     Cost  Rtrns  TrnsDly  Pri  Hello  Dead
128.185.236.33   0.0.0.0   1      5       1      1     10    40

                             Multicast parameters
IP address    MCForward    DLUnicast    IGMPPoll    IGMPtimeout
128.185.236.33    On           Off          60           180

OSPF Config>exit
```

Configuring ASRT

DLSw requires SRB (Source Route Bridging) to run over a Token Ring interface. Conversely, transparent bridging is required for Ethernet or FDDI devices, but does not work if the attached device is Token Ring.

This example is based upon a Token Ring connection to the DLSw router. Begin by enabling the bridge as shown:

```
Config (only)>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
```

Disable Transparent Bridging

The **list port** command shows that the port defaults to transparent bridging.

```
ASRT config>list port
Port Id (dec)    : 128: 1, (hex): 80-01
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 0
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++
```

Begin by disabling transparent bridging on the Token Ring port. Port number one is *port 1 on interface 0.* In other words, port 1 is the logical bridge port for the physical interface set up for the Token Ring (see Figure 1–3).

```
ASRT config>dis transparent
Port Number [1]?
ASRT config>
```

Enable Source Route Bridging

Next, enable source route bridging for the Token Ring port as shown:

```
ASRT config>enable source
Port Number [1]?
```

Assign a Port Segment Number and Enable DLSw

Now, assign a segment number for the port. You only have to assign segment numbers when configuring a source route bridge device, such as Token Ring. In this example (see Figure 1–3) **b0b** is the hexadecimal number assigned to the Token Ring device.

```
Segment Number for the port in hex(1 - FFF) [1]? b0b
Bridge number in hex (1 - 9, A - F) [1]?
```

After assigning a segment number, enable DLSw for the bridge.

```
ASRT config>enable dls
```

Listing the bridge configuration confirms that you have configured ASRT correctly.

```
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                ===============================================

   Bridge:                Enabled                Bridge Behaviour: Unknown
                        +---------------------------+
   -------------------- | SOURCE ROUTING INFORMATION |------------------------------
                        +---------------------------+
   Bridge Number:           01                     Segments:           1
   Max ARE Hop Cnt:         14                     Max STE Hop cnt:   14
   1:N SRB:                 Not Active             Internal Segment:  0x000
   LF-bit interpret:        Extended
```

```
                    +-------------------+
-------------------| SR-TB INFORMATION |---------------------------------------
                    +-------------------+
SR-TB Conversion:         Disabled TB-Virtual Segment:  0x000    MTU of TB-Domain:  0


                    +-----------------------------------+
-------------------| SPANNING TREE PROTOCOL INFORMATION |----------------------
                    +-----------------------------------+
Bridge Address:           Default                 Bridge Priority:   32768/0x8000
STP Participation:        IEEE802.1d

                    +-------------------------+
-------------------| TRANSLATION INFORMATION |---------------------------------
                    +-------------------------+
FA<=>GA Conversion:       Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:       Enabled


                    +------------------+
-------------------| PORT INFORMATION |----------------------------------------
                    +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behaviour:    SRB Only   STP:  Enabled
```

Implementing Protocol Filtering

This is an important step when configuring DLSw (see the section “Configuring the Internet Protocol for DLSw” in this chapter).

You only need to implement the filter described here if you configure parallel bridging and DLSw. Such is not the case in the example at the end of this section. The procedure for creating a SAP filter is provided for reference purposes only.

Since DLSw, rather than bridging, is used to forward traffic on SAPs (Service Access Points) 04, 08, 0C, we are adding a special protocol filter to the bridging set up.

The filter’s purpose is to prevent the bridge from forwarding, on other ports, packets that should only be handled by DLSw.

This command shown below creates a filter that works on all packets with a destination SAP of 4. The **list** command issued subsequently displays the filter characteristics.

```
ASRT config>add prot-filter dsap 4
Filter packets arriving on all ports?(Yes or [No]): yes

ASRT config>list prot-f dsap
Protocol Class: DSAP
Protocol Type : 04
Protocol State: FILTERED
Port Map      : 1
=========================
No ETHER type Filter Records Associated
No SNAP Filter Records Associated
```

Once the filtering you need is in place, exit the ASRT configuration module.

```
ASRT config>exit
```

Configuring DLSw

The final step involves configuring the DLSw protocol itself. The **list** command below shows the defaults.

```
Config (only)>protocol dls
DLSw protocol user configuration
DLSw config>list dls
DLSw is                             DISABLED
LLC2 send Disconnect is             ENABLED

TCP Receive Buffer Size             5120
Automatic TCP connection            ALWAYS CONNECT

SRB Segment number                  000
MAC <-> IP mapping cache size       128
Max DLSw sessions                   1000
DLSw global memory allotment        153600
LLC per-session memory allotment    8192
SDLC per-session memory allotment   4096
                                  No MAC Address set

Database age timer                  1200 seconds
Age timer resolution                300  seconds
Max wait timer for ICANREACH        20   seconds
Wait timer for LLC test response    15   seconds
Wait timer for SDLC test response   15   seconds
Join Group Interval                 900  seconds
```

Enable DLSw and set the SRB segment number. The segment number is the virtual segment number that identifies DLSw in the RIF of all LLC frames.

```
DLSw config>enable dls
DLSw config>set srb 020
```

Configuring DLSw Groups and Static Sessions

You must define either a DLSw group or a static TCP session to connect to one or more neighbor DLSw routers. This example defines both a group and a static (explicitly configured) TCP session.

The **join** command is used to join a DLSw group. You designate each group member as Client, Server or Peer. Client is the default.

Using the Join-Group Command

The **join-group** command executed for R1 (see Figure 1–3), designates this DLSw router as a Client in group 1. To join this group, R2 is added as a Server in group 1.

```
DLSw config>join
Group ID (1-64 Decimal) [1]?
Client/Server or Peer Group Member(C/S/P)- [C]?
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive?(E/D)- [D]?

DLSw config>list group
Group  Role       Xmit Bufsize   Max Segsize  Keepalive
 1    CLIENT          5120         1024       DISABLED
```

Using the Add TCP Command

The **add tcp** command is used to create explicitly configured DLSw routes. The neighbor DLSw IP Address added here is the internal IP Address of the neighbor DLSw router (called R2 in Figure 1–3). Note that you must also configure R2 with the neighbor IP Address of R1.

```
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.122.234
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive?(E/D)- [D]?

DLSw config>list tcp
Neighbor      Xmit Bufsize   Max Segsize  Keepalive
128.185.234.98    5120          1024      DISABLED
```

Define Each SDLC Link Station

You must define each SDLC link station as shown. The MAC addresses and SAPs used must correspond to their remote SNA node definitions, with MAC addresses entered in non-canonical (Token ring) format. Note that the local PU2.0/T2.1 SDLC device itself has no actual LAN address configuration. The MAC and SAP addresses used are those "spoofed" to the (LAN-attached) remote SNA node.

```
DLSw config>add sdlc
Interface # [0]? 2
SDLC Address [C1]?
Source MAC Address [000000000000]? 4000003174d1
Idblk in Hex (0-0xfff) [0]?
Idnum in Hex (0-0xfffff) [0]?
LLC Source SAP (0 for auto-assign) [0]?
LLC Destination SAP [4]?
Destination MAC Address [000000000000]? 400000000002

DLSw config>list sdlc all
Iface  Link Addr  State
 2        C1     Enabled
```

Open SAPs

The next thing to do is open SAPs on each of the bridging interfaces that perform DLSw switching. SAP numbers 0, 4, 8, and C are typically used for SNA.

```
DLSw config>open
Interface # [1]? 0
Enter SAP in hex (range 0-ff) [0]? 0
DLSw config>open 0 4
DLSw config>open 0 8
DLSw config>open 0 c

DLSw config>list open
Interface  SAP
0            0
0            4
0            8
0            C
DLSw config>
```

Following is the DLSw display after configuring. Note that the router automatically sets the SDLC MAC address when the first SDLC link station is added. Alternatively, you can use the **set mac** command to set the MAC address.

```
DLSw config>list dls
DLSw is                            ENABLED
LLC2 send Disconnect is            ENABLED

TCP Receive Buffer Size            5120
Automatic TCP connection           ALWAYS CONNECT

SRB Segment number                 020
MAC <-> IP mapping cache size      128
Max DLSw sessions                  1000
DLSw global memory allotment       153600
LLC per-session memory allotment   8192
SDLC per-session memory allotment  4096
SDLC MAC Address                   40:00:00:31:74:C1

Database age timer                 1200 seconds
Age timer resolution               300  seconds
Max wait timer for ICANREACH       20   seconds
Wait timer for LLC test response   15   seconds
Wait timer for SDLC test response  15   seconds
Join Group Interval                900  seconds
```

When you have finished configuring DLSw, exit the DLSw configuration environment and restart the router.

```
DLSw config>exit
Config (only)>restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

On Demand and Explicitly Configured TCP Sessions

DLSw can automatically re-establish TCP sessions both after a session breaks, and at start-up. The software accomplishes this through use of two DLSw configuration or monitoring commands.

- **enable auto-tcp-reconnect**
- **disable auto-tcp-reconnect**

The **enable auto-tcp-reconnect** command allows preconfigured TCP sessions to establish themselves automatically upon startup, and causes broken sessions to re-establish. This is the default behavior for the router.

Note: The **enable auto-tcp-reconnect** command only applies if you have explicitly added TCP neighbor addresses. TCP sessions created through group membership always reconnect.

If you disable the default using the **disable auto-tcp-reconnect** command, DLSw sessions are established until they are needed, and broken TCP sessions do not re-establish themselves until they are needed again. TCP group connections re-establish themselves after the interval specified using the **set timers** command expires. This command is available within the DLSw configuration and monitoring modules.

Using DLSw Groups

You can use DLSw Group capability to designate groups of DLSw routers. Setting up groups can be extremely beneficial, as it reduces the need for long lists of static IP addresses and the cost associated with maintaining them. A DLSw router can be a member of up to 64 groups.

There are three types of groups: Client, Server and Peer-to-peer Routers designated as Servers only form DLSw connections with Client routers; likewise, Client routers can only form connections with Servers. In Peer-to-peer groups, all routers form connections with each other.

Setting Up DLSw Groups

You need to configure OSPF and MOSPF if you want to use the DLSw group feature. “Configuring OSPF or RIP,” on page 10, provides instructions on how to configure these protocols.

Assign OSPF Addresses to Hardware Interfaces

Begin by issuing the **protocol ospf** command from the `Config>` prompt to enter the OSPF configuration module. Use the **set interface** command to assign the OSPF address to the hardware interface you are using to connect to the other DLSw neighbor.

Issue the DLSw Join-Group Command

At the `DLSw config>` prompt, issue the DLSw **join-group** command. The router prompts you for a group number, type of membership in the group, and other values, as shown:

```
DLSw config>join-group
Group ID (1-64 Decimal) [1]? 4
Client/Server or Peer Group member (C/S/P)- [C]?
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D)- [D]?
DLSw config>
```

Enable OSPF and Multicast OSPF

Enable the OSPF routing protocol and OSPF multicast routing at the `OSPF config>` prompt, as shown:

```
OSPF Config>enable ospf
Estimated # external routes [0]? 100
Estimated # OSPF routers [0]? 25
OSPF Config>enable multicast
Inter-area multicasting enabled? [No]:
OSPF Config>
```

Mixing T2.0 and T2.1 Remote Link Stations on Multipoint Lines

Digital routers support coexistence of SNA T2.0 and T2.1 link stations on SDLC multipoint lines.

By default, Digital's router software treats all SDLC link stations as if they are of the same type. That is, these stations all function as either T2.0 (secondary) or T2.1 (negotiable) nodes from the routers perspective.

To mix roles among the link stations on a single SDLC link, you must configure the router to support whichever remote nodes do not match the default. Link station defaults are as follows:

MaxBTU	The maximum allowed by the interface
Receive Window	7 for MOD 8, 127 for MOD 128
Transmit Window	7 for MOD 8, 127 for MOD 128
Role	Secondary

To assign mixed roles to remote link stations, use the **set remote-secondary role** command from the SDLC command prompt. The **set remote-secondary role** command enables you to configure a particular link station as Secondary or Negotiable. Use this command after adding the remote secondary with the **add-remote-secondary** command.

Note: Specify a Secondary role for PU2.0 (T2.0) SDLC devices that do not exchange XID3 configuration information; a Negotiable role for T2.1 (LEN and APPN) SDLC devices that do perform XID3 link negotiation.

2

Configuring the DLSw Protocol

This chapter lists and explains all of the configuration commands applicable to DLSw.

About DLSw Configuration and Monitoring Commands

DLSw configuration commands are available at the `DLSw config>` prompt. Changes made to the router's configuration do not take effect immediately. They only become part of the router's non-volatile configuration memory when it restarts.

Accessing the DLSw Configuration Environment

Use the router's configuration process to change the configuration of the router. The new configuration takes effect when the router is restarted.

To enter the configuration environment, type **talk 6**, or just **t 6**, This brings you to the `Config>` prompt as shown here:

```
MOS Operator Control

* talk 6
Gateway user configuration
```

If the `Config>` prompt does not appear immediately, press RET again.

All DLSw configuration commands are entered at the `DLSw config>` prompt. To access this prompt, enter the **protocol dlsw** command as shown:

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>
```

DLSw Configuration Commands

Enter DLSw configuration commands at the `DLSw config>` prompt. Table 2–1 lists the DLSw configuration commands.

Table 2–1 DLSw Command Summary

Command	Function
?(Help)	Lists the configuration commands or lists any parameters associated with that command.
Add	Adds an SDLC link station or a TCP neighbor IP address.
Ban	Lets you configure and monitor the Boundary Access Node. See Chapters 6, 7, and 8 for information about BAN.
Close-Sap	Closes a currently opened Service Access Point (SAP). A SAP is used by SDLC interface for communication on the network.
Delete	Removes configured SDLC link stations and TCP connections.
Disable	Disables the DLSw protocol, Auto-TCP-Reconnect, SDLC link station, and LLC disconnect functionality.
Enable	Enables the DLSw protocol, Auto-TCP-Reconnect, SDLC link station, and LLC disconnect functionality.
Join-Group	Allows DLSw neighbors to find each other dynamically.
Leave-Group	Removes the router from the specified DLSw group.
List	Displays information for SDLC link stations, SAPs, TCP connections, and DLSw groups.
Open-SAP	Allows DLSw to transmit data over the specified SAP.
Set	Configures LLC2 parameters, DLSw MAC address, number of DLSw sessions, SRB segment number, TCP buffer size, memory allocation, and protocol timers.
Exit	Exits the DLSw configuration process and returns you to the `Config>` process.

? (Help)

Use the **? (help)** command to list the commands available from the current prompt level. You can also enter **?** after a specific command name to list its options.

Syntax: ?

Example: **?**

```
LIST
ADD
BAN
CLOSE-SAP
DELETE
DISABLE
ENABLE
JOIN-GROUP
LEAVE-GROUP
OPEN-SAP
SET
EXIT
```

Add

Use the **add** command to configure an SDLC link station or a TCP neighbor IP address to the DLSw configuration.

Syntax: add

sdlc

tcp

sdlc

Adds information specifically for adding an SDLC link station to the configuration on a given SDLC serial interface. The **sdlc** command should be used once for each secondary station on the SDLC line.

Example: **add sdlc**

```
Interface #[0]?
SDLC Address [C1]?
Source MAC Address [0000C9123456]
Idblk in Hex (0-0xfff) [0]?
Idnum in Hex (0-0xfffff) [0]?
LLC Source SAP (0 for auto-assign) [0]?
LLC Destination SAP [4]?
Destination MAC Address [400000000001]?
```

Interface #	The interface number of the router you are adding to the SDLC link station.
SDLC Address	The SDLC address of the link station that you are connecting between 01 - FE.
Source MAC address	The MAC address for the attached SDLC PU.
Idblk in Hex	The 3-digit hexadecimal value that identifies the device (PU) to which you are connecting. Normally you use Idblk for PUs on switched lines (as opposed to leased lines). Therefore, this value should match this same parameter in the VTAM Switched Major Node that corresponds to this PU.
Idnum in Hex	The 5-digit hexadecimal value that identifies the specific device type (2.0) that you are connecting. Normally you use Ibnum for PUs on switched lines (as opposed to leased lines). Therefore, this value should match this same parameter in the VTAM Switched Major Node that corresponds to this PU.
LLC Source SAP	Identifies the PU link station to the DLSw Domain. This can be explicitly assigned via configuration or automatically assigned by software. SAPs only apply to LLC use.
LLC Destination SAP	Defines the SAP to be used when automatically attempting a connection when the link station comes up. If this SAP is 0, then the link station is in *passive* mode and does not send a CANUREACH. In this case, the router ignores the destination MAC address.
Destination MAC Address	The MAC address of the remote link station that you are connecting to. The MAC address is in non-canonical bit order (token-ring) format. This is true even if the remote end station is on the Ethernet.

tcp

Adds the IP address of the DLSw neighbor to which the TCP is connected. You can make this connection in two ways: manual configuration of IP neighboring addresses or with DLSw groups.

Example: **add tcp**

```
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.14.1
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive? (E/D) - [D]?
```

Enter the DLSw neighbor IP Address	The IP address of the remote DLSw neighbor in the IP network to which you want to make a connection.
Transmit Buffer Size	The size of the packet transmit buffer between 1024 and 32768. The default size is 5120.
Maximum Segment Size	The maximum size of the TCP segment between 1024 and 16384. The default size is 1024.
Enable/Disable Keepalive (E/D)	Indicates whether you want the DLSw neighbor to send link keepalive messages. The default is D (Disable).

Close-sap

Use the **close-sap** command to disable DLSw switching for the specified Service Access Point (SAP) by the DLSw protocol. These SAPs are used by LLC for configuration on the network.

Syntax: close-sap

Example: **close-sap**

```
Interface #[1]?
Enter SAP in hex (range 0-FE) [0] 04
Record found, will be deleted
```

Interface #	The interface number used by the open SAP.
Enter SAP in hex	The SAP number in the range 0 to FE. This value must be an even number.

Delete

Use the **delete** command to remove an SDLC link station or a TCP neighbor IP address from the DLSw configuration.

Syntax: delete

sdlc

tcp

sdlc

Removes the specified SDLC link station from the list of stations to which DLSw can connect. This also terminates any existing session.

Example: **delete sdlc**

```
Interface #[0]?
SDLC Address [C1]?
Record deleted
```

Interface #	The interface number of the router that connects to the SDLC link station.
SDLC Address	The SDLC address of the remote link station that you are deleting. Values are in the range 01 to FE.

tcp

Removes the IP address (*ip_address)* of the DLSw neighbor to which you are making the TCP connection.

Example: **delete tcp**

```
IP Address [0.0.0.0]? 128.185.14.1
```

Disable

Use the **disable** command to disable the DLSw protocol, an SDLC link station, the LLC disconnect functionality, or automatic TCP reconnection.

Syntax: disable

dls

llc disconnect on session loss

sdlc

auto-tcp-reconnect

dls

Prevents the router from transmitting DLSw functions over all DLSw configured interfaces.

Example: **disable dls**

llc

Prevents the router from terminating an LLC connection actively by issuing a DISC LLC frame when a DLSw session terminates.

This command does not affect switching functionality for LLC in DLSw. Use the **close-sap** command to stop LLC switching functionality.

Example: **disable llc**

sdlc

Prevents DLSw connections to the specified SDLC link station.

If you enter this command in the monitoring environment, it terminates the existing SDLC connection.

Example: **disable sdlc**

```
Interface #[0]? 1
SDLC Address [C1]?
Record updated
```

auto-tcp-reconnect

Disables automatic TCP station re-establishment. When this feature is disabled, TCP sessions are not established until DLSw needs them.

Example: **disable auto**

Enable

Use the **enable** command to enable the DLSw protocol, SDLC link station, and the LLC switching functionality.

Syntax: enable

dls
llc
sdlc
auto-tcp-reconnect

dls

Enables DLSw operation on the router.

Example: **enable dls**

llc

Allows the router to terminate an LLC connection upon the loss of the TCP connection.

Example: **enable llc**

sdlc

Enables DLSw connections to the specified SDLC link station.

Example: **enable sdlc**

```
Interface #[0]? 1
SDLC Address [C1]?
Record updated
```

auto-tcp-reconnect

Enables automatic TCP station re-establishment when a session breaks, and at startup. The default behavior is for this feature is enabled. When **auto-tcp-reconnect** is enabled, TCP sessions are automatically established at startup, and are re-established when they break.

Example: **enable auto**

Join-Group

Use the **join-group** command to allow DLSw neighbors to find and to create TCP sessions with each other dynamically. This eliminates the need to define TCP neighbors with the **add tcp** command.

There are three types of groups: Client, Server and Peer-to-peer. DLSw groups alleviate the need for long lists of static IP addresses, and the costs associated with maintaining them. The IP internet being used must support multicast routing.

A DLSw router can be a member of a maximum of 64 groups. DLSw group membership uses the MOSPF protocol. To use the functionality of the **join-group** command, you must configure OSPF and MOSPF from the `OSPF Config>` prompt.

When you assign a DLSw router to a group, the DLSw protocol automatically adds one of two addresses to the group number to form a multicast address. The router transmits the multicast address to identify itself to other group members and to transmit packets to those members. The two addresses that are added to the group number are **225.0.1.0** for DLSw clients and neighbors, and **225.0.65.0** for DLSw servers.

For example, the multicast address for client in group 2 is 225.0.1.2.

Syntax: join-group

Example: **join-group**

```
Group ID (1-64 Decimal) [1]? 2
Client/Server or neighbor Group member (C/S/P)- [C]?
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D)- [D]?
```

Group ID	The number of the group that you want this router to join.
Client/Server or neighbor Group Member	The type of group that you want to join, **C** for client, **S** for server, and **P** for peer-to-peer. A server forms a TCP connection with a client.
Transmit Buffer Size	The size of the packet transmit buffer in the range of 1024 to 32768. The default size is 5120.

Maximum Segment Size	The maximum size of the TCP segment in the range of 64 to 32768. The default size is 1024.
Enable/Disable Keepalive	Indicates whether you want the DLSw neighbor to send link keepalive messages. Default is **D** (Disable).

Leave-Group

Use the **leave-group** command to remove the router from any specified DLSw groups that were configured with the **join-group** command.

If you issue the **leave-group** command in the configuration environment environment, it does not affect existing TCP connections belonging to the specified group.

Syntax: leave-group *group#*

Example: **leave-group 2**

List

Use the **list** command to display DLSw information on SDLC link stations, SAPs, TCP neighbors, and groups.

Syntax: list

- dls
- groups
- llc2 sap parameters
- open llc2 saps
- sdlc link stations
- tcp neighbors

dls

Displays the information configured with the **enable** and **set** commands.

Example: **list dls**

```
DLSw is                                    ENABLED
LLC2 send Disconnect is                    ENABLED

SRB Segment number                         0030
Max DLSw Sessions                          30000
DLSw global memory allotment               600000
LLC per-session memory allotment           8192
SDLC per-session memory allotment          4096

DLSw MAC Address                  00:00:C9:00:11:19

Database age timer                         1200 seconds
Age timer resolution                       300 seconds
Max wait timer for ICANREACH               20 seconds
Wait timer for LLC response                15 seconds
Wait timer for SDLC test response          15 seconds
Join Group Interval                        900 seconds
```

DLSw is	Status of the DLSw protocol, enabled or disabled.
LLC2 send Disconnect is	Status of preventing the router from terminating an LLC2 connection upon the loss of the TCP connection. Values are enabled or disabled.
SRB Segment number	The SRB segment that identifies DLSw in the RIF.
Max DLSw Sessions	The maximum number of DLSw sessions that the router supports.
DLSw global memory allotment	The maximum amount of memory allowed for use by DLSw.
LLC per-session memory allotment	The maximum amount of memory allowed for use by each LLC session.
SDLC per-session memory allotment	The maximum amount of memory allowed for use by each SDLC DLSw session.
DLSw MAC address	The default MAC address for all SDLC PUs.
Database age timer	The maximum time to hold active database entries.
Age timer resolution	The frequency with which the database age timer fires.

Max wait timer for ICANREACH	The time to wait for a response to a CANUREACH before giving up.
Wait timer for LLC response	The maximum amount of time (in seconds) the router waits for an LLC TEST response before retransmitting an LLC TEST frame.
Wait timer for SDLC test response	The maximum amount of time (in seconds) the router waits for an SDLC TEST response before retransmitting an SDLC TEST frame.
Join Group Interval	Amount of time (in seconds) between DLSw group advertisement broadcasts.

groups

Displays group information for a DLSw neighbor previously configured with the **join-group** command.

Example: **list groups**

```
Group   Role   Xmit Bufsize   Max Segsize   Keepalive
  40   CLIENT     5120          1024        DISABLED
  42   SERVER     4096          1024        DISABLED
```

Group	The group number.
Role	The type of group: Client, Server, or Peer-to-peer.
Xmit Bufsize	The size of the TCP transmit buffer between the range of 1024 and 32768. The default size is 5120.
Max Segsize	The maximum size of the TCP segment between the range of 64 and 16384. The default size is 1024.
Keepalive	The status of the keepalive functionality, enabled or disabled.

llc2 sap parameters

Displays the LLC2 parameters configured with the **set llc2** command (refer to the **set** command for a complete explanation of these tunable parameters). These parameters are set per interface. If no changes to the LLC2 parameters were made using the **set llc2** command, no output is generated.

Example: **list llc2**

```
SAP           t1   t2   ti   n2   n3   tw   rw   nw   acc
 0             1    1   30    8    1    2    2    1    0
```

SAP	SAP number.
t1	Reply timer.
t2	Receive Ack timer.
ti	Inactivity timer.
n2	Maximum retry value.
n3	Number of I-frames received before sending ACK.
tw	Transmit window.
rw	Receive window.
nw	ACKs needed to increment Ww.
acc	The current LLC2 implementation does not use access priority. As a result, this parameter always defaults to 0.

open

Displays all open SAPs and their associated interfaces.

Example: **list open**

```
Interface      SAP
0                0
0                4
1                4
```

sdlc

Displays the SDLC link station information configured with the **add sdlc link station** command.

Example: **list sdlc**

```
Iface LinkAdr  State  Idblk Idnum Src SAP Dst SAP   Src Mac      Dest MAC
  1    C1     Enabled  000  00000  AUTO     04    0000C9123456 400000000001
```

Iface The ID number of the interface that connects to the SDLC link station.

LinkAdr The SDLC address, between 01 and FE, of the connecting link station.

State The state, enabled or disabled, of the link station.

Idblk The 3-digit hexadecimal value that identifies the device (PU) that you are connecting. Normally you use Idblk for PUs on switched lines (as opposed to leased lines). Therefore, this value should match this same parameter in the VTAM Switched Major Node that corresponds to this PU.

Idnum The 5-digit hexadecimal value that identifies the specific SDLC PU type (2.0). Normally you use Idnum for PUs on switched lines (as opposed to leased lines). Therefore, this value should match this same parameter in the VTAM Switched Major Node that corresponds to this PU.

Src SAP Identifies the PU link to the DLSw domain. This can be explicitly assigned via configuration or automatically assigned by software.

Dst SAP Identifies the remote side of the connection to the DLSw domain. If this SAP is 0, then the link station is in passive mode and does not send a CANUREACH.

Dest MAC The MAC address of the remote link station that you are connecting to. The MAC address is in non-canonical bit order (token-ring) format. This is true even if the remote end station is on the Ethernet. Use the ASRT monitoring **flip** command to help flip the MAC address, in such cases.

tcp neighbors

Displays configured DLSw neighbors that are TCP neighbors. The neighbors were configured with the **add tcp neighbor ip address** command.

Example: **list tcp**

```
Neighbor      Xmit Bufsize  Max Segsize   Keepalive
128.185.236.49    5120         1024       DISABLED
```

Neighbor	The IP address of the TCP neighbor
Transmit Buffer Size	The size of the packet transmit buffer between the range of 1024 and 32760. The default is 5120.
Maximum Segment Size	The maximum size of the TCP segment between the range of 64 and 16384. The default is 1024.
Keepalive	Displays the status of the keepalive functionality, enabled or disabled.

Open-Sap

Use the **open-sap** command to enable the transmitting of data for the specified link SAP by the DLSw protocol.

The **open-sap** command should be executed on the router which resides on the session initiator side of the connection. For example, if the client is always the sessions initiator, then you need to only open the SAPs on the client side router. If you are unsure of which side initiates the connection, then you should open the SAPs on both sides of the connection. The commonly used SNA SAP values are 04, 08, and 0C. Digital recommends that you open 04, 08, and 0C on all participating DLSw routers.

Syntax: open-sap

Example: **open-sap**

```
Interface #[1]?
Enter SAP in hex (range 0-FE) [0]?
```

Interface #	The number of the interface over which you want to open the SAP.
Enter SAP in hex	The SAP used in the range 0 to FE. The SAP must be an even number

Set

Use the **set** command to configure the size of the MAC address-to-IP address mapping cache, LLC2 parameters, DLSw MAC address, maximum number of DLSw sessions, SRB segment number, protocol timers, and TCP receive buffer size.

Syntax: set

- cache
- llc2
- mac
- maximum
- memory
- srb
- timers
- TCP

cache

The **set cache** command enables you to specify the size of the MAC address-to-IP address mapping cache.

DLSw uses information stored in this cache to discover routes to remote stations. Thus, the larger the cache, the better the chances of DLSw finding a desired remote station without broadcasting CANUREACH frames to all known TCP/IP neighbors.

Nonetheless, it is wise to avoid setting this cache size too large. Doing so consumes memory in the router. The effect is a reduction in the number of DLSw sessions the router can handle.

Example: **set cache**

```
MAC <-> IP cache size (4 - 65535) [128]?
```

llc2

Allows you to configure specific LLC2 attributes for a specific SAP.

Example: **set llc2**

```
Enter SAP in hex (range 0-FE)  [0]?
Reply timer (T1) in sec. [1]?
Receive Ack timer (T2) in 100 millisec. [1]?
Inactivity Timer (Ti) in sec. [30]?
Transmit Window (Tw), 1-128, 0=default [2]?
Receive Window (Rw), 127 Max [2]?
Acks needed to increment Ww (Nw) [1]?
Max Retry value (N2) [8]?
Number I-frames received before sending ACK (N3) [1]?
```

Enter SAP in hex	The SAP number that you want to tune. Values in the range of 0 - FE.
Reply timer (T1)	This timer expires when the LLC2 neighbor fails to receive a required acknowledgment or response from the other LLC2 neighbor.
Receive Ack timer (T2)	The delay it takes to send an acknowledgment for a received I-format frame in milliseconds.
Inactivity Timer (Ti)	This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires, the LLC2 neighbor transmits an RR until the LLC2 neighbor responds or the N2 retry count is exceeded. Default is 30 seconds.
Transmit Window (Tw)	The maximum number of I-frames that can be sent before receiving an RR. Values in the range 1 - 127. 0 sets Tw to the default. Default is 2.
Receive Window (Rw)	The maximum number of unacknowledged sequentially numbered I-frames that an LLC2 neighbor can receive from a remote host.
Acks needed to increment Ww (Nw)	The working window (Ww) is a dynamically changing shadow of the transmit window (Tw). After an LLC error is detected, the working window (Ww) is reset to 1. The 'Acks needed to increment Ww' value specifies the number of acks that the station must receive before incrementing Ww by 1. The Ww continues to be incremented in this fashion until Ww = Tw.

Max Retry value (N2)	The maximum number of times the LLC2 neighbor transmits an RR without receiving an acknowledgment when the inactivity timer (Ti) expires.
Number I-frames received before sending ACK (N3)	The value used with the T2 timer to reduce acknowledgment traffic for received I-frames. This counter is set to a specified value and decrements each time an I-frame is received. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. The default is 1. To ensure good performance, N3 should be set to a value less than the remote LLC's Tw.

mac

Sets the default source MAC address that is used for all SDLC PUs.

Example: **set mac**

```
Local DLSw MAC Address [008800880088]?
```

maximum

Sets the maximum number of DLSw sessions that the DLSw protocol can support.

Example: **set maximum**

```
Maximum number of DLSw sessions (1-60000) [1000]?
```

memory

Allows you to specify the total amount of memory allocated to DLSw, and the total amount of memory to be allotted to each DLSw session.

Example: **set memory**

```
Number of bytes to allocate for DLSw (at least 38656)[153384]?
Number of bytes to allocate per LLC session [8192]?
Number of bytes to allocate per SDLC session [4096]?
```

Note that the default value offered for the number of bytes to allocate to DLSw is probably too low to be useful for more than a small number of DLSw sessions. You should raise the memory value depending on the anticipated number of DLSw sessions, TCP neighbors, and the amount of memory available in the router.

The maximum memory required by a single session is approximately the following:

session_allocation * number_of_sessions * 75%

This number should be adjusted to 80-85% if the data stream includes many small packets.

Each TCP connection to a DLSw neighbor requires roughly 512 bytes.

For example, assuming 8K per LLC session and 4K per SDLC session, a total of 100 DLSw sessions (20 SDLC and 80 LLC) through a combination of 4 DLSw neighbors require approximately

(20 * 4K * 75%) + (80 * 8K * 75%) + (4 * 512) = 555,008 bytes.

If many small packets are anticipated, then

(20 * 4K * 85%) + (80 * 8K * 85%) + (4 * 512) = 628,736 bytes.

At no point does bad judgement in determining the DLSw allocation result in lost data. In general, the more memory allocated to DLSw, the better the overall DLSw performance. When DLSw runs out of memory, an ELS message, DLS.161 (Entering GLOBAL congestion on global DLS pool) is generated. It is okay for these messages to appear occasionally. If they appear very often, then consider increasing the DLSw allocation value.

srb

Sets the Source Routing Bridge (SRB) segment number that identifies DLSw on Token Ring networks.

Example: **set srb**

```
Enter segment number hex (1-FFF) [5]?
```

timers

Sets the DLSw protocol timers.

Example: **set timers**

```
Database age timer (1-1000 secs. Decimal) [1200]?
Age down timer resolution (1-1000 secs. Decimal) [300]?
Max wait timer ICANREACH (1-1000 secs Decimal) [20]?
Wait timer LLC test response (1-1000 secs. Decimal) [15]?
Wait timer SDLC test response (1-1000 secs. Decimal) [15]?
Group join timer interval (1-60000 secs. Decimal) [15]?
```

Database age timer	Indicates how long to hold unused DLSw database entries. Database entries map destination MAC addresses into the set of DLSw neighbors that can reach them.
Age down timer resolution	Indicates how often the database age timer fires.
Max wait timer ICANREACH	Indicates how long to wait for an ICANREACH response for a previously transmitted CANUREACH.
Wait timer LLC test response	Indicates how long to wait for an LLC test response before giving up.
Wait timer SDLC test response	Indicates how long to wait for an SDLC test response before giving up.

Group join timer interval

The group interval timer is significant when you configure a pair of DLSw routers to use a TCP group with the **join** command, rather than statically configuring each router with the adjacent IP address of its DLS neighbor using the **add tcp** command.

When you use the **set timer** command from the DLSw> prompt, you are prompted for a group update interval value. When the router is first powered up, it sends group packets every 15 seconds or the configured group update interval, whichever is smaller, for the first 6 transmissions, and then the configured time thereafter.

If an IP router between two partner DLSw routers goes down, the attempt to re-establish the TCP connection takes place once the configured group update interval value has elapsed after the IP router has recovered. If the configured value is 15 seconds, then the attempt to re-establish the TCP connection takes place 15 seconds after the recovery of the IP router is detected.

The range is 1 to 60000 seconds in decimal. The default is 900 seconds.

tcp

Sets the TCP receive buffer size for the router. The mimimum value is 1024 and the maximum is 32768. Note that the command does not enable you to set the buffer size for each TCP session.

Example: **set TCP**

```
TCP receive buffer size (Decimal) [4096]?
```

The ability to set the receive buffer size is useful when communicating over networks that use a high bandwidth delay product, such as a FR network running over a T1 line. Unless you have a reason to increase the buffer size, you should accept the default value of 4096. Setting the buffer size too high uses up router memory.

Exit

Use the **exit** command to return to the `Config>` or + prompt.

Syntax: exit

`Example:` **`exit`**

3

Monitoring the DLSw Protocol

This chapter includes all of the monitoring commands applicable to DLSw.

About DLSw Monitoring Commands

DLSw monitoring commands are available at the `DLSw>` prompt. Monitoring commands take effect immediately, but do not become part of router's non-volatile configuration memory. Thus, while monitoring commands allow you to make real-time changes to the router's configuration, these changes are temporary. The router's configuration memory overwrites them when the router restarts.

Monitoring consists of these actions:

- Monitoring the protocols and network interfaces currently in use by the router.
- Displaying ELS (Event Logging System) messages relating to router activities and performance.
- Making real-time changes to the DLSw configuration without permanently affecting the router's non-volatile configuration memory.

Accessing the DLSw Monitoring Environment

To enter the monitoring environment, enter **talk 5**, or just **t 5**. This brings you to the monitoring environment as shown:

```
MOS Operator Control

* talk 5
+
```

You enter DLSw monitoring commands at the DLSw> prompt. To access this prompt, enter the **protocol dls** command at the + prompt as shown:

```
+ protocol dls
DLSw>
```

DLSw Commands

Enter DLSw monitoring commands at the DLSw> prompt. Table 3–1 lists the DLSw configuration and monitoring commands.

Table 3–1 DLSw Command Summary

Command	Function
?(Help)	Lists the configuration commands or lists any parameters associated with that command.
Add	Adds an SDLC link station or a TCP neighbor IP address.
Ban	Lets you configure and monitor the Boundary Access Node. See Chapters 6, 7, and 8 for information about BAN.
Close-Sap	Closes a currently opened Service Access Point (SAP). A SAP is used by SDLC interface for communication on the network.
Delete	Removes configured SDLC link stations and TCP connections.
Disable	Disables the DLSw protocol, Auto-TCP-Reconnect, SDLC link station, and LLC disconnect functionality.
Enable	Enables the DLSw protocol, Auto-TCP-Reconnect, SDLC link station, and LLC disconnect functionality.
Join-Group	Allows DLSw neighbors to find each other dynamically.
Leave-Group	Removes the router from the specified DLSw group.
List	Displays information for SDLC link stations, SAPs, TCP connections, and DLSw groups.
Open-SAP	Allows DLSw to transmit data over the specified SAP.

Set	Configures LLC2 parameters, DLSw MAC address, number of DLSw sessions, SRB segment number, TCP buffer size, memory allocation, and protocol timers.
Exit	Exits the DLSw configuration process and returns you to the `Config>` process.

? (Help)

Use the **? (help)** command to list the commands available from the current prompt level. You can also enter **?** after a specific command name to list its options.

Syntax: ?

`Example:` **`?`**

```
ADD
BAN
CLOSE-SAP
DELETE
DISABLE
ENABLE
JOIN-GROUP
LEAVE-GROUP
LIST
OPEN-SAP
SET
EXIT
```

Add

Use the **add** command to configure an SDLC link station or a TCP neighbor IP address to the DLSw configuration.

Syntax: add

sdlc

tcp

sdlc

Adds information specifically for adding an SDLC link station to the configuration on a given SDLC serial interface. The **sdlc** command should be used once for each secondary station on the SDLC line.

Example: **add sdlc**

```
Interface #[0]?
SDLC Address [C1]?
Source MAC Address [0000C9123456]
Idblk in Hex (0-0xfff) [0]?
Idnum in Hex (0-0xfffff) [0]?
LLC Source SAP (0 for auto-assign) [0]?
LLC Destination SAP [4]?
Destination MAC Address [400000000001]?
```

Interface #	The interface number of the router you are adding to the SDLC link station.
SDLC Address	The SDLC address of the link station that you are connecting between 01 - FE.
Source MAC address	The MAC address for the attached SDLC PU.
Idblk in Hex	The 3-digit hexadecimal value that identifies the device (PU) to which you are connecting. Normally you use Idblk for PUs on switched lines (as opposed to leased lines). Therefore, this value should match this same parameter in the VTAM Switched Major Node that corresponds to this PU.
Idnum in Hex	The 5-digit hexadecimal value that identifies the specific device type (2.0) that you are connecting. Normally you use Ibnum for PUs on switched lines (as opposed to leased lines). Therefore, this value should match this same parameter in the VTAM Switched Major Node that corresponds to this PU.

LLC Source SAP	Identifies the PU link station to the DLSw Domain. This can be explicitly assigned via configuration or automatically assigned by software. SAPs only apply to LLC use.
LLC Destination SAP	Defines the SAP to be used when automatically attempting a connection when the link station comes up. If this SAP is 0, then the link station is in *passive* mode and does not send a CANUREACH. In this case, the router ignores the destination MAC address.
Destination MAC Address	The MAC address of the remote link station that you are connecting to. The MAC address is in non-canonical bit order (token-ring) format. This is true even if the remote end station is on the Ethernet.

tcp

Adds the IP address of the DLSw neighbor to which the TCP is connected. You can make this connection in two ways: manual configuration of IP neighboring addresses or with DLSw groups.

Example: **add tcp**

```
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.14.1
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive? (E/D) - [D]?
```

Enter the DLSw neighbor IP Address	The IP address of the remote DLSw neighbor in the IP network to which you want to make a connection.
Transmit Buffer Size	The size of the packet transmit buffer between 1024 and 32768. The default size is 5120.
Maximum Segment Size	The maximum size of the TCP segment between 1024 and 16384. The default size is 1024.
Enable/Disable Keepalive (E/D)	Indicates whether you want the DLSw neighbor to send link keepalive messages. The default is D (Disable).

Close-sap

Use the **close-sap** command to disable DLSw switching for the specified Service Access Point (SAP) by the DLSw protocol. These SAPs are used by LLC for configuration on the network.

Syntax: close-sap

Example: **close-sap**

```
Interface #[1]?
Enter SAP in hex (range 0-FE) [0] 04
Record found, will be deleted
```

Interface #	The interface number used by the open SAP.
Enter SAP in hex	The SAP number in the range 0 to FE. This value must be an even number.

Delete

Use the **delete** command to remove an SDLC link station or a TCP neighbor IP address from the DLSw configuration.

Syntax: delete
sdlc
tcp

sdlc

Removes the specified SDLC link station from the list of stations to which DLSw can connect. This also terminates any existing session.

Example: **delete sdlc**

```
Interface #[0]?
SDLC Address [C1]?
Record deleted
```

Interface #	The interface number of the router that connects to the SDLC link station.
SDLC Address	The SDLC address of the remote link station that you are deleting. Values are in the range 01 to FE.

tcp

Removes the IP address (*ip_address)* of the DLSw neighbor to which you are making the TCP connection. This also terminates the TCP connection if one exists.

```
Example: delete tcp

IP Address [0.0.0.0]? 128.185.14.1
```

Disable

Use the **disable** command to disable the DLSw protocol, an SDLC link station, the LLC disconnect functionality, or automatic TCP reconnection.

Syntax: disable

dls

llc disconnect on session loss

sdlc

auto-tcp-reconnect

dls

Prevents the router from transmitting DLSw functions over all DLSw configured interfaces.

```
Example: disable dls
```

llc

Prevents the router from terminating an LLC connection actively by issuing a DISC LLC frame when a DLSw session terminates.

This command does not affect switching functionality for LLC in DLSw. Use the **close-sap** command to stop LLC switching functionality.

```
Example: disable llc
```

sdlc

Prevents DLSw connections to the specified SDLC link station.

If you enter this command in the monitoring environment, it terminates the existing SDLC connection.

Example: **disable sdlc**

```
Interface #[0]? 1
SDLC Address [C1]?
Record updated
```

auto-tcp-reconnect

Disables automatic TCP station re-establishment. When this feature is disabled, TCP sessions are not established until DLSw needs them.

Example: **disable auto**

Enable

Use the **enable** command to enable the DLSw protocol, SDLC link station, and the LLC switching functionality.

Syntax: enable

- dls
- llc
- sdlc
- auto-tcp-reconnect

dls

Enables DLSw operation on the router.

Example: **enable dls**

llc

Allows the router to terminate an LLC connection upon the loss of the TCP connection.

Example: **enable llc**

sdlc

Enables DLSw connections to the specified SDLC link station.

Example: **enable sdlc**

```
Interface #[0]? 1
SDLC Address [C1]?
Record updated
```

auto-tcp-reconnect

Enables automatic TCP station re-establishment when a session breaks, and at startup. The default behavior is for this feature is enabled. When **auto-tcp-reconnect** is enabled, TCP sessions are automatically established at startup, and are re-established when they break.

Example: **enable auto**

Join-Group

Use the **join-group** command to allow DLSw neighbors to find and to create TCP sessions with each other dynamically. This eliminates the need to define TCP neighbors with the **add tcp** command.

There are three types of groups: Client, Server and Peer-to-peer. DLSw groups alleviate the need for long lists of static IP addresses, and the costs associated with maintaining them. The IP internet being used must support multicast routing.

A DLSw router can be a member of a maximum of 64 groups. DLSw group membership uses the MOSPF protocol. To use the functionality of the **join-group** command, you must configure OSPF and MOSPF from the `OSPF Config>` prompt.

When you assign a DLSw router to a group, the DLSw protocol automatically adds one of two addresses to the group number to form a multicast address. The router transmits the multicast address to identify itself to other group members and to transmit packets to those members. The two addresses that are added to the group number are **225.0.1.0** for DLSw clients and neighbors, and **225.0.65.0** for DLSw servers.

For example, the multicast address for client in group 2 is 225.0.1.2.

Syntax: join-group

Example: **join-group**

```
Group ID (1-64 Decimal) [1]? 2
Client/Server or neighbor Group member (C/S/P)- [C]?
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D)- [D]?
```

Group ID	The number of the group that you want this router to join.
Client/Server or neighbor Group Member	The type of group that you want to join, **C** for client, **S** for server, and **P** for peer-to-peer. A server forms a TCP connection with a client.
Transmit Buffer Size	The size of the packet transmit buffer in the range of 1024 to 32768. The default size is 5120.
Maximum Segment Size	The maximum size of the TCP segment in the range of 64 to 32768. The default size is 1024.
Enable/Disable Keepalive	Indicates whether you want the DLSw neighbor to send link keepalive messages. Default is **D** (Disable).

Leave-Group

Use the **leave-group** command to remove the router from any specified DLSw groups that were configured with the **join-group** command.

If you issue the **leave-group** command in the monitoring environment, it terminates existing TCP connections belonging to the specified group.

Syntax: leave-group *group#*

Example: **leave-group 2**

List

Use the **list** command to display DLSw information on SDLC link stations, SAPs, TCP neighbors, and groups.

Syntax: list

dls global
dls sessions all
dls sessions ban
dls sessions dest
dls sessions detail
dls sessions src
dls sessions ip
dls sessions range
dls sessions state
dls cache all
dls cache range
dls memory
llc2 open
llc2 sap
llc2 session
sdlc sessions
sdlc link
tcp config
tcp sessions
groups

dls

Displays information that pertains to the DLSw protocol. The options (*global, sessions,* and *cache)* for the DLSw parameters are described below and on the following pages.

Global	Displays status, timer, and MAC address information about the DLSw protocol.
Sessions	Displays current DLS session information including source, destination, state, flags, destination IP address, and ID.
Cache	Lists the addresses in the DLSw MAC address cache.

dls global

Displays DLS global parameter information.

Example: **list dls global**

```
DLSw is                          ENABLED
LLC2 send Disconnect is          ENABLED

SRB Segment number               020
Max DLSw Sessions                30000
DLSw global memory allotment             600000
LLC per-session memory allotment         8192
SDLC per-session memory allotment        4096

DLSw MAC Address                         00:00:C9:00:11:19

Database age timer                           1200 seconds
Age timer resolution                         300  seconds
Max wait timer for ICANREACH                 20   seconds
Wait timer for LLC test response             15   seconds
Wait timer for SDLC test response            15   seconds
Join Group Interval                          900  seconds
```

DLSw is	Status of the DLSw protocol, enabled or disabled.
LLC2 send disconnect is	Status of preventing the router from terminating an LLC2 connection upon the loss of the TCP connection. Values are enabled or disabled.
SRB Segment number	The SRB segment that identifies DLSw in the RIF.
Max DLSw Sessions	The maximum number of DLSw sessions that the router can support.
DLSw global memory allotment	The maximum amount of memory allowed for use by DLSw.

LLC per-session memory allotment	The maximum amount of memory allowed for use by each LLC session.
SDLC per-session memory allotment	The maximum amount of memory allowed for use by each SDLC session.
DLSw MAC address	The default MAC address for all SDLC PUs.
Database age timer	The maximum time to hold active database entries.
Age timer resolution	The frequency with which the database age timer fires.
Max wait timer for ICANREACH	The time to wait for a response to a CANUREACH before giving up.
Wait timer for LLC test response	The maximum amount of time (in seconds) the router waits for an LLC TEST response before retransmitting an LLC TEST frame.
Wait timer for SDLC test response	The maximum amount of time (in seconds) the router waits for an SDLC TEST response before retransmitting an SDLC TEST frame.
Join Group Interval	Amount of time (in seconds) between DLSw group advertisement broadcasts.

dls sessions all

Displays current dls session information.

Example: **list dls session all**

```
   Source           Destination       State    Flags  Dest. IP Addr Id
1. 400000000003 04 500000000003 04  Connected       128.185.236.51   2
```

Source	The source MAC address of the session.
Destination	The destination MAC address of the session.
State	Current state of the session:
	Disconnected The initial state with no circuit or connection established.

Rslv_pend The target DLSw is awaiting either a SSP_STARTED indication following a SSP_START request.

Circ_pend The target DLSw is waiting a SSP_REACHACK response to an SSP_ICANREACH message.

Circ_est The end-to-end circuit was established.

Cir_rstrt The DLSw that originated the reset is awaiting the restart of the data link and a SSP_RESTARTED response to an SSP_RESTART message.

Conn_pend The origin DLSw is awaiting an SSP_CONTACTED response to an SSP_CONTACT message.

Cont_pend The target DLSw is awaiting an SSP_CONTACTED confirmation to an SSP_CONTACT message.

Connect_state The origin DLSw is awaiting an SSP_CONTACTED response to a SSP_CONTACT message.

Disc_pend The DLSw that originated the disconnect is awaiting an SSP_HALTED response to an SSP_HALT message.

Halt_pending The remote DLSw is awaiting an SSP_HALTED indication following an SSP_HALT request.

Halt_rstrt The remote DLSw is awaiting an SSP_HALTED indication following an SSP_HALT request.

Restart_pend The remote DLSw is awaiting an SSP_HALTED indication following an SSP_HALT request.

Reset_pend The remote DLSw is awaiting the SSP_HALTED indication following an SSP_HALT request.

Flags Flags can be one of the following:

A – CONTACT MSG PENDING
B – SAP RESOLVE PENDING
C – EXIT BUSY EXPECTED
D – TCP BUSY

Dest. IP Addr The IP address of the remote DLSw peer.

Id The number used to identify the session. Use this number in any command that requires the session ID.

dls sessions ban

Displays current information on BAN sessions.

Example: **list dls session ban**

```
BAN port number (user 0 for all ports) [0]?
No active sessions
```

dls session dest

Displays DLS session information by destination MAC address.

Example: **list dls session dest**

```
Destination MAC Address [40000000001]? 50000000003

   Source         Destination    State       Flags  Dest. IP Addr Id
1. 400000000003  500000000003    Connected          128.185.236.51 2
2. 400000000002  500000000003    Connected          128.185.236.52 3
```

dls session detail

Displays detailed DLS session information.

Example: **list dls session detail**

```
Session Identifier [1]?

    Source        Destination      State       Dest. IP Addr  Id
1. 400000000003  500000000003 04   Connected   128.185.236.51  2

              Personality:          TARGET
              XIDs sent:            2
              XIDs rcvd:            0
              Datagrams sent:       0
              Datagrams rcvd:       0
              Info frames sent:     15
              Info frames rcvd:     0
              RIF:                  0620 0202 B0B0
```

Personality	The ORIGINATOR (initiator) or TARGET (recipient) of the connection.
XIDs sent *XIDs rcvd*	The total number of XIDs that this DLSw peer has sent and received from the remote DLSw peer.
Datagrams sent *Datagrams rcvd*	The total number of datagrams that this DLSw peer has sent and received from the remote DLSw peer.
Info frames sent *Info frames rcvd*	The total number of I-frames that this DLSw peer has sent and received from the DLSw peer.
RIF	The information that is included in the RIF of the LLC test frame.

dls session ip

Displays IP session information.

Example: **list dls session ip**

```
    Source        Destination      State       Dest. IP Addr  Id
1. 400000000003  500000000003 04   Connected   128.185.236.51  2
```

dls session range

The range of DLS sessions that you want to display. This number is located to the left of the source MAC address.

Example: **list dls session range**

```
              Start [1]?
              Stop  [1]?
```

```
    Source        Destination      State       Dest. IP Addr  Id
1. 400000000003  500000000003 04   Connected   128.185.236.51  2
```

dls session src

Displays all DLSw session information by source MAC Address.

Example: **list dls session src**

```
              Source MAC Address [400000000001]?

   Source      Destination    State    Flags   Dest. IP Addr    Id
1. SDLC 04  400000000002 04  Connected        10.1.49.401       1
```

Note: In this example source MAC address 400000000001 maps to the "SDLC 04" name. If the user does not know the source MAC address required as a parameter for this command, then do a "list SDLC link" to obtain this information.

dls session state

Displays all DLSw sessions in the specified state. The DLSw session states are defined as follows:

Example: **list dls session state**

```
              DISCONECT = 0,  RSLV_PEND = 1
              CIRC_PEND = 2,  CIRC_EST  = 3
              CIR_RSTRT = 4,  CONN_PEND = 5
              CONT_PEND = 6,  CONNECTED = 7
              DISC_PEND = 8,  HALT_PEND = 9
              REST_PEND = 10

       Enter state value (0–10) [7]?

   Source            Destination    State     Flags  Dest. IP Addr  Id
1. 400000000003 04 10005AF181A4 04 Connected        128.185.236.84   0
2. 400000000002 04 400000000088 04 Connected        128.185.236.84   1
```

dls cache all

Lists the entries in the DLSw MAC address cache. This cache contains a database of the most recent MAC address to IP neighbor translations. It provides the MAC address, time to live (in seconds) in the cache, and the neighbor's IP address.

Example: **list cache all**

```
      Mac Address      Age        IP Address(es)
1.    10005AF1809B     810        128.185.236.84
2.    10005AF181A4     1170       128.185.236.84
3.    400000000088     1170       128.185.236.84
```

dls cache range

Displays information for a specified range of cache entries.

Example: **list cache range**

```
Start[2]?

Stop[2]?

            Mac Address        Age     IP Address(es)
     2.     10005AF181A4       1170    128.185.236.84
```

dls memory

This command lists all existing DLSw sessions and the amount of memory in use by each session. It also displays the following flow control states.

Ready	The session is not congested.
Session	The session has used most of its session allotment and probably has flow controlled the data link.
G*lobal*	The session is congested due to a shortage of memory in the router.

The *currently in use* field shows the total amount of memory currently allocated by DLS. This includes all session allocations, control messages and TCP receive buffers.

Example: **list dls memory**

```
              Global DLS pool bytes requested:     600000
              bytes granted:                       600000
              currently in use:                    6144


              Session   Initial  Current  Congest
Id Source           Destination      State     alloc  alloc   State
6. 400000000003 04 0000c9001119 04  Connected  16384  16384   READY
5. SDLC 04-C1   04 400000000003 04  Connected  16384  16384   READY
```

groups

Displays information for all configured groups to which the router belongs.

Example: **list groups**

```
Group   Role   Xmit Bufsize   Max Segsize   Keepalive
  40   CLIENT     5120          1024        DISABLED
  42   SERVER     4096          1024        DISABLED
```

Group The number of the group.

Role The type of group.

Xmit Bufsize The size of the TCP transmit buffer between the range of 1024 and 32768. The transmit buffer size must be at least twice the maximum segment size. Default is 5120.

Max Segsize The maximum size of the TCP segment, between the range of 64 and 16384. The default is 1024.

Keepalive The status of the keepalive functionality, enabled or disabled.

llc2 open

Displays information that pertains to LLC2. The options (*open SAPs, SAP parameters,* and *sessions)* for LLC2 are described below and on the following pages.

Open Displays information for all currently open SAPs on interfaces between LLC2 peers.

Example: **list llc2 open**

```
Interface      SAP
    0           0
    0           4
```

llc2 sap

Displays LLC2 parameter configuration information. Only configurations that were changed are displayed. If the **set llc2** command was not used, no output is generated.

Example: **list llc2 sap**

```
SAP           T1    t2    ti    n2    n3    tw    rw    nw    acc
```

llc2 sessions all

Displays current information for all LLC2 sessions.

Example: **list llc2 sessions**

```
   SAP  Int.   Remote Addr    Local Addr   State        RIF
1. 04   6      400000000003   500000000003   CONTACTED  0620 0202 B0B0
```

State The state of the llc session. The following states can be displayed:

Disconnected Indicates the data link control structure exists but no data link is established.

Connect_pend The connect pending state is entered when a test command frame to NULL SAP is received or when a DLC_START_DL command is received from DLSw.

Resolve_pend The resolve pending state is entered when a DLC_RESOLVE_C command is sent to DLSw.

Connected This is a steady state where LLC Type 1 level services are available through the DLSw cloud. This state is entered when a DLC_RESOLVE_R command is received from DLSw or when a TEST response frame is received from the network.

Contact_pend This state is entered whenever a response to a transmitted or received SABME is outstanding.

Disconnect_Pending

This state is entered whenever a DISC command was transmitted or received, or a DLC_HALT was received from DLSw.

llc2 sessions range

Displays current information for the selected range of LLC2 sessions.

Example: **list llc2 sessions range**

```
Start[1]?

Stop[1]?


   SAP  Int.   Remote Addr    Local Addr     State      RIF
1. 04   6      400000000003   500000000003   Contacted  0620 0202 B0B0
```

sdlc sessions

Displays information about all SDLC DLS sessions within the router.

Example: **list sdlc sessions**

```
   NET  Addr.  Source SAP  Dst SAP   Dest Mac        InQ  OutQ  State
1. 2    C1         04         04  40:00:00:00:00:02  00  00  Contacted
```

sdlc link

Displays configured parameters for the SDLC attached PU.

Example: **list sdlc link**

```
Interface #, or 'ALL' [0]? 2
SDLC Address [C1]? D1
State:    Enabled
Idblk:    000
Idnum:    00000
Src SAP:  04
Dest SAP: 04
Src MAC:  50:00:00:00:00:16
Dest MAC: 40:00:00:00:00:02
```

tcp config

Displays information on all configured TCP sessions.

Example: **list tcp config**

```
Neighbor       Xmit Bufsize    Max Segsize     Keepalive
128.185.236.49    5120            1024          DISABLED
```

tcp sessions

Displays the status of all known TCP sessions to peer DLSw routers.

Example: **list tcp sessions all**

```
  Group IP Address     Conn State  Pkts Sent Pkts Rcvd Bytes Sent Bytes Rcv
1.Clnt  50 10.1.49.16 Established    325       338        1876      1948
2.Clnt  10 10.1.59.16 Established    426       451        2130      2202
```

Open-Sap

Use the **open-sap** command to enable the transmitting of data for the specified link SAP by the DLSw protocol.

The **open-sap** command should be executed on the router which resides on the session initiator side of the connection. For example, if the client is always the sessions initiator, then you need to only open the SAPs on the client side router. If you are unsure of which side initiates the connection, then you should open the SAPs on both sides of the connection. The commonly used SNA SAP values are 04, 08, and 0C. Digital recommends that you open 04, 08, and 0C on all participating DLSw routers.

Syntax: open-sap

Example: **open-sap**

```
Interface #[1]?
Enter SAP in hex (range 0-FE) [0]?
```

Interface #	The number of the interface over which you want to open the SAP.
Enter SAP in hex	The SAP used in the range 0 to FE. The SAP must be an even number

Set

Use the **set** command to configure the size of the MAC address-to-IP address mapping cache, LLC2 parameters, DLSw MAC address, maximum number of DLSw sessions, SRB segment number, protocol timers, and TCP receive buffer size.

Syntax: set

- llc2
- maximum
- memory
- timers

llc2

Allows you to configure specific LLC2 attributes for a specific SAP.

Example: **set llc2**

```
Enter SAP in hex (range 0-FE)  [0]?
Reply timer (T1) in sec. [1]?
Receive Ack timer (T2) in 100 millisec. [1]?
Inactivity Timer (Ti) in sec. [30]?
Transmit Window (Tw), 1-128, 0=default [2]?
Receive Window (Rw), 127 Max [2]?
Acks needed to increment Ww (Nw) [1]?
Max Retry value (N2) [8]?
Number I-frames received before sending ACK (N3) [1]?
```

Reply timer (T1)	This timer expires when the LLC2 neighbor fails to receive a required acknowledgment or response from the other LLC2 neighbor.
Receive Ack timer (T2)	The delay it takes to send an acknowledgment for a received I-format frame in milliseconds.
Inactivity Timer (Ti)	This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires, the LLC2 neighbor transmits an RR until the LLC2 neighbor responds or the N2 retry count is exceeded. Default is 30 seconds.
Transmit Window (Tw)	The maximum number of I-frames that can be sent before receiving an RR. Values in the range 1 - 127. 0 sets Tw to the default. Default is 2.

Receive Window (Rw)	The maximum number of unacknowledged sequentially numbered I-frames that an LLC2 neighbor can receive from a remote host.
Acks needed to increment Ww (Nw)	The working window (Ww) is a dynamically changing shadow of the transmit window (Tw). After an LLC error is detected, the working window (Ww) is reset to 1. The 'Acks needed to increment Ww' value specifies the number of acks that the station must receive before incrementing Ww by 1. The Ww is incremented in this fashion until Ww = Tw.
Max Retry value (N2)	The maximum number of times the LLC2 neighbor transmits an RR without receiving an acknowledgment when the inactivity timer (Ti) expires.
Number I-frames received before sending ACK (N3)	The value used with the T2 timer to reduce acknowledgment traffic for received I-frames. This counter is set to a specified value and decrements each time an I-frame is received. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1.

maximum

Sets the maximum number of DLSw sessions that the DLSw protocol can support.

Example: **set maximum**

```
Maximum number of DLSw sessions (1-60000) [1000]?
```

memory

Allows you to specify the total amount of memory allocated to DLSw, and the total amount of memory to be allotted to each DLSw session. This command affects only new DLSw sessions.

Example: **set memory**

```
Number of bytes to allocate for DLSw (at least 38656)[600000]?
Number of bytes to allocate per LLC session [8192]?
Number of bytes to allocate per SDLC session [4096]?
```

Note that the default value offered for the number of bytes to allocate to DLSw is probably too low to be useful for more than three to four DLSw sessions. You should raise the memory value depending on the anticipated number of DLSw sessions, TCP neighbors, and the amount of memory available in the router.

The maximum memory required by a single session is approximately the following:

session_allocation * number_of_sessions * 75%

This number should be adjusted to 80-85% if the data stream includes many small packets.

Each TCP connection to a DLSw neighbor requires roughly 512 bytes.

For example, assuming 8K per LLC session and 4K per SDLC session, a total of 100 DLSw sessions (20 SDLC and 80 LLC) through a combination of 4 DLSw neighbors requires approximately

(20 * 4K * 75%) + (80 * 8K * 75%) + (4 * 512) = 555,008 bytes.

If many small packets are anticipated, then

(20 * 4K * 85%) + (80 * 8K * 85%) + (4 * 512) = 628,736 bytes.

At no point does bad judgement in determining the DLSw allocation result in lost data. In general, the more memory allocated to DLSw, the better the overall DLSw performance. When DLSw runs out of memory, an ELS message, DLS.161 (Entering GLOBAL congestion on global DLS pool) is generated. It is okay for these messages to appear occasionally. If they appear very often, then consider increasing the DLSw allocation value.

timers

Sets the DLSw protocol timers.

Example: **set timers**

```
Database age timer (1-1000 secs. Decimal) [1200]?
Age down timer resolution (1-1000 secs. Decimal) [300]?
Max wait timer ICANREACH (1-1000 secs Decimal) [20]?
Wait timer LLC test response (1-1000 secs. Decimal) [15]?
Wait timer SDLC test response (1-1000 secs. Decimal) [15]?
Group join timer interval (1-60000 secs. Decimal) [15]?
```

Database age timer	Indicates how long to hold unused DLSw database entries. Database entries map destination MAC addresses into the set of DLSw neighbors that can reach them.
Age down timer resolution	Indicates how often the database age timer fires.
Max wait timer ICANREACH	Indicates how long to wait for an ICANREACH response for a previously transmitted CANUREACH.
Wait timer LLC test response	Indicates how long to wait for an LLC test response before giving up.
Wait timer SDLC test response	Indicates how long to wait for an SDLC test response before giving up.
Group join timer interval	The group interval timer is significant when you configure a pair of DLSw routers to use a TCP group with the **join** command, rather than statically configuring each router with the adjacent IP address of its DLS neighbor using the **add tcp** command. When you use the **set timer** command from the DLSw> prompt, you are prompted for a group update interval value. When the router is first powered up, it sends group packets every 15 seconds or the configured group update interval whichever is smaller, for the first 6 transmissions, and then the configured time thereafter. If an IP router between two partner DLSw routers goes down, the attempt to re-establish the TCP connection takes place once the configured group update interval value has elapsed after the IP router has recovered. If the configured value is 15 seconds, then the attempt to re-establish the TCP connection takes place 15 seconds after the recovery of the IP router is detected. The range is 1 to 60000 seconds in decimal. The default is 15 seconds.

Exit

Use the **exit** command to return to the `Config>` or + prompt.

Syntax: exit

`Example:` **`exit`**

4

Configuring SDLC Interfaces

This chapter describes the SDLC configuration commands.

About SDLC Configuration Commands

SDLC configuration commands are available at the `SDLC # Config>` prompt, where # identifies the interface you specify with the **network** command. Changes made to the router's configuration do not take effect immediately, but become part of the router's non-volatile configuration memory when the router restarts.

When the router restarts, the configuration stored in non-volatile configuration memory supersedes the effects of monitoring commands.

Accessing the SDLC Configuration Environment

To enter the configuration process, follow these steps.

1. At the MOS prompt (*), enter **talk 6** or just **t 6**. This brings you to the `Config>` prompt.

   ```
   * talk 6

   Config>
   ```

   If the `Config>` prompt does not appear immediately, press RET again.

2. Next, enter the **network** command, plus the number of an SDLC interface configured earlier.

```
Config>network 3
SDLC 3 Config>
```

SDLC Commands

This section describes the SDLC configuration commands.

When you enter commands, the router interface often prompts you for values and parameters. In cases where a default answer exists, you can accept it by pressing ↵. Default answers are enclosed in brackets immediately following the command prompt.

Table 4–1 lists SDLC configuration commands and their functions.

Note: Digital routers support SDLC connections over RS-232, X.21 and V.35 serial interfaces.

Table 4–1 SDLC Command Summary

Command	Function
?(Help)	Lists the configuration and monitoring commands or lists any parameters associated with that command.
Add	Adds an SDLC remote-secondary link station.
Delete	Removes an SDLC remote-secondary link station.
Disable	Prevents connections to an SDLC link station.
Enable	Allows connections to an SDLC link station.
List	Displays configured information for an SDLC link station.
Set	Configures specific interface and remote- secondary information.
Exit	Exits the SDLC configuration or monitoring environment.

? (Help)

Use the **? (help)** command to list the available commands that are available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: ?

Example: **?**

```
Set
Add
Disable
Delete
Enable
List
Exit
```

Add

Use the **add** command to add a remote-secondary end station. You may elect not to use this command. By default, the router adds a remote-secondary end station to ensure proper operation of the SDLC interface. However, you must use this command if you want to mix T2.0 and T2.1 link stations on the same multipoint line. The router is considered the primary end station by default.

Syntax: add remote-secondary

Example: **add remote-secondary**

```
Enter station address (in hex) [C3]?
Enter remote station name [SDLC_C3]?
Enter max packet size [2009]?
Enter receive window [7]?
Enter transmit window [7]?
Enable negotiable mode [Yes or (No)]?
```

Enter station address	The remote station's SDLC address in the range 01 - FE.
Enter remote station name	The name designation of the SDLC station (maximum characters is 8).
Enter max packet size	The maximum packet size that can be sent to or received from the remote link station. This value cannot be greater than that specified for the link with the **set link frame-size** command.

Enter receive window	The maximum number of packets that the router can receive without sending a response.
Enter transmit window	The maximum number of packets that the router can transmit without receiving a response.
Enter negotiable mode	Indicates whether the remote-secondary end station you are adding is a negotiable (T2.1) or secondary (T2.0) node on the multipoint line.

Note: Specify a Secondary role for PU2.0 (T2.0) SDLC devices that do not exchange XID3 configuration information; a Negotiable role for T2.1 (LEN and APPN) SDLC devices that do perform XID3 link negotiation.

Delete

Use the **delete** command to remove the specified remote-secondary end station (remote station name or address) from the SDLC configuration. The router is considered the primary end station (default).

Syntax: delete remote-secondary *name* or *address*

Example: **`delete remote-secondary C1`**

Disable

Use the **disable** command to prevent connections from being created with a SDLC link station.

Syntax: disable
link
remote-secondary . . .

link

Prevents the establishment of SDLC sessions on any SDLC link stations on the interface.

Example: **`disable link`**

remote-secondary *name* or *address*

Prevents establishment of an SDLC session to the specified remote-secondary end station (remote station name or address).

Example: **disable remote-secondary c1**

Enable

Use the **enable** command to enable connections to remote SDLC link stations.

Syntax: enable
link
remote-secondary . . .

link

Allows subsystems in the router (e.g. DLSw) to use SDLC's facilities.

Example: **enable link**

remote-secondary *name* or *address*

Allows connections to the specified remote-secondary end station (link station name).

Example: **enable remote-secondary C1**

List

Use the **list** command in the SDLC configuration process to display configuration information on one or all SDLC link stations.

Syntax: list

link

remote-secondary . . .

link

Displays information for the SDLC interface.

Example: **list link**

```
Link configuration for: LINK_0   (ENABLED)

Default role:  PRIMARY        Type:          POINT-TO-POINT
Duplex:        FULL           Modulo:        8
Idle State:    FLAG           Encoding:      NRZ
Clocking:      EXTERNAL       Frame Size:    2048

Timers:        XID/TEST response:            0.5 sec
               SNRM response: 2.0 sec
               Poll response: 0.5 sec
               Inter-poll delay:             0.2 sec
               RTS hold delay:               0.0 sec
               Inter-frame delay:            DISABLED

Counters:      XID/TEST retry:               4
               SNRM retry:                   6
               Poll retry:                   10
```

Link configuration	The name and status of SDLC link stations in the router's configuration.
Default Role	The link role used for link stations created with a default configuration. You can change this role using the **add remote- secondary** command.
Type	The type of link, either Multipoint or Point-to-point.
Duplex	Duplex configuration, HALF or FULL.
Modulo	The sequence number range to use on the link: MOD 8 (0-7) or MOD 128 (0 - 127).
Idle state	The bit pattern (FLAG or MARK) transmitted on the line when the interface is not transmitting data.
Encoding	Configures the SDLC transmission encoding scheme as NRZ (Non-Return to Zero) or NRZ1 (Non-Return to Zero Inverted).
Clocking	Interface clocking, either external, internal, or mixed.
Frame Size	The maximum frame size that can be sent over the interface.
Timers:	All the timers listed below have a 100ms resolution.
XID/TEST resp.	The time the router waits for an XID or TEST response message before retransmitting the XID or TEST frame. A value of 0 indicates that the router continues to retry indefinitely.
SNRM response	The maximum time the router waits for an UA response message before the station retransmits SNRM(E).
Poll response	The maximum time to wait for a response from any polled station before retrying.
Inter-poll delay	The amount of time the router (configured with a primary role) waits after receiving a response, before polling the next station.

RTS hold delay	The amount of time that the primary router waits before dropping RTS low after the transmission of a frame. This parameter is specific to half-duplex operation.
Inter-frame delay	The minimum amount of time (in 5.12 microsecond time units) that the primary router waits between transmitting frames.

Counters:

XID/TEST retry	The maximum number of times the router sends an XID or TEST frame without receiving a response before timing out. A value of 0 indicates that the router continues to retry indefinitely.
SNRM	The maximum number of times the router sends an SNRM(E) frame without receiving a response before timing out. A value of 0 indicates that the router continues to retry.
Poll retry	The maximum number of times the router polls the station without receiving a response before timing out. A value of 0 indicates that the router continues to retry indefinitely.

remote-secondary *all* or *address* or *link station name*

Displays information for the specified SDLC link station on the interface, or for all link stations.

Example: **list remote-secondary C1**

```
Address  Name  Status   Max BTU  Rx Window   Tx Window   Role
-------  ----  ------   -------  ---------   ---------   ----
  C1   SDLC_C1 Enabled   2005       7           7        SECONDARY
```

Example: **list remote-secondary all**

```
Address  Name  Status   Max BTU  Rx Window   Tx Window   Role
-------  ----  ------   -------  ---------   ---------   ----
  C1   SDLC_C1 Enabled   2005       7           7        SECONDARY
  C2   SDLC_C2 Disabled  2005       7           7        NEGOTIABLE
  C3   SDLC_C3 Enabled   2009       7           7        SECONDARY
```

Address	The address of the SDLC link station.
Name	The name of the SDLC link station.
Status	The status of the SDLC link station, ENABLED or DISABLED.
Max BTU	The frame size limit of the remote station. It must not be larger than the maximum Basic Transmission Unit (BTU) packet size configured with the **set link frame-size** command. The default is 521 bytes.
Rx Window	The size of the receive window.
Tx Window	The size of the transmit window.
Role	The role of the remote link station, either Secondary (Type 2.0) or Negotiable (Type 2.1)

Set

Use the **set** command in the SDLC configuration process to configure specific information for one or all SDLC link stations.

All time values are in seconds, with a 0.1 second resolution.

Syntax: set

link clocking

link duplex . . .

link encoding . . .

link frame-size

link idle . . .

link modulo . . .

link name

link poll . . .

link role . . .

link rts-hold
link snrm
link speed
link transmit-delay
link type . . .
link xid/test
remote-secondary . . .

Set link . . .

link clocking *internal* or *external* or *mixed*

Configures the SDLC link's clocking. To connect to a modem or DSU, configure clocking as External. To connect directly to another DTE device, use a DCE cable and set the clocking to Internal. Use Mixed if the modem provides the receive clock lines and expects the transmit clock line. For internal and mixed clocking, you must enter the **set speed** command to configure a clock speed in the range 0 to 6250000 bits per second.

Note: If your Digital Distributed Router hardware supports internal clocking and you wish to connect directly to an SDLC device without a modem pair or modem eliminator, you can use **set link clocking internal**. If you do use internal clocking, you must supply a synchronous null modem cable interface (not provided by Digital).

Example: **set link clocking internal**

link duplex *full* or *half*

Configures the SDLC line for full-duplex or half-duplex.

Example: **set link duplex full**

link encoding *nrz* or *nrzi*

Configures the SDLC transmission encoding scheme as NRZ (Non-Return to Zero) or NRZI (Non-Return to Zero Inverted). NRZ is the default.

Example: **set link encoding nrz**

link frame-size

Configures the maximum size of the frames that can be transmitted and received on the data link. The valid entries are 576 to 18000. The default is 2048.

The remote secondary max packet value cannot be greater than the value of the link frame-size. If this occurs, the router automatically resets this value equal to that set for the link, and generates an ELS message warning the user that the remote secondary max packet value was changed.

Example: **set link frame-size**

```
Frame size in bytes (576 - 18000) [2048]?
```

link idle flag

Configures the transmit idle state for SDLC framing. The default is the *flag* option which provides continuous flags (7E hex) between frames.

Example: **set link idle flag**

link idle mark

Configures the transmit idle state for SDLC framing. The mark option puts the line in a marking state (OFF, 1) between frames.

Example: **set link idle mark**

link modulo *8* or *128*

Specifies the sequence number range to use on the link: MOD 8 (0-7) or MOD 128 (0 - 127). The default is 8.

Note: When you change this value, the transmit and receive window sizes become invalid.

Use the **set remote-secondary** command to change the receive-window and transmit-window sizes. Valid window sizes for mod 8 are 0 to 7; valid window sizes for mod 128 are 8 to 127.

At connection start-up, a SNRME (rather than a SNRM) and extended SDLC frame headers are used.

Example: **set link modulo 8**

link name *name*

Establishes a name for the link that you are configuring. This parameter is for informational purposes only.

Example: **set link name**

```
Enter link name: [LINK_0]?
```

link poll delay

Configures the time delay between each poll that is sent over the interface.

Example: **set link poll delay**

```
Enter delay between polls [0.2]?
```

link poll retry

Configures the number of times the interface retries to poll the remote SDLC link station before it decides the link station is down and closes the connection.

Example: **set link poll retry**

```
Enter poll retry count (0=forever) [10]?
```

link poll timeout

Configures the amount of time the router waits for a poll response before timing out.

Example: **set link poll timeout**

```
Enter poll timeout [0.5]?
```

link role *primary* or *negotiable*

Configures the interface as an SDLC primary link station (default).

Note: The SDLC interface negotiates only to primary. It does not negotiate to secondary.

Example: **set link role primary**

link rts-hold

The time to hold RTS high after transmitting a frame. This setting is for half-duplex mode. This setting has no effect in full-duplex mode.

Example: **set link rts-hold**

```
Enter RTS hold duration after transmit complete [0.0]?
```

link snrm timeout

Configures the time to wait for a UA response before retransmitting an SNRM(E).

Example: **set link snrm timeout**

```
Enter SNRM response timeout [2.0]?
```

link snrm retry

Configures the number of times to retransmit an SNRM(E) without receiving a response before giving up.

Example: **set link snrm retry**

```
Enter SNRM retry count (0=forever)[6]?
```

link speed

For internal clocking, this command specifies the speed of the transmit and receive clock lines. For mixed clocking, the speed applies to the transmit clock line only.

Example: **set link speed**

```
Internal Clock Speed [0]?
```

link transmit-delay

Allows the insertion of a delay between transmitted packets. This command ensures a minimum delay between frames so that it is compatible with older, slower serial devices at the other end. This value is passed in 5.12 microsecond units.

Example: **set link transmit-delay 6**

link type *multipoint* or *point-to-point*

Configures the SDLC link to either a multipoint link or a point-to-point link.

Example: **set link type multipoint**

link xid/test timeout

Configures the maximum amount of time to wait for an XID or TEST frame response.

Example: **set link xid timeout 10**

link xid/test retry

Configures the maximum number of times an XID or TEST frame is resent before giving up.

Example: **set link xid retry 5**

Set remote-secondary . . .

remote-secondary *address* or *name* address

Changes the remote station's SDLC address in the range 01 to FE.

Example: **set remote-secondary C1 address CE**

remote-secondary *address* or *link station name* role *secondary* or *negotiable*

Changes the remote station's link role:

Secondary	The designated remote link station functions as a secondary (i.e., Type 2.0) node.
Negotiable	The designated link station functions as a negotiable (i.e., Type 2.1) node.

Example: **set remote-secondary c1 role neg**

remote-secondary *address* or *name* max-packet

The maximum size of the packet that a remote-secondary station can receive. The default size is 521 bytes.

Note that you cannot set the maximum packet size *larger* than the link frame size configured with the **set link frame-size** command. If you do this, the router automatically resets the max packet size to the link frame size, and issues the following message:

```
SDLC.054: nt 3 SDLC/0 Stn C4 - MaxBTU too large for Link adjusted (4096->2048)
```

Example: **set remote-secondary c1 max-packet 521**

remote-secondary *address* or *name* name

The name of the SDLC station.

Example: **set remote-secondary c1 name Brad**

remote-secondary *address* or *name* receive-window

The maximum number of frames the router can receive before sending a response.

Example:
set remote-secondary c1 receive-window 4

remote-secondary *address* or *name* transmit-window

The maximum number of frames the router can transmit before receiving a response frame.

Example:
set remote-secondary c1 transmit-window 6

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: **exit**

5

Monitoring SDLC Interfaces

This chapter describes the SDLC monitoring commands.

About SDLC Monitoring Commands

SDLC monitoring commands entered within the SDLC monitoring module take effect immediately. However, changes made with monitoring commands do *not* become part of the router's non-volatile configuration.

When the router restarts, the configuration stored in non-volatile configuration memory supersedes the effects of monitoring commands.

Monitoring consists of these actions:

- Monitoring the protocols, and network interfaces currently in use by the router.
- Making real-time changes to the SDLC configuration without permanently affecting the router's non-volatile configuration memory.
- Displaying ELS (Event Logging System) messages relating to router activities and performance.

Accessing the SDLC Monitoring Environment

To enter the SDLC monitoring process, follow these steps.

1. At the MOS prompt (*), enter **talk 5** or just **t 5**. This brings you to the monitoring environment, designated by the + prompt.

```
t 5

CGW Operator Console
+
```

2. At the + prompt, enter the **network** command, and the number that identifies the interface associated with a previously configured SDLC device.

```
+ net 3
SDLC Console
SDLC-3>
```

Displaying Statistics on SDLC Interfaces

You can use the **interface** command to display physical line status attributes for SDLC device interfaces without entering the SDLC monitoring module. To do this, enter the interface command and an interface number at the + prompt, as shown:

Example: + **interface 3**

```
                                Self-Test  Self-Test      Maintenance
Nt  Nt'  Interface      CSR       Passed     Failed           Failed
3   1    SDLC/1    80000000            1          0                0


SDLC MAC/data-link on SCC Serial Line interface.

Level converter:  RS-232/V.35   Adapter cable:  RS-232 DCE

V.24 circuit:  105      106      107   108   109
Nicknames:     RTS      CTS      DSR   DTR   DCD
RS-232 DCE:    CA       CB       CC    CD    CF
State:         OFF      OFF      OFF   OFF   OFF

Line speed (configured):  9.615 Kbps
Last port reset:   1 minute, 24 seconds ago

Input frame errors:
    CRC error                0        alignment (byte length)    0
    Too short (< 2 bytes)    0        Too long (> 2051 bytes)    0
    aborted frame            0        DMA/FIFO overrun           0

Output frame errors:
    DMA/FIFO Underrun errors 0        Outputs aborts sent        0
```

Note: If a cable is not connected, then cable and signal information is not displayed.

Nt	Interface number assigned by software during initial configuration.
Nt'	Interface number assigned by software during initial configuration.
CSR	Memory location of the control status register for the SDLC interface.
Self-test passed	Number of times the SDLC interface passed its self-test.
Self-test failed	Number of times the SDLC interface was unable to pass its self-test.
Maintenance failed	Number of maintenance failures.

The following six parameters only appear if a cable is connected, and varies according to cable type.

Level converter	Type of level converter connected to the SDLC interface.
Adapter cable	Type of adapter cable that the level converter is using.
V.24 circuit	Circuits in use on the V.24 circuit.
Nicknames	Signals in use on the V.24 circuit.
RS-232 DCE	Current level converter is RS-232 DCE.
State	State of V24 circuits, signals, and pin assignments (ON or OFF).
Line speed (configured)	Currently configured line speed for the SDLC interface.
Last port reset	How long ago the port was last reset.
Input frame errors	Input frame error type (CRC error, too short, aborted, alignment, too long, DMA/FIFO overrun) and the total number of errors that have occurred.
Output frame counters	Total number of DMA/FIFO overruns and output aborts sent for output frames.

SDLC Commands

This section describes SDLC monitoring commands.

When you enter commands, the router interface often prompts you for values and parameters. In cases where a default answer exists, you can accept it by pressing RET. Default answers are enclosed in brackets immediately following the command prompt.

Table 5–1 lists SDLC monitoring commands and their functions.

Note: Digital routers support SDLC connections over RS-232, X.21 and V.35 serial interfaces.

Table 5–1 SDLC Command Summary

Command	Function
?(Help)	Lists the configuration and monitoring commands or lists any parameters associated with that command.
Add	Adds an SDLC remote-secondary link station.
Clear	Clears link or remote-secondary counters.
Disable	Prevents connections to an SDLC link station.
Enable	Allows connections to an SDLC link station.
List	Displays configured information for an SDLC link station.
Set	Configures specific interface and remote- secondary information.
Test	Performs an echo test on a remote-secondary station.
Exit	Exits the SDLC configuration or monitoring environment.

? (Help)

Use the **? (help)** command to list the available commands that are available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: ?

Example: **?**

```
Set
Add
Disable
Delete
Enable
List
Exit
```

Add

Use the **add** command to add a remote-secondary end station. You may elect not to use this command. By default, the router adds a remote-secondary end station to ensure proper operation of the SDLC interface. However, you must use this command if you wish to mix T2.0 and T2.1 link stations on the same multipoint line, or if you wish to override any other default station characteristics. The router is considered the primary end station by default.

Syntax: add remote-secondary

Example: **add remote-secondary**

```
Enter station address (in hex) [C3]?
Enter remote station name [SDLC_C3]?
Enter max packet size [2009]?
Enter receive window [7]?
Enter transmit window [7]?
Enable negotiable mode [Yes or (No)]?
```

Enter station address	The remote station's SDLC address in the range 01 - FE.
Enter remote station name	The name designation of the SDLC station (maximum characters is 8).
Enter max packet size	The maximum packet size that can be sent to or received from the remote link station. This value cannot be greater than that specified for the link with the **set link frame-size** command.

Enter receive window	The maximum number of packets that the router can receive without sending a response.
Enter transmit window	The maximum number of packets that the router can transmit without receiving a response.
Enter negotiable mode	Indicates whether the remote-secondary end station you are adding is a negotiable (T2.1) or secondary (T2.0) node on the multipoint line.

Clear

Use the **clear** command to clear counters for the remote-secondary end station. Use the SDLC **list remote all** command to list existing sessions.

Syntax: clear

link
remote-secondary . . .

link *name* or *address*

Clears the counters for an SDLC interface.

Example: **clear link**

remote-secondary *name* or *address* or *all*

Clears counters for either a specific, or all, remote-secondary end stations.

Example: **clear remote-secondary c1**

Delete

Use the **delete** command to remove the specified remote-secondary end station (remote station name or address) from the SDLC configuration. The router is considered the primary end station (default).

When used in the monitoring environment, this command terminates any SDLC session in progress.

Syntax: delete remote-secondary *name* or *address*

Example: **delete remote-secondary C1**

Disable

Use the **disable** command to prevent connections from being created with a SDLC link station.

Syntax: disable
link
remote-secondary . . .

link

Prevents the establishment of SDLC sessions on any SDLC link stations on the interface.

When used in the monitoring environment, the **disable** command also terminates all existing connection on the link.

Example: **disable link**

remote-secondary *name* or *address*

Prevents establishment of an SDLC session to the specified remote-secondary end station (remote station name or address).

When used in the monitoring environment, the **disable remote-secondary** command also terminates any existing SDLC session.

Example: **disable remote-secondary c1**

Enable

Use the **enable** command to enable connections to remote SDLC link stations.

Syntax: enable
link
remote-secondary . . .

link

Allows subsystems in the router (e.g. DLSw) to use SDLC's facilities.

Example: **enable link**

remote-secondary *name* or *address*

Allows connections to the specified remote-secondary end station (link station name).

Example: **enable remote-secondary C1**

List

Use the **list** command in the monitoring module to display statistics specific to the data link layer and the interface.

Syntax: list

link configuration

link counters

remote-secondary . . .

link configuration

Displays information for the SDLC interface. Displayed output is identical to that generated with the **list link** command in the configuration environment.

link counters

Displays information for the SDLC counters since the last router restart or the last clear counters.

Example: **list link counters**

```
         I-Frames   I-Bytes     Re-Xmit    UI-Frames      UI-Bytes
        _________  _________  _________  __________  ____________
Send           0          0          0           0             0
Recv           0          0                      0             0

           RR         RNR        REJ
        _________  _________  _________
Send           0          0          0
Recv           0          0          0
```

I-Frames Total number of information frames received and sent.

I-Bytes Total number of information bytes received and sent.

Re-Xmit	Total number of retransmitted frames.
UI-Frames	Total number of Unnumbered Information frames received and transmitted.
UI-Bytes	Total number of Unnumbered Information bytes received and transmitted.
RR	Total number RRs (Receive Ready) received and transmitted.
RNR	Total number RNRs (Receive Not Ready) received and transmitted.
REJ	Total number of Rejects received and transmitted.

remote-secondary *all* or *address* or *link station name*

Displays status for the specified SDLC link station (link station name) on the interface.

Example: **list remote-secondary all**

```
Address  Name    Status     Max BTU  Rx Window Tx Window
  A0    SDLC_A0  Discnected 2009        7          7
  C1    SDLC_C1  Idle       2005        7          7
  C2    SDLC_C2  Disabled   2005        7          7
  C3    SDLC_C3  Enabled    2009        7          7
```

Example: **list remote-secondary C2**

```
Address  Name    Status   Max BTU   Rx Window  Tx Window
  C2    SDLC_C2  Disabled 2005         7          7
```

Address	The address of the SDLC link station.
Name	The character string name designation of SDLC link station.

Status — The status of the SDLC link station:

Enabled	Enabled, but not allocated.
Idle	Allocated, but not used yet
Connected	Connected
Disconnected	Disconnected
Connecting	Connection establishment in progress.
Discnectng	Disconnection in progress
Recovering	Attempting to recover from a temporary data link error.

Max BTU — The frame size limit of the remote station. This frame size must not be larger than the maximum basic transmission unit (BTU) packet size configured with the **set link frame-size** command. The default is 521 bytes.

Rx Window — The size of the receive window.

Tx Window — The size of the transmit window.

remote-secondary *name* or *address* counters

Displays frame transmit and receive counts for the specified remote secondary station.

Example: **list remote c1 counters**

```
Counters for: SDLC_C1 , address C1 (ENABLED)

      I-Frames      I-Bytes    Re-Xmit   UI-Frames   UI-Bytes  XID-Frames
      --------      -------   --------   ---------    --------  ----------
Send       569      88870             0            0        0           0
Recv       345       4804             0            0        0           0

            RR          RNR         REJ         TEST        SNRM        DISC
      --------      -------   --------   ---------    --------  ----------
Send      4779          0             0            1        1           0
Recv      4443          0             0            1        0           0

            UA          DM        FRMR
      --------      -------   --------
Send         0          0             0
Recv         1          0             0
```

```
            RR          RNR         REJ         TEST        SNRM         DISC
       --------      -------   --------   ---------     --------  ----------
Send       4779          0             0             1         1           0
Recv       4443          0             0             1         0           0

            UA          DM        FRMR
       --------      -------   --------
Send          0           0           0
Recv          1           0           0
```

I-Frames	The total number of Information frames received and sent.
I-Bytes	The total number of Information bytes received and sent.
Re-Xmit	The total number of frames retransmitted.
UI-Frames	The total number of Unnumbered Information frames received and transmitted.
UI-Bytes	The total number of Unnumbered Information bytes received and transmitted.
XID-Frames	The total number of Exchange Identification frames received and transmitted.
RR	The total number of Receive Ready frames received and transmitted.
RNR	The total number of Receive Not Ready frames received and transmitted.
REJ	The total number of Rejects received and transmitted.
TEST	The total number of Test frames received and transmitted.
SNRM	The total number of Set Normal Response Mode frames received and transmitted.
DISC	The total number of Disconnect frames received and transmitted.
UA	The total number of Unnumbered Acknowledgment frames received and transmitted.

DM	The total number of Disconnected Mode frames received and transmitted.
FRMR	The total number of Frame Reject frames received and transmitted.

Set

When used in the SDLC monitoring environment, the **set** command enables you to dynamically configure specific information for one or all SDLC link stations without affecting the router's non-volatile configuration memory.

You can only issue the **set** command on disabled stations. You can only issue the **set link** command on a disabled link. All time values are in seconds, with a 0.1 second resolution.

Syntax: set

link modulo . . .
link name
link poll . . .
link role . . .
link rts-hold
link snrm
link type . . .
link xid/test
remote-secondary . . .

link modulo

Dynamically changes the range of sequence numbers to be used on the data link without affecting the SRAM configuration. Modulo 8 specifies a sequence number range of 0 - 7, and modulo 128 specifies 0 - 127. Default is 8.

Example: **set link modulo 8**

Note: When you change this value, the transmit and receive window sizes become invalid.

Use the **set remote-secondary** command to change the receive-window and transmit-window sizes. Valid window sizes for mod 8 are 0 to 7; valid window sizes for mod 128 are 8 to 127.

link name

Dynamically changes the name of the link without affecting the SRAM configuration. A maximum of 8 characters may be entered. This parameter is for informational purposes only.

Example: **set link name**

```
Enter link name: [LINK_0]?
```

link poll delay

Dynamically changes the time delay between polls sent over the interface.

Example: **set link poll delay**

```
Enter delay between polls [0.2]?
```

link poll timeout

Dynamically changes the amount of time the router waits for a poll response before timing out.

Example: **set link poll timeout**

```
Enter poll timeout [0.5]?
```

link poll retry

Dynamically configures the number of times the interface retries to poll the remote SDLC link station before deciding the link station is down and closing the connection.

Example: **set link poll retry**

```
Enter poll retry count (0=forever) [10]?
```

link role *primary* or *negotiable*

Dynamically configures the interface as an SDLC primary link station (default) or the role of the interface without affecting the router's non-volatile configuration memory.

Note: The SDLC interface negotiates only to primary. It does not negotiate to secondary.

Example: **set link role primary**

link rts-hold

Dynamically changes the time to hold RTS high after transmitting a frame without affecting the router's non-volatile configuration memory. This setting is for half-duplex mode. It has no effect in full-duplex mode.

Example: **set link rts-hold**

```
Enter RTS hold duration after transmit complete [0.0]?
```

link snrm *timeout*

Dynamically changes the time to wait for a Unnumbered Acknowledgements (UA) response before retransmitting an SNRM.

Example: **set link snrm timeout**

```
Enter SNRM response timeout [2.0]?
```

link snrm retry

Dynamically changes the number of times to retransmit an SNRM(E) without receiving a response before giving up.

Example: **set link snrm retry**

```
Enter SNRM retry count (0=forever)[6]?
```

link type *multipoint* or *point-to-point*

Dynamically changes the SDLC link to either a multipoint link or a point-to-point link without affecting the router's non-volatile configuration memory.

Example: **set link type multipoint**

link xid/test timeout

Dynamically changes the maximum amount of time to wait for an XID or TEST frame response.

Example: **set link xid/test timeout 10**

link xid/test retry

Dynamically changes the maximum number of times an XID or TEST frame is resent before giving up.

Example: **set link xid/test retry**

remote-secondary *name* or *address* address

The remote station's SDLC address within a range of 01 to FE.

Example: **set remote-secondary address CE**

remote-secondary *name* or *address* max-packet

The maximum size of the packet that a remote-secondary station can receive. The default size is 521 bytes.

Note that you cannot set the maximum packet size larger than the link frame size configured with the **set link frame-size** command. If you do this, the the router automatically resets the max packet size to the link frame size.

Example: **set remote-secondary max-packet 521**

remote-secondary *name* or *address* name

The name designation of the SDLC station. A maximum of 8 characters may be entered.

Example: **set remote-secondary c1 name Brad**

remote-secondary *name* or *address* receive-window

The maximum number of frames that can be received by the router before sending a response.

Example:
set remote-secondary C1 receive-window 4

remote-secondary *name* or *address* transmit-window

The maximum number of frames that the router can transmit before receiving a response frame.

Example:
set remote-secondary c1 transmit-window 6

Test

Transmits a specified number of TEST frames to the specified remote-secondary link station and waits for a response. Use this command to test the integrity of the connection.

Note: Disable the specified link station before using this command.

Syntax: test remote *name or address #frames frame-size*

Example: **test remote c1**

```
Number of frames to send [1]? 5
Frame length [265]?
Starting echo test -- press any key to abort
5 frames sent, 5 frames received, 0 compare errors, 0 timeouts
```

Number of frames	Total number of frames to send.
Frame length	Length of the frame sent. This frame cannot be any larger than the maximum frame length of the remote-secondary station.

Cancel the test by pressing any key.

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: **exit**

6

Using Boundary Access Node

This chapter describes Digital's implementation of Boundary Access Node (BAN). Developed in close collaboration with IBM, BAN provides a reliable, low-cost way for attached PU Type 2.0 and 2.1 end stations to communicate with the SNA environment across wide area links.

The following sections explain how to configure your router for BAN.

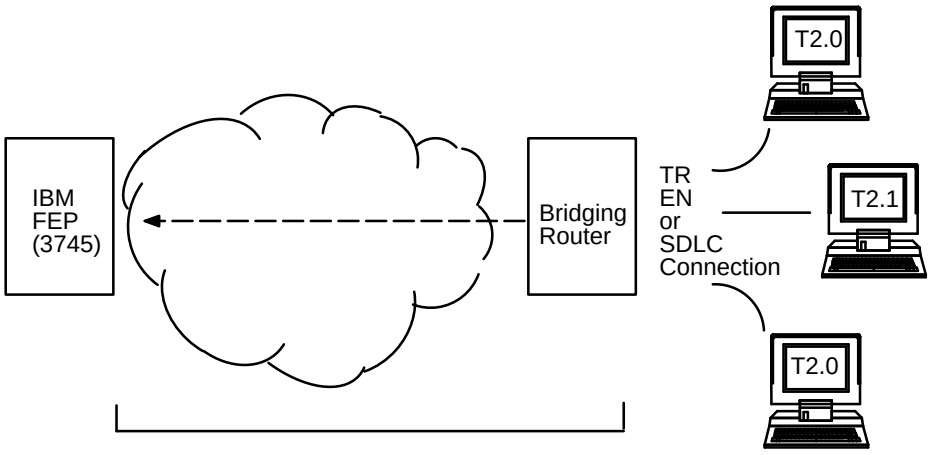
About Boundary Access Node

Boundary Access Node (BAN) is an enhancement of the Frame Relay (FR), DLSw and Adaptive Source Route Bridging (ASRT) capabilities of Digital router software.

BAN is designed to meet the business goals of customers who do not yet need a full DLSw implementation. It provides a low-cost method for connecting to IBM environments, enabling SNA end stations to bridge Ethernet, FDDI or Token Ring traffic directly to the FEP without frame conversion by another DLSw router. This saves significantly on capital equipment costs, since it removes the need for another router, a Token Ring, and TIC-3745 interface card attached to the remote SNA device.

BAN accomplishes this by enabling IBM type 2.0 and 2.1 end nodes connected to a Digital router to make a direct connection via Frame Relay with the front end processor (FEP) attached to an IBM mainframe.

Figure 6–1 Direct Connection of End Nodes to IBM FEP Using BAN



Though traffic passes through them, the bridging router and FR network are transparent to end nodes when using BAN.

How BAN Works

BAN works by filtering the frames sent by Type 2.0 or 2.1 end stations. The router modifies each BAN frame to comply with Bridged 802.5 (Token Ring) Frame format. The router subsequently examines each frame and allows only those *with the BAN DLCI MAC address* to pass over a DLCI (Data Link Connection Identifier) to the FEP.

Note: To support BAN, an IBM FEP must be running the Network Control Program (NCP) software 7.3 or greater, or NCP software 7.1 or 7.2 with an APAR applied. If you have questions about whether your FEP can support BAN, contact your IBM representative.

With BAN, one DLCI is ordinarily all that is needed. However BAN may use many DLCI connections between the router and the IBM environment. In some cases, you may want to set up more than one DLCI to handle BAN traffic. See "Setting up Multiple DLCIs" in this chapter for more information.

There are two ways to use BAN: straight bridging, using the router's bridging capability, and DLSw terminated. In most cases, choose the bridging option. However, you may consider choosing the terminated option if you want to reduce session timeouts on the DLCI. The sections that follow explain how to set up each option.

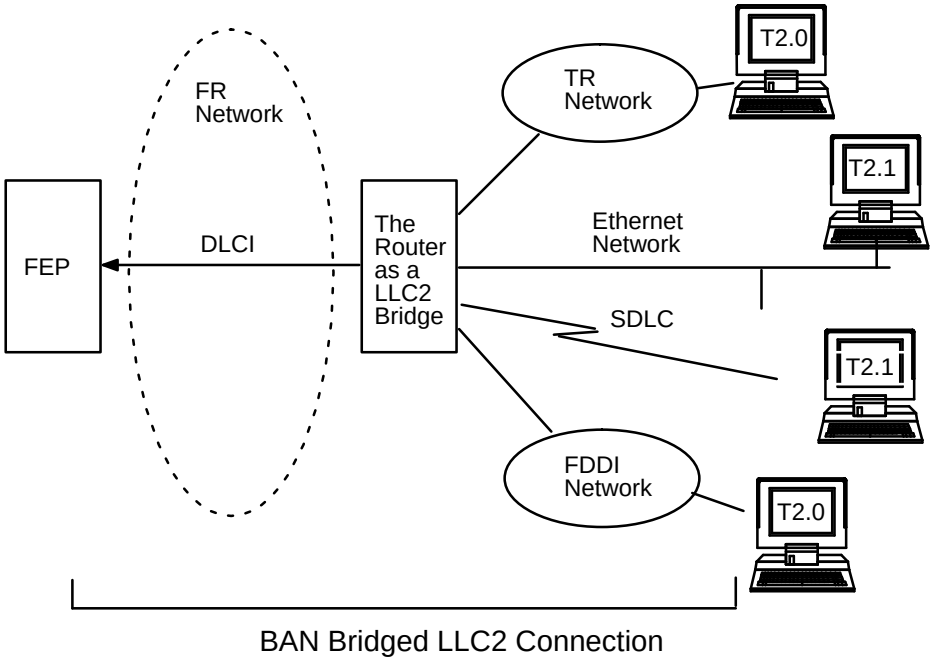
Bridged and DLSw-terminated BAN

Digital enables you to implement BAN in two ways. With the straight bridging method, you configure BAN to bridge LLC2 frames from Type 2.0 or Type 2.1 end stations straight into the NCP. With the DLSw Terminated method, BAN terminates the LLC2 connection at the DLSw router.

Within this discussion, we refer to these two methods as BAN Type 1 and BAN Type 2, respectively.

Figure 6–2 shows a BAN Type 1 (bridged) connection. In this illustration, notice that the router does not terminate the LLC2 traffic received from attached end nodes. Instead, the router converts the BAN DLCI-addressed frames it receives to bridged Token-ring format (RFC1490 802.5 header) frames, and bridges them directly to the NCP.

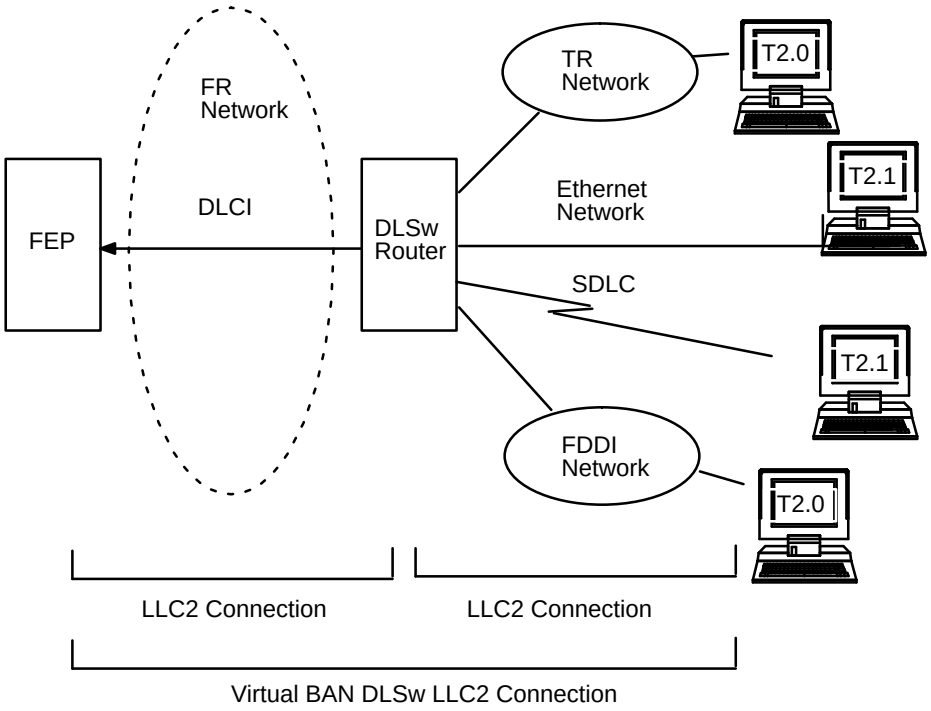
Figure 6–2 BAN Type 1: The Router as an LLC-2 Bridge



In this case, the router acts as a bridge between the FEP and end stations. DLSw does not terminate LLC2 session at the router, as in BAN Type 2. End station frames can be Token Ring, SDLC, Ethernet, or FDDI format, provided the bridge is configured to support that type of frame.

Figure 6–3 shows a BAN Type 2 (Virtual BAN DLSw) connection. In this illustration, notice that the DLSw router does not function as a bridge. The router terminates the LLC2 traffic received from attached end nodes. At the same time, the router establishes a new LLC2 connection to the NCP over the Frame Relay network. Thus, though two LLC2 connections exist within the transaction, the break between them is transparent both to the NCP and the end nodes. The result is a virtual LLC2 connection between NCP and end nodes.

Figure 6–3 BAN Type 2: Local DLSw Conversion



Which Method Do You Use?

Straight bridging of frames (BAN Type 1) is generally preferable. This method provides fast delivery of data with minimal network overhead. However there are exceptions to this rule. If usage on a DLCI is too high, session timeouts may occur in a bridged configuration.

Conversely, session timeouts rarely occur in a DLSw-terminated configuration (BAN Type 2) since this type of configuration terminates and then recreates LLC2 sessions at the local (DLSw) router. For this reason, you may may want to use DLSw-terminated BAN in situations when reducing the possibility of session timeouts is an overriding concern. When running in DLSw-terminated mode, the router terminates *all* traffic on the DLCI. This mode also limits the number of remote end stations the BAN configuration can support.

Using BAN

When you are configuring BAN, the system prompts you to enter information. Often, the system provides default responses, which you can accept by pressing RET.

To use configure BAN, follow these steps:

1. Configure the router for Frame Relay (FR)
2. Configure the router for Adaptive Source Route Bridging (ASRT)
3. Configure the Router for BAN
4. Open Service Access Points (SAPs) on the FR and LAN Interfaces

These steps are documented in the example that follows.

This example assumes that you are setting up a single DLCI to carry BAN traffic. Depending on your circumstances and needs, you may want to set up multiple DLCIs for the sake of redundancy, or to increase total bandwidth to the IBM environment. See "Setting up Multiple DLCIs" for more information.

Configuring Frame Relay

To access the Frame Relay user configuration area, use the **network** command at the `Config>` prompt as shown:

```
Config>net 2
Frame Relay user configuration
FR Config>
```

At the `FR Config>` prompt, add a permanent circuit as shown. The router prompts you for a circuit number. This is the DLCI number. The router then prompts you for a committed information rate, and for a circuit name.

The circuit name is *extremely important*. It tells the bridge which DLCI to use for BAN frames. In doing so, it provides the linkage between the router (which is acting as a bridge in this case) and the FR protocol.

```
FR Config>add permanent
Circuit number  [16]? 20
Committed Information Rate in bps  [64000]?
Assign circuit name []? 20-ncp10
FR Config>
```

Assign a circuit name that identifies the IBM NCP in some obvious way (as in this example, where the assigned circuit name is `20-ncp10`). Also use a name that has 8 characters or fewer. Choosing a short name may prevent it from being truncated on some bridge configuration screens.

The DLCI you create by assigning a circuit number and name becomes the PVC that connects Digital's bridging router with the IBM FEP when using BAN. The next step consists of configuring this PVC as a bridge port.

Note: If you want to set up multiple BAN DLCIs connected to the same or different FEPs, you have to configure Frame Relay separately for each DLCI.

Configuring the Router for Adaptive Source Route Bridging

Next, you must configure the PVC as a bridge port. To do this, use the **network** command at the `Config>` prompt as shown:

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>
```

At the `ASRT Config>` prompt, add a port as shown. The router prompts you for an interface number. The number you assign is the FR interface number on the bridge. The router then prompts you for a port number, and for a circuit name. The circuit name you assign must be the same as that used when configuring the router for bridging over FR in Step 1.

```
ASRT config>add port
Interface Number [0]? 2
Port Number [5]?
Assign circuit name []? 20-ncp10
ASRT config>
```

The next step consists of enabling source routing and defining source routing segment numbers for the FR port.

```
ASRT config>enable source routing
Port Number [3]? 5
Segment Number for the port in hex(1 - FFF) [1]? 456
Bridge Virtual Segment Number in hex(1 - FFF) [1]? 789
ASRT config>
```

Then, disable transparent bridging on the bridge port as shown:

```
ASRT config>disable transparent bridging
Port Number [3]? 5
ASRT config>
```

The final step consists of configuring the router for BAN.

Configuring the Router for BAN

You configure the router for BAN from the `ASRT config>` prompt. The addition of a BAN port is not verified until you restart the router. Note that, as in steps 1 and 2, bridge port 5 is the port used throughout this step.

```
Config> Protocol ASRT
ASRT config>ban
BAN (Boundary Access Node) configuration
BAN config>
```

At the `BAN config>` prompt, add the port number (5) on which you want to enable BAN. The router prompts you to enter a BAN DLCI MAC address, and the Boundary Node Identifier address as shown:

```
BAN config>add 5
Enter the BAN DLCI MAC Address []? 400000000001
Enter the Boundary Node Identifier MAC Address [4FFF00000000]?
```

In this example, 400000000001 is the MAC address of the DLCI: this is the address to which attached end stations send data. The other address, 4FFF00000000, is the default Boundary Node Identifier Address. To accept it, press RET.

Note: Always choose the default Boundary Node Identifier address unless the Boundary Node Identifier address of the receiving FEP was changed. This is because the Boundary Node Identifier address *must match* the corresponding value in the NCP definition. This value is specified by the LOCADD keyword of the LINE statement that defines the physical Frame Relay connection.

Specifying the Type of BAN Connection You Need

The next prompt asks you to specify which type of BAN connection you want to add, bridged (described earlier as BAN Type 1) or DLSw-terminated (Type 2). Type 1, straight bridging, is the default. Accept the default unless you want inbound traffic to be terminated at the router.

After you enter **b** (bridged) or **t** (terminated), the router informs you that the BAN port was added. The default choice is **b** .

```
Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) [b]?

BAN port record added.
```

Opening Service Access Points (SAPs)

To use BAN, you must open the Service Access Points (SAPs) associated with the FR interface, and the LAN interface. If you fail to open these SAPs, you cannot use BAN. Failure to open all SAPs is often the cause of configuration problems.

You open the SAPs from the `DLSw config>` prompt as follows:

```
DLSw config>open
Interface # [0]?
Enter SAP in hex (range 0-ff) [0]? 4
DLSw config>
```

Issuing the open command for interface 0 opens the SAP on the LAN interface. You issue the same command to open the SAP on the FR interface. Note that in each case, you enter **4** to open a SAP.

```
DLSw config>open
Interface # [2]?
Enter SAP in hex (range 0-ff) [0]? 4
DLSw config>
```

Note: The above examples use interface numbers 0 and 2 for the LAN and FR interfaces. These are acceptable defaults, but you can obtain better results using the interface numbers that correspond to your particular platform.

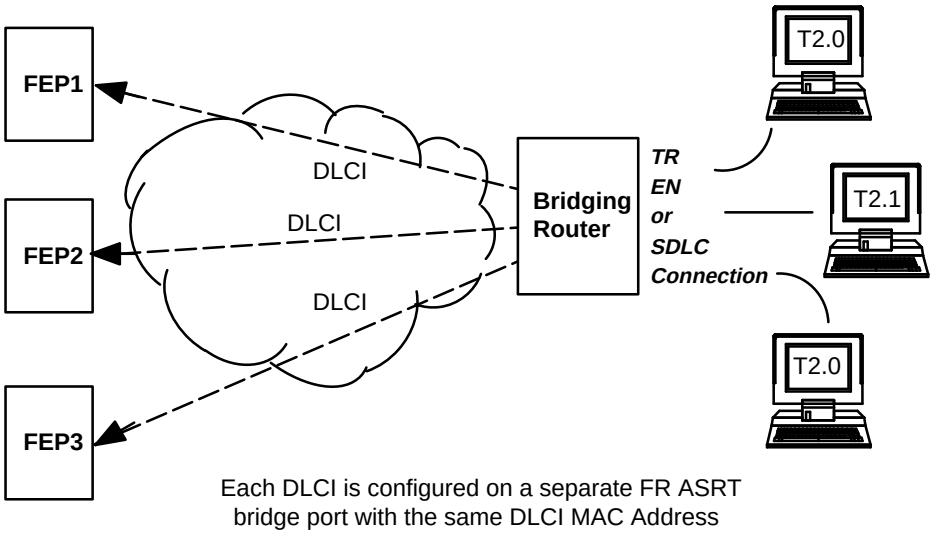
Using Multiple DLCIs for BAN Traffic

You can set up redundant DLCIs to overcome traffic overloading. While one DLCI is usually sufficient to handle BAN traffic to and from the IBM environment, setting up two or more DLCIs may prove useful in some circumstances. The following sections discuss the benefits of redundant DLCIs and how you set them up.

Benefits of Setting Up a Fault-tolerant BAN Connection

Redundant connections to multiple NCPs protect against a single NCP failure. In addition, sharing BAN traffic among several DLCIs reduces the chance of one NCP becoming overloaded. In a redundant DLCI configuration, PU Type 2.0 and 2.1 end stations can pass BAN traffic to different NCPs, as shown in Figure 6–4.

Figure 6–4 BAN Configuration with Multiple DLCIs to Different FEPs



Each DLCI is configured on a separate FR ASRT bridge port with the same DLCI MAC Address

Setting Up Multiple DLCIs

Setting up multiple DLCIs is a simple matter, particularly if you elect to do this during the initial BAN configuration.

In setting up multiple connections, keep in mind that each Frame Relay DLCI corresponds with a specific FEP in the IBM environment. To pass BAN frames to that FEP, you must specify the correct circuit number when establishing the Frame Relay connection. Your Frame Relay provider can tell you the circuit number for each of your connections.

To set up DLCI connections to different FEPs (Figure 6–4) you must:

1. Within the Frame Relay configuration:

   Define another Frame Relay DLCI on a second bridge port.

2. Within the ASRT configuration:

   Add a bridge port for that DLCI.

3. Configure the bridge port for BAN, as shown earlier in this chapter.

Checking the BAN Configuration

When you restart the router, the BAN bridge appears as a FR bridge port with source-routing behavior. Check the BAN configuration with the **list** command as shown here:

```
BAN config>list

bridge  BAN                Boundary              bridged or
port    DLCI MAC Address   Node Identifier       DLSw terminated
5       40:00:00:00:00:01  4F:FF:00:00:00:00     bridged
```

As this example shows, the list command displays each aspect of the BAN configuration, giving the bridge port (5, in this case) the MAC addresses of the router and the NCP, and whether the port is bridged or DLSw terminated.

To check to see that BAN has initialized properly on startup, you can use the router's monitoring environment (at **t 5**) as follows:

```
+p asrt
ASRT>ban
BAN (Boundary Access Node) console
BAN>list

bridge  BAN                Boundary           bridged or
port    DLCI MAC Address   Node Identifier    DLSw terminated  Status
5       40:00:00:00:00:01  4F:FF:00:00:00:00  bridged          Init Fail
```

BAN has three associated status messages:

- `Init Fail` indicates that a configuration problem exists.
- `Up` indicates that the FR DLCI is up and running.
- `Down` indicates that the DLCI is not running.

If you receive a status other than `Up`, check the router's ELS messages to diagnose the problem. The following section explains how to enable ELS messages.

Enabling BAN Event Logging System Messages

After initial BAN configuration and restart, it is a good idea to enable ELS messages to see whether the configuration is working as planned. You can enable BAN-specific messages from the `Config>` prompt as shown:

```
Config>event
Event Logging System user configuration
ELS config>display subsystem ban all
ELS config>
```

Note: You must restart the router after enabling ELS messages as shown above before the action takes effect. Alternatively, you can enable ELS messages from the GWCONS prompt for immediate action.

Entering this command displays all BAN subsystem messages. This causes ELS to notify you of all BAN-related behavior. After running BAN for a while, you may want to turn off some messages.

You can switch off specific ELS BAN messages using the **nodisplay** command and the specific message number. This example illustrates how to turn off the `ban.9` message.

```
ELS config>nodisplay event ban.9
```

For a list and explanation of all BAN-related messages, see the *Event Logging System Messages Guide*.

7

Configuring Boundary Access Node

BAN Configuration Commands

This chapter includes all of the Boundary Access Node configuration commands.

Accessing the BAN Configuration Environment

Use the router's configuration process to change the configuration of the router. The new configuration takes effect when the router is restarted.

To enter the configuration environment, type **talk 6**, or just **t 6**, at the + prompt. This brings you to the `Config>` prompt as shown:

```
MOS Operator Control

* talk 6
Gateway user configuration
```

If the `Config>` prompt does not appear immediately, press RET again.

Enter all BAN configuration commands at the `BAN config>` prompt. You can access this prompt by entering the **ban** command at either the `DLSw config>` or `ASRT config>` prompt as shown:

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>ban
BAN config>
```

BAN Command Summary

Enter BAN configuration commands at the `BAN config>` prompt. Table 7–1 lists the DLSw configuration and monitoring commands.

Table 7–1 BAN Command Summary

Command	Function
? (Help)	Lists available BAN commands or associated parameters.
Add	Add a BAN port
Delete	Deletes a BAN port.
List	Displays the existing BAN configuration, and informs you whether the port has initialized properly.
Exit	Exits the BAN configuration process and returns you to the `DLSw config> or ASRT config>` process.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter **?** after a specific command name to list its options.

Syntax: ?

Example: **?**

```
ADD
DELETE
LIST
EXIT
```

Add

Use the **add** command to add a BAN port.

Syntax: add *port #*

Example: **add 2**

```
Enter the BAN DLCI MAC Address []? 400000000001
Enter the Boundary Node Identifier MAC Address [4FFF00000000] ?

Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) [b]?

BAN port record added.
```

Delete

Use the **delete** command to delete a previously added BAN port from the configuration.

Syntax: delete *port#*

Example: **delete 2**

List

Use the **list** command to display information on the existing BAN configuration, or to assess whether the DLCI is functioning properly.

When issued in the BAN configuration module, the **list** command provides general information on the BAN configuration.

Syntax: list

Example: **list**

```
bridge  BAN                Boundary              bridged or
port    DLCI MAC Address   Node Identifier       DLSw terminated
5       40:00:00:00:00:01  4F:FF:00:00:00:00     bridged
```

To check to see that BAN has initialized properly on startup, you can use the router's monitoring environment (at **t 5**) as follows:

```
+p asrt
ASRT>ban
BAN (Boundary Access Node) console
BAN>list

bridge  BAN                Boundary           bridged or
port    DLCI MAC Address   Node Identifier    DLSw terminated  Status
5       40:00:00:00:00:01  4F:FF:00:00:00:00  bridged          Init Fail
```

Exit

Use the **exit** command to exit the BAN configuration. When you exit from the configuration, you return to the DLSw config> or ASRT config> prompt.

Syntax: exit

Example: **exit**

8

Monitoring Boundary Access Node

BAN Monitoring Commands

This chapter explains all the BAN monitoring commands.

Accessing the BAN Monitoring Environment

To enter the GWCON process, enter **talk 5**, or just **t 5**, at the * prompt. This brings you to the GWCON prompt (+) as shown:

```
MOS Operator Control

* talk 5
+
```

Enter BAN monitoring commands at the BAN> prompt. To access this prompt, enter the **ban** command at the DLSW> or ASRT> prompt as shown:

```
+ protocol dls
DLSW>ban
BAN>
```

BAN Command Summary

Enter BAN monitoring commands at the BAN> prompt. Table 8–1 lists the DLSw monitoring commands.

Table 8–1 BAN Command Summary

Command	Function
? (Help)	Lists available BAN commands or associated parameters.
List	Displays the existing BAN configuration, and informs you whether the port has initialized properly.
Exit	Exits the BAN configuration process and returns you to the `DLSw config> or ASRT config>` process.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter **?** after a specific command name to list its options.

Syntax: ?

Example: **?**

```
LIST
EXIT
```

List

Use the **list** command to display information on the existing BAN configuration, or to assess whether the DLCI is functioning properly.

When issued in the BAN monitoring module, the **list** command provides general information on the BAN configuration. The command also informs you whether each BAN port has initialized properly. For detailed information on the BAN port status values and their meanings, refer to Chapter 6.

Syntax: list

Example: **list**

```
bridge  BAN                Boundary           bridged or
port    DLCI MAC Address   Node Identifier    DLSw terminated  Status
5       40:00:00:00:00:01  4F:FF:00:00:00:00  bridged          Init Fail
```

Exit

Use the **exit** command to exit BAN monitoring. When you exit from the monitoring module, you return to the DLSW> or ASRT> prompt.

Syntax: exit

Example: **exit**

9

Using SDLC Relay

This chapter describes Digital's implementation of Synchronous Data Link Control Relay (SRLY).

About SDLC Relay

Like DLSw, (see Chapter 1) SRLY is a method for consolidation of SDLC traffic onto the corporate multiprotocol backbone.

Unlike DLSw, SDLC Relay does not terminate the SDLC data link to reduce the likelihood of session timeouts, and does nothing to help reduce congestion on the WAN link. What SRLY provides is a serviceable method for shipping HDLC-formatted frames across WAN links in situations when it is not possible to use data link switching (Digital's DLSw product).

For more information on Digital's DLSw product, see Chapter 1, "Using the DLSw Protocol."

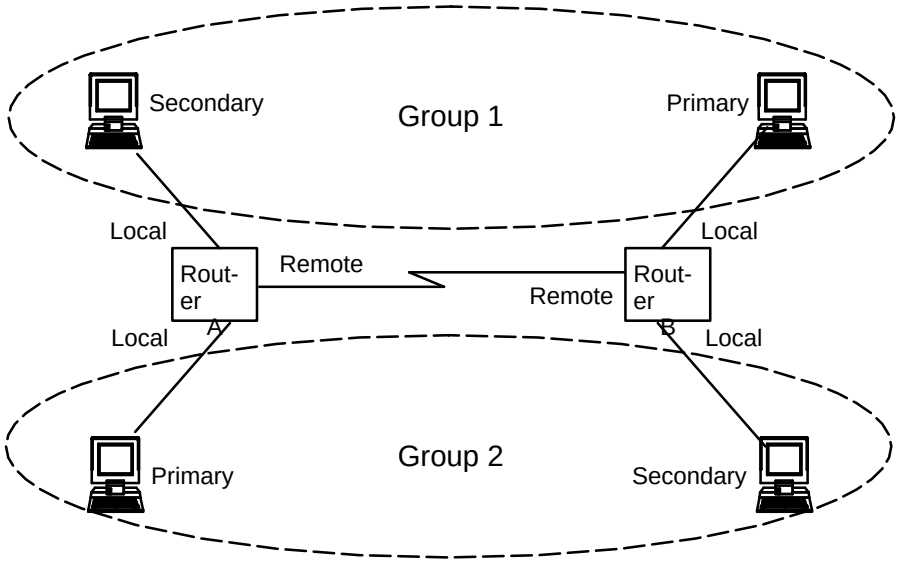
How SDLC Relay Works

Despite its name, the SDLC Relay protocol (SRLY) is designed to handle other protocols besides SDLC. The protocol works by encapsulating SDLC or any bit-oriented protocol (HDLC, LAPB) in UDP packets, and transmitting them through the IP cloud on a point-to-point connection to another SRLY device.

These connections are established by matching SRLY traffic to specific *ports* and *groups*. During configuration, each group has a unique group number assigned, and exactly two ports: one SDLC *primary* port, and one SDLC *secondary.* Matching SRLY traffic to group numbers and ports ensures that attached end stations can only send packets to the end stations for which they are intended.

Once packets are received, they are stripped of their UDP/IP header and transmitted to their destination address in their original protocol format.

Figure 9–1 SDLC Primary/Secondary Stations and Local/Remote Ports



Encapsulation in UDP/IP packets allows for SDLC frames to be handled via IP routing techniques. And since each SDLC frame is encapsulated unchanged, SRLY is transparent to sending and receiving stations. This transparency allows SRLY to support all SNA PU Types.

SDLC Primary and Secondary Stations

When configuring SRLY, a router's primary port must be connected to its primary end station. Its secondary port must be connected to its secondary end station. Within the primary -secondary communication process, the primary end station is responsible for initiation, scheduling, and termination of the session. The secondary station does not initiate communication, but responds to commands from its primary partner.

When running balanced protocols like LAP-B or HDLC, you can assign roles arbitrarily as long as one device is Primary, and its connected counterpart is Secondary.

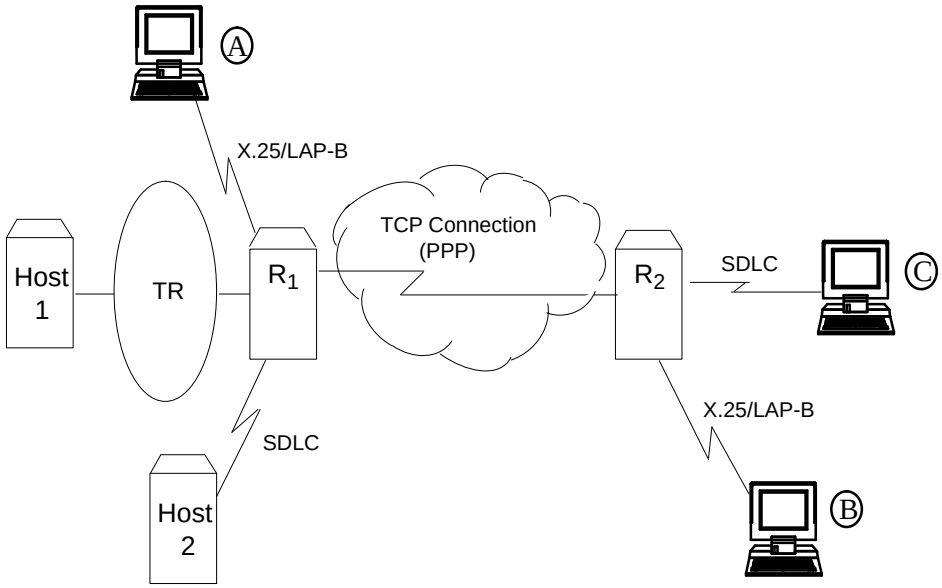
When to Use SDLC Relay

There are two general cases when you must use SRLY instead of DLSw. These are:

- When you cannot use DLSw owing to the router's inability to function as an SDLC secondary device.
- When you need to exchange any bit-oriented protocol, such as LAPB, HDLC, or SDLC primary over the wide area, between SNA or non-SNA devices.

DLSw can be configured for Host 1 and end station C in Figure 9–2: other wide-area connections would have to be accomplished using SDLC Relay.

Figure 9–2 SDLC Relay Configurations



In this diagram, DLSw can only be run between Host 1 and end-station C. Host 2 can only reach end station C via SRLY. SRLY can also be used to support wide-area communication between end stations A and B.

Setting Up SDLC Relay

Configuring SDLC Relay (SRLY) involves performing these steps on each of two routers.

1. Set the data link on the serial line using the **set data-link** command and the appropriate interface number.
2. Assign a group number using the **add group** command. The group number must be the same on each SRLY router. Group number 1 is the default.
3. At the `SDLC Config>` prompt, add a local port with the **add local** command. Be sure you add this port to the group defined in Step 2.
4. This port's data link type must be SDLC Relay (SRLY). Use the **set data link** command at the `Config>` prompt to set the data link type for the port.
5. At the `SDLC Config>` prompt, add a remote port with the **add remote** command. The IP address of the remote port is that of the cooperating SRLY router.
6. Repeat these steps for the second SRLY router. When prompted for the IP address of the remote port, provide the address of the first router.

Sample SDLC Relay Configuration

Following is a complete SDLC Relay configuration. The example assumes that the router has not been configured for any other protocols or data links.

Context Diagram

The example is based on the information shown in Figure 9–3. The IP connection between the two routers is over Digital serial line.

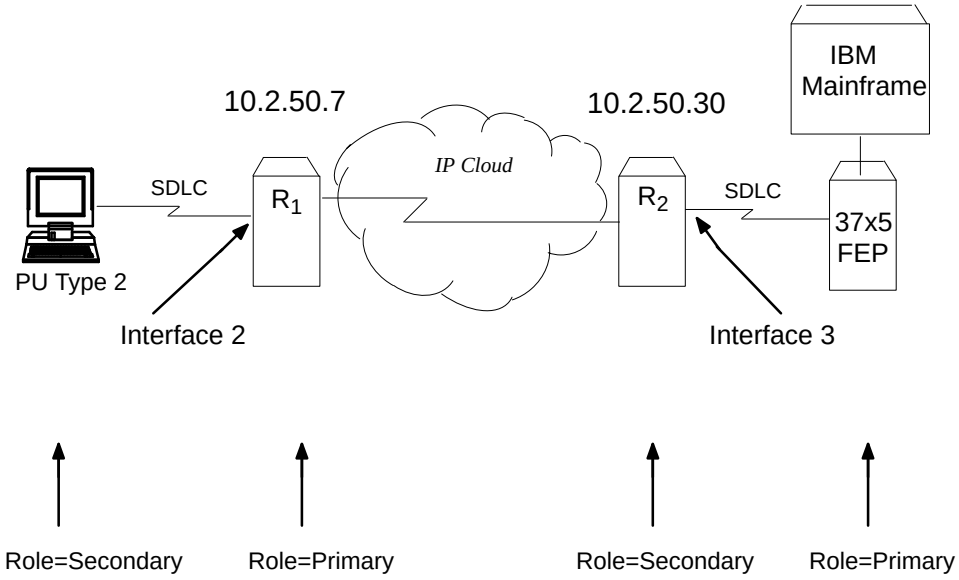
Configuring R_1 for SDLC Relay requires all of the information shown. This information includes the following:

- Group numbers for each group of SRLY ports
- Interface numbers for each SRLY port

- The internet addresses for each SRLY router

The example indicates where this information is provided in the course of the configuration procedure.

Figure 9–3 Context Diagram for SRLY Configuration



This example explains how to configure two routers for SRLY traffic. Router 1 (R_1) is connected to a PU Type 2.0 node. Router 2 (R_2) is connected to a front end processor (FEP).

Configuring SDLC Relay

On R_1, set the data link of the serial line to an SDLC Relay device. Notice that interface 2 is specified with the **set data-link** command shown here.

```
Config>set data-link srly 2
```

You can list the devices to confirm that an SDLC Relay device has been added.

```
Config>list dev
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN Digital Serial): CSR  81620, CSR2  80D00, vector 93
Ifc 2 (WAN SDLC Relay): CSR  81640, CSR2  80E00, vector 92
```

Set Serial Line Parameters

Next, set the line speed parameter for the SRLY line.

```
SLC Config>set speed
Internal Clock Speed [0]? 56000
```

After setting the line speed, you can check the configuration with the **list** command as shown:

Note: The prompt for the SRLY configuration module is `SRLY # Config>`, where `#` is the interface number specified with the **network** command.

```
SRLY 2 Config>list
Synchronous serial line interface configuration

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Internal Clock Speed: 56000
Transmit Delay Counter: 0
SLC Config>exit
```

Configuring the SDLC Relay Protocol

Configure the SDLC Relay protocol as shown:

```
Config>protocol sdlc
SDLC relay protocol user configuration
SDLC config>
```

As this example shows, the prompt for the SDLC Relay (SRLY) area is `SDLC config>`. Commands entered at this prompt only affect the SDLC Relay protocol. They have nothing to do with, and do not affect, SDLC data links or devices.

You can exit the SDLC Relay configuration procedure at any time by typing the **exit** command.

Assign a Group Number

The group number provides the association or binding between the router's local and remote ports, as well as the necessary correlation with the corresponding ports on the partner router. (The group number is actually carried over UDP in the SDLC Relay protocol header.)

To assign a group number, use the **add group** command. This number is assigned to the *primary* and *secondary* ports on the router you are configuring for SRLY. The group number you designate must be the same for each router.

```
SDLC config>add group
Group number: [1]?
```

Notice that the **list group** command shows that no ports have yet been configured for group 1.

```
SDLC config>list group
Group number: [1]? 2

                        SDLC Relay Configuration

 Group Number     Port Status       Net    SDLC Station     IP Address
                                   Number  address (hex)
-------------- ------------------  ------  -------------   ------------
No ports configured for group  2
```

Note: While the `SDLC Station address (hex)` appears in the listing, it is currently not implemented.

Add a Local Port

The local port is the serial interface that runs the SDLC (or HDLC or LABP) protocol to the physical device being relayed across the IP WAN network.

Next, add a local port to group 1. The port you add is the SRLY line defined earlier.

```
SDLC config>add local
Group number: [1]?
Interface number: [0]? 2
(P)rimary or (S)econdary: [P]?
```

Notice that the **list all** command shows that a local secondary port has been configured for group 1.

Note: The port role is actually arbitrary and does not have any correspondence to the actual attached SDLC station role.

```
SDLC config>list all

                        SDLC Relay Configuration

 Group Number     Port Status       Net    SDLC Station     IP Address
                                   Number  address (hex)
-------------- ------------------  ------  -------------   ------------
    1 (E)      Local  PRIMRY (E)    2
```

The (E) shown within the Port Status column stands for Enabled. A (D) in the Port Status column indicates that the port is Disabled. By default, SRLY ports are enabled; SRLY ports must remain enabled in order to use the feature.

Add a Remote Port

Next add a remote port for group 1. This is the port that leads to the IP cloud. Each group must consist of a pair of ports, one primary, the other secondary. The remote port added here must be secondary since the local port attached to it is primary.

The IP address provided is that of the router on the other side of the IP cloud, R_2.

```
SDLC config>add remote
Group number: [1]?
IP address of remote router: [0.0.0.0]? 10.2.50.30
(P)rimary or (S)econdary: [S]? s
SDLC config>list all

                        SDLC Relay Configuration

 Group Number     Port Status       Net    SDLC Station     IP Address
                                   Number  address (hex)
-------------- ------------------  ------  -------------   ------------
    1 (E)      Local   PRMRY  (E)    2

    1 (E)      Remote  SCNDRY (E)                          10.2.50.30
-------------------------------------------------------------------------
```

Configure the Neighbor Router

Up to this point, this example has shown how to configure R_1 in Figure 9–3. SRLY requires two routers, one on either side of the IP cloud. You must configure SRLY on each of them.

Set Data Link, Add Group, and Add Port

First, set up an SRLY data link for R_2. Do this in the same manner as shown earlier for R_1.

Next, add a group for R_2, assigning the same group number (1, in this case) as that assigned on R_1. Add a local port for the assigned group. This is the SRLY line you have already defined. In this case, the port type is normally *secondary* since a front end processor (FEP) (which, like a host, is always primary) is on the line.

```
SDLC config>add local
Group number: [1]?
Interface number: [0]?
(P)rimary or (S)econdary: [S]?
SDLC config>list all

                        SDLC Relay Configuration

 Group Number     Port Status       Net    SDLC Station     IP Address
                                   Number  address (hex)
-------------- ------------------  ------  -------------   ------------
    1 (E)      Local   SCNDRY (E)    0
```

Add a Remote Port

Finally, add a remote port for group 1. This is the port that leads to the IP cloud. Since the FEP is primary, this port is secondary. As mentioned earlier, each group must consist of a primary and secondary station.

Since we are configuring R_2, the the IP address of the remote router belongs to R_1. See Figure 9–3 for the addresses of R_1 and R_2, and their roles in the overall SRLY configuration.

```
SDLC config>add remote
Group number: [1]?
IP address of remote router: [0.0.0.0]? 10.2.50.7
(P)rimary or (S)econdary: [S]? p

SDLC config>list all

                        SDLC Relay Configuration

 Group Number     Port Status       Net    SDLC Station     IP Address
                                   Number  address (hex)
-------------- ------------------  ------  -------------   ------------
    1 (E)      Remote PRMRY   (E)                         10.2.50.7
    1 (E)      Local  SCNDRY  (E)    0
```

10

Configuring SDLC Relay

This chapter describes the Synchronous Data Link Control (SDLC) Relay configuration commands.

For more information about the SDLC Relay protocol, refer to Chapter 9, “Using SDLC Relay.”

About SDLC Relay Configuration Commands

SDLC Relay configuration commands are entered at the `SDLC Config>` prompt. Changes made to the router’s configuration do not take effect immediately. They affect the operating router only after it is restarted..

Accessing the SDLC Relay Configuration Environment

Use the SDLC Relay configuration process to change the configuration of the router. To enter the configuration process, type **talk 6**, or just **t 6**, at the MOS prompt (*). This brings you to the `Config>` prompt as shown:

```
MOS Operator Control

* talk 6
Gateway user configuration
Config>
```

Note: The `Gateway user configuration` banner appears only when you enter CONFIG after a restart.

If the `Config>` prompt does not appear immediately, press RET again.

All SDLC Relay configuration commands are entered at the `SDLC config>` prompt. To access this prompt, enter the **protocol sdlc** command as shown:

```
Config>protocol sdlc
SDLC Relay user configuration
SDLC config>
```

SDLC Relay Commands

Enter the SDLC Relay configuration commands at the `SDLC config>` prompt, and monitoring commands at the `SDLC>` prompt. Table 10–1 lists the SDLC Relay configuration commands.

Table 10–1 SDLC Relay Command Summary

Command	Function
?(Help)	Lists the configuration and monitoring commands or parameters associated with these command.
Add	Adds groups, local ports, and remote ports.
Delete	Disables or temporarily suppresses, groups, local ports, or remote ports.
Disable	Disables or temporarily suppresses groups and ports.
Enable	Enables groups and ports.
List	Displays SDLC Relay and group-specific configurations.
Exit	Exits the SDLC Relay configuration or monitoring environment.

? (Help)

Use the **? (help)** command to list the commands available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: ?

Example: **?**

```
ADD
DELETE
DISABLE
ENABLE
LIST
EXIT
```

Add

Use the **add** command to add group numbers, local ports, and remote ports.

Syntax: add
group
local-port
remote-port

group

Assigns a number to a group of primary or secondary ports added to the router.

Example: **add group**

```
Group number: [1]? 1
Point to Point connection: (Yes of No)? Y
```

Group number The group number that you are designating for the port.

local-port

Identifies the interface that you are using for the local port.

Example: **add local-port**

```
Group number: [1]?1
Interface number: [0]? 0
(P)rimary or (S)econdary:[S}? p
```

Group number	The group number for the port. This number must correspond to a group number assigned previously with the **add group** command.
Interface number	The interface number of the router that designates the local port.
Primary or Secondary	Designates the port type, primary (P) or secondary (S).

remote-port

Identifies the IP address of the port directly connected to the serial line on the remote router.

Example: **add remote-port**

```
Group number: [1]? 1
IP address of remote router:[0.0.0.0]? 128.185.121.97
(P)rimary or (S)econdary:[S]? s
```

Group number	The group number for the port. This number must match one of the **add group** parameters configured previously.
IP address of remote router	Identifies the IP address of the interface on the remote router.
Primary or Secondary	Designates the port type, primary (P) or secondary (S).

Delete

Use the **delete** command to remove group numbers, local ports, and remote ports.

Syntax: delete
group . . .
local-port . . .
remote-port . . .

group *group#*

Removes a group (group#) of SDLC Relay configured ports.

Example: **delete group 1**

local–port ***interface#***

Removes the local port for the specified interface (interface#).

Example: **delete local-port 0**

remote–port

Removes the remote port for the specified group.

Example: **delete remote-port**

```
Group number: [1]? 1
(P)rimary or (S)econdary:[S}? S
```

Group number	The group number for the remote port.
Primary or Secondary	Designates the port type, primary (P) or secondary (S).

Disable

Use the **disable** command to suppress forwarding for an entire relay group or a specific relay port.

Syntax: disable
group . . .
port . . .

group ***group#***

Suppresses transfer of SDLC Relay frames to or from a specific group (group#).

Example: **disable group 1**

port

Suppresses transfer of SDLC Relay frames to or from a specific local port.

Example: **disable port**

```
Interface number: [0]? 0
(P)rimary or (S)econdary:[S]? s
```

Interface number	The interface number of the port that you want to disable.
Primary or Secondary	Designates the port type, primary (P) or secondary (S).

Enable

Use the **enable** command to enable data transfer for an entire group or a specific local interface port.

Syntax: enable
group . . .
port

group *group#*

Allows transfer of SDLC Relay frames to or from the specified group.

Example: **enable group 1**

port

Allows transfer of SDLC Relay frames to or from the specified local port.

Example: **enable port**

```
Interface number: [0]? 0
(P)rimary or (S)econdary:[S]? s
```

Interface number	The interface number of the port that you want to disable.
Primary or Secondary	Designates the port type, primary (P) or secondary (S).

List

Use the **list** command to display the configuration or status of a specific group or of all groups.

Syntax: list

all

group . . .

all

Displays the configurations of all local ports.

Example: **list all**

```
                    SDLC Relay Configuration

                    SDLC Relay Configuration

 Group Number     Port Status       Net    SDLC Station     IP Address
                                   Number  address (hex)
-------------- ------------------  ------  -------------   ------------
    1 (E)      Local PRMRY    (D)     2
    1 (E)      Remote SCNDRY  (E)                         128.185.452.11
    2 (D)      Local PRMRY    (D)     0
    2 (D)      Remote SCNDRY  (D)                         128.185.450.31
```

Note: While the `SDLC Station address (hex)` appears in the listing, it is currently not implemented.

Group Number	Indicates the group number and the status of the group, enabled (E) or disabled (D).
Port Status	Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).
Net Number	Indicates the device number of the local port. This number matches the number displayed using the **list devices** command.
IP Address	Indicates the IP address of the remote port.

group *group#*

Displays the configuration of a specified group.

Example: **list group 1**

```
                    SDLC Relay Configuration

 Group Number     Port Status       Net    SDLC Station     IP Address
                                   Number  address (hex)
-------------- ------------------  ------  -------------   ------------
    1 (E)      Local PRMRY   (D)      2
    1 (E)      Remote SCNDRY (E)                          128.185.452.11
```

Group Number	Indicates the group number and the status of the group, enabled (E) or disabled (D).
Port Status	Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).
Net Number	Indicates the device number of the local port. This number matches the number displayed using the Config> **list devices** command.
IP Address	Indicates the IP address of the remote port.

Exit

Use the **exit** command to exit the SDLC Relay configuration or monitoring process. environment.

Syntax: exit

Example: **exit**

11

Monitoring SDLC Relay

This chapter describes the Synchronous Data Link Control (SDLC) Relay monitoring commands.

For more information about the SDLC Relay protocol, refer to Chapter 9, “Using SDLC Relay.”

About SDLC Relay Monitoring Commands

You enter SDLC Relay monitoring commands at the `SDLC>` prompt. These commands take effect immediately, but do not become part of router’s non-volatile configuration memory. Thus, while monitoring commands allow you to make real-time changes to the router’s configuration, these changes are temporary. The router’s configuration memory overwrites them when the router restarts. Any permanent changes you wish to make (by storing them in FLASH) should be made with SDLC Relay configuration commands (see Chapter 10).

Monitoring consists of these actions:

- Monitoring the protocols and network interfaces currently in use by the router.
- Displaying Event Logging System (ELS) messages relating to router activities and performance.
- Making real-time changes to the SDLC Relay configuration without permanently affecting the router’s non-volatile configuration memory.

Accessing the SDLC Relay Monitoring Environment

To enter the monitoring environment, enter **talk 5**, or just **t 5**, at the MOS prompt (*). This brings you to the monitoring environment as shown:

```
MOS Operator Control

* talk 5
+
```

You enter SDLC Relay monitoring commands at the SDLC> prompt. To access this prompt, enter the **protocol sdlc** command at the + prompt as shown:

```
+ protocol sdlc
SDLC>
```

SDLC Relay Commands

Enter the SDLC Relay monitoring commands at the SDLC> prompt. Table 11–1 lists the SDLC Relay monitoring commands.

Table 11–1 SDLC Relay Command Summary

Command	Function
?(Help)	Lists the configuration and monitoring commands or parameters associated with these command.
Clear–Port–Statistics	Clears SDLC statistics for the specified port.
Disable	Disables or temporarily suppresses groups and ports.
Enable	Enables groups and ports.
List	Displays SDLC Relay and group-specific configurations.
Exit	Exits the SDLC Relay configuration or monitoring environment.

? (Help)

Use the **? (help)** command to list the commands available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: ?

Example: **?**

```
CLEAR-PORT-STATISTICS
LIST
ENABLE
DISABLE
EXIT
```

Clear-Port-Statistics

Use the **clear-port-statistics** command to reset the SDLC Relay statistics for all ports. The statistics being cleared include the number of packets forwarded and the number of packets discarded for each group. You can display statistics with the **list group** and **list all** commands.

Syntax: clear-port-statistics

Example: **clear-port-statistics**

```
Clear all port statistics? (Yes or No): Y
```

Disable

Use the **disable** command to suppress forwarding for an entire relay group or a specific relay port.

When you use this command within the monitoring process, its effects are not stored in the router's non-volatile configuration memory.

Syntax: disable
group . . .
port . . .

group *group#*

Suppresses transfer of SDLC Relay frames to or from a specific group (group#).

Example: **disable group 1**

port

Suppresses transfer of SDLC Relay frames to or from a specific local port.

Example: **disable port**

```
Interface number: [0]? 0
(P)rimary or (S)econdary:[S]? s
```

Interface number	The interface number of the port that you want to disable.
Primary or Secondary	Designates the port type, primary (P) or secondary (S).

Enable

Use the **enable** command to enable data transfer for an entire group or a specific local interface port.

When you use this command within the monitoring process, its effects are not stored in the router's non-volatile configuration memory.

Syntax: enable
group . . .
port . . .

group *group#*

Allows transfer of SDLC Relay frames to or from the specified group.

Example: **enable group 1**

port

Allows transfer of SDLC Relay frames to or from the specified local port.

Example: **enable port**

```
Interface number: [0]? 0
(P)rimary or (S)econdary:[S]? s
```

Interface number	The interface number of the port that you want to disable.
Primary or Secondary	Designates the port type, primary (P) or secondary (S).

List

Use the **list** command to display the configuration or status of a specific group or of all groups.

Syntax: list
all
group . . .

all

Displays the configurations of all local ports.

Example: **list all**

```
                    SDLC Relay Configuration

 Group    Port Status    Net    SDLC Station      Packets        IP Address
  Num                    Num    address (hex)   fwrd    disc
-------- -------------- ------ ------------- -------- -------- -------------
 1 (E) Local  SCNDRY (E)    2                     0        0

 1 (E) Remote  PRMRY (E)                          0        0   16.20.104.94
```

Note: While the `SDLC Station address (hex)` appears in the listing, it is currently not implemented.

Group Number	Indicates the group number and the status of the group, enabled (E) or disabled (D).
Port Status	Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).

Net Number	Indicates the device number of the local port. This number matches the number displayed using the **list devices** command.
IP Address	Indicates the IP address of the remote port.

group *group#*

Displays the configuration of a specified group.

Example: **list group 1**

```
                    SDLC Relay Configuration

 Group    Port Status    Net    SDLC Station      Packets        IP Address
  Num                    Num    address (hex)   fwrd    disc
-------- -------------- ------ ------------- -------- -------- -------------
 1 (E) Local  SCNDRY (E)    2                    63        0

 1 (E) Remote  PRMRY (E)                         45        2   16.20.104.94
```

Group Number	Indicates the group number and the status of the group, enabled (E) or disabled (D).
Port Status	Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).
Net Number	Indicates the device number of the local port. This number matches the number displayed using the Config> **list devices** command.
IP Address	Indicates the IP address of the remote port.

Exit

Use the **exit** command to exit the SDLC Relay configuration or monitoring process. environment.

Syntax: exit

Example: **exit**

A

DLSw MIB Support

DLSw MIB

The full text of the DLS extensions is contained in IBM®'s enterprise tree in the 6611 MIB. Refer to *6611 Network Processor Network Management Reference*, IBM manual number GC30–3567–01 for more information.

NO TAG lists the subgroups within the DLS MIB that Proteon supports.
NO TAG lists the extensions within a supported subgroup that are supported.

Table A–1 DLSw MIB Tables Supported

DLSw Group Attributes	Supported	Not Supported
Virtual Ring Segment Number	✓	
Filter Types		✓
Participating Router Table	✓	
SNA Local Filter Frame Table		✓
SNA Remote Filter Frame Table		✓
NETBIOS Local Name Filter Table		✓
NETBIOS Remote Name Filter Table		✓
SNA Default Destination Table		✓
NETBIOS Default Destination Table		✓
SNA Station Table		✓
Circuit Table	✓	

Table A–2 DLSw MIB Objects Supported

DLSw Table Name	DLSw Object Name	Supported	Not Supported
Participating Router Table			
	IBM DLS Router Address	✓	
	IBM DLS Router Status	✓	
	IBM DLS Router Defined By	✓	
	IBM DLS Router In Frames		✓
	IBM DLS Router Out Frames		✓
Circuit Table			
	IBM DLS Cir If Index	✓	
	IBM DLS Cir Src Address	✓	
	IBM DLS Cir Src Sap	✓	
	IBM DLS Cir Dest Address	✓	
	IBM DLS Cir Dest Sap	✓	
	IBM DLS Cir Partner Router Address	✓	
	IBM DLS Cir Local Link State	✓	
	IBM DLS Cir Local Link Sub State	✓	
	IBM DLS Cir Local Link Routing	✓	
	IBM DLS Cir Local Link Test Cmds Sent		✓
	IBM DLS Cir Local Link Test Cmds Fail		✓
	IBM DLS Cir Local Link Test Cmds Rcv		✓
	IBM DLS Cir Local Link Data Pkt Sent	✓	
	IBM DLS Cir Local Link Data Pkt Resent		✓
	IBM DLS Cir Local Link Max Cont Resent		✓
	IBM DLS Cir Local Link Data Pkt Rcv	✓	
	IBM DLS Cir Local Link Invalid Pkt Rcv		✓
	IBM DLS Cir Local Link Adp Rcv Err		✓
	IBM DLS Cir Local Link Adp Send Err		✓
	IBM DLS Cir Local Link Rcv Inactive Timeouts		✓

Table A–2 (Cont.) DLSw MIB Objects Supported

DLSw Table Name	DLSw Object Name	Supported	Not Supported
Circuit Table (cont.)			
	IBM DLS Cir Local Link Cmd Polls Sent		✓
	IBM DLS Cir Local Link Cmd Repolls Sent		✓
	IBM DLS Cir Local Link Cmd Cont Repolls		✓
	IBM DLS Cir Local Address		✓

B

Interoperating with the IBM 6611 Router

A number of configuration issues must be addressed for Digital's DLSw implementation to interoperate with that of the IBM 6611™ router.

The following sections provide an overview of these issues, and indicate which features of Digital's DLSw implementation are not interoperable with that of the IBM 6611.

Note: The issues cited explained here derive from testing performed with the IBM 6611's MPNP V1.2 software. The issues may not apply to other MPNP software versions.

Bridge Configuration Issues

The following are bridge configuration issues:

- The LAN identification (Segment number) of the DLSw must match on both the Digital and IBM 6611 routers. If a mismatch persistently exists, enter the DLSw configuration environment (**T 6**) and select the DLSw protocol. The **set srb** command can then be used to set a Segment Number value that matches the IBM 6611 equivalent.
- The maximum MTU value that can be used for the Bridge Frame is 2100 bytes. This is the largest value currently supported by the IBM 6611. If MTU values less than 2100 are specified, it is important that the configured values match on both the Digital and IBM 6611 routers.

- Currently Digital interoperates with the IBM 6611 only for SNA traffic over DLSw. The Digital router does not support NetBIOS traffic over DLSw. There is, however, a proprietary Digital solution that permits NetBIOS traffic to be bridged through an IP tunnel.

IP-related Configuration Issues

- The client/server and peer/peer DLSw group feature that enables Digital DLSw neighbors to dynamically find each other is not interoperable with the IBM 6611 DLSw implementation. As a result, the DLSw's **add tcp neighbor** configuration command must be used to define the static IP addresses of adjacent IBM 6611 DLSw peers. However, DLSw group functionality can still be used to locate other Digital routers even though IBM 6611 routers exist in the network.

- The preceding interoperability restriction on the Digital DLSw group feature has implications for the selection of RIP/OSPF:

  – To utilize DLSw groups on a Digital router, the configuration of OSPF/MOSPF is also required. But since these DLSw groups are not interoperable with the 6611, it is possible to configure the Digital DLSw router with only RIP enabled and no OSPF configuration.

  – Although OSPF and RIP can both be enabled on the Digital side, MOSPF (if selected through the OSPF configuration) is not currently supported by the IBM 6611.

  – For the IBM 6611 MPNP V1R2.0 software, the APPN network node implementation on the 6611 only appears to work with RIP.

- Within the Digital IP configuration make sure that the fill patterns configured for broadcast addresses on a given interface match their equivalent definition on the IBM 6611.

- Digital's Bandwidth Reservation System (BRS) that can be utilized to guarantee bandwidth for the transport of SNA traffic over DLSw, is not interoperable with the IBM 6611 DLSw implementation.

  Although the prioritization assigned by the Digital hardware for BRS can be implemented in an outbound direction, the prioritization order will not be guaranteed if intermediate IP routers do not support BRS. Also, since

the 6611 does not support BRS in its end of the line, BRS could only be applicable in a single direction.

TCP-related Issues

- **TCP Connection Break Detection Differences.** If Keepalive is disabled, the Digital DLSw implementation will not detect a broken TCP connection until it attempts to send data on the connection.
- **TCP Connection Reestablishment Differences.** Once a TCP connection is broken, the Digital DLSw implementation re-establishes the TCP connection when a new DLSw SSP_CANUREACH is generated upon receipt of a DLC TEST message from an end station. The IBM 6611 may not exhibit the same behavior.
- **Keepalive Disable/Enable Related Differences.** The Digital DLSw implementation permits the enabling/disabling of a Keepalive option when a TCP neighbor IP address is added (configured). Although TCP in the IBM 6611 DLSw implementation will respond to Keepalive messages received on a TCP session, there is no mechanism to configure the resident 6611 TCP so as to enable the generation of TCP Keepalive messages.
- **Maximum Number of TCP Connections Supported.** In the Digital DLSw implementation, there is no hard-coded restriction on the maximum number of TCP connections supported. As a result, the maximum number of TCP connections supported is directly related to a Digital DLSw Router's available memory. In the IBM 6611 case, there is a hard coded internal restriction of 100 TCP connections that can be supported in the DLSw implementation.

DLSw-related Issues

- The Digital DLSw implementation does not support generation of SSP_IAMOKAY message (SSP Message Type 'x1D') while IBM 6611 DLSw implementation is supported. This SSP message is undocumented in RFC 1434, and is silently discarded by the Digital DLSw implementation upon receipt.
- The IBM 6611 DLSw implementation processes SSP_ENTER_BUSY/EXIT_BUSY messages received from the Digital DLSw implementation but will not generate similar flow control related SSP messages.

- The Digital DLSw implementation does support the user defined SSP_TEST_CIRCUIT_REQ message (SSP message type 'x7A') that is generated by an IBM 6611 DLSw router functioning as an APPN network node. Upon receipt of this message, the Digital DLSw implementation will return the user defined SSP_TEST_CIRCUIT_RSP message (SSP message type 'x7B'). This response is expected by the IBM 6611 DLSw router's APPN network node implementation.

Miscellaneous Interoperability Issues

- The IBM 6611 chooses to fill bytes in reserved fields with 'xFF' values, whereas the Digital DLSw implementation zeros these fields whenever SSP Control or Information messages are transmitted. These differences should be noted whenever a Wide Area Sniffer is being used to monitor DLSw SSP messages flowing across a DLSw WAN connection.

- If a problem is encountered when trying to establish a DLSw connection initiated by the IBM 6611, check the IBM 6611 configuration to ensure that MAC address filtering has not been inadvertently enabled for an associated source or destination MAC address.

- Although RFC 1434 does not specifically address the issue of orphan DLSw sessions (e.g., DLSw sessions that remain in a DLSw circuit established state with no subsequent activity), both the Digital and IBM 6611 DLSw implementations resolve this issue by providing orphan DLSw session timeouts. DLSw sessions that remain inactive while in DLSw circuit established state for longer than 30 seconds are eliminated by both implementations.

Glossary

A

Advanced Peer-to-Peer Networking

See APPN.

Advanced Program-to-Program Communication

See APPC.

APPC

Advanced Program-to-Program Communication. The general facility characterizing the LU 6.2 architecture and its various implementations in products.

APPN

Advanced Peer-to-Peer Networking. An extension of SNA. It features greater distributed network control, avoiding critical hierarchical dependencies and thereby isolating the effects of single points of failure. It also features dynamic exchange of network topology information among network nodes, fostering ease of connection and reconfiguration, adaptive route selection, simplified network definition, and distributed directory lookup.

B

BAN

Boundary Access Node. An enhancement of Frame Relay, bridging, and DLSw functionality enabling remote T2.0 and T2.1 endstations to establish wide-area communication with an IBM front-end processor.

basic transmission unit

The unit of data and control information passed between path control components.

bit-oriented protocol

A protocol that sends data between devices as a steady stream of bits. Clocks at source and destination are synchronized to use a predetermined time interval to determine where characters begin and end. Examples include SDLC and LAP-B.

C

cache

An optional part of a directory database in network nodes where frequently used directory information can be stored to speed directory searches.

cluster controller

A device that controls the input/output operations of multiple devices attached to it.

D

datagram delivery protocol

A protocol, such as IP or UDP, designed to deliver data in a series of discrete packets. The packets may take different routes to the same destination, and their delivery may not be guaranteed.

data-link layer

The second layer in the OSI protocol stack, and the one in which bridging occurs.

Data Link Connection Identifier

See DLCI.

Data Link Switching

See DLSw.

DCE

Data Circuit-terminating Equipment. The X.25 term for a device, a modem, for instance, to which an end node attaches.

DLCI

Data Link Connection Identifier. A 10-bit field in the frame relay header identifying the permanent virtual circuit between the user and frame relay device.

DLSw

Data Link Switching. Based on RFC 1434, and originally developed within the IBM 6611 router, a technique for reliable delivery of SDLC and LLC2 traffic across WANs.

DSAP

Destination SAP. The Service Access Point associated with a destination port.

DTE

Data Terminal Equipment. The X.25 term for an end node, such as a terminal.

dynamic routing

Routing that adjusts automatically to network topology or traffic changes, based on information from routing protocol transmissions.

E

encapsulation

The insertion of protocol information into the data-area of another protocol, such as IP or UDP, for transport across a wide area network.

End System

See ES.

End System Hello

See ESH.

ES

End System. In the OSI protocol, a host system that performs the functions of all of the layers of the OSI reference model.

ESH

End System Hello. A packet originating in an end system and passing information to an intermediate system.

F

FR

Frame Relay.

frame

Informal name for a data-link packet data unit. Control information in the frame provides addressing, sequencing, flow control, and error control to the respective protocol levels.

H

HDLC

High-level Data Link Control. An ISO standard bit-oriented data link protocol that specifies the encapsulation method of data on synchronous data links.

Hello/I-H-U

Hello and I-Heard-You. An EGP protocol that requests and confirms neighbor reachability.

High-level Data Link Control

See HDLC.

I

I–Frame

Information Frame.

IGP

Interior Gateway Protocol. A protocol that distributes routing information to the routers within an autonomous system.

IP

Internet Protocol. The Department of Defense (DoD) Internet standard protocol that defines the Internet datagram as the unit of information passed across the Internet. IP corresponds to the OSI reference model layer 3 and provides connectionless datagram service.

IP datagram

A packet containing IP control information exchanged between network entities.

L

link station

An SDLC station with which a link has been established. Each SDLC link station has either a primary or secondary role in the communication process.

Logical Unit

See LU.

low-entry networking

A capability in type 2.1 nodes allowing them to attache directly to one another using peer-to-peer protocols and allowing them to support multiple parallel sessions between logical units.

LU

Logical Unit. A type of network accessible unit that enables end users to gain access to network resources and communicate with one another.

LU type

The classification of an LU in terms of the specific subset of SNA protocols and options it supports for a given session.

M

MAC

Medium Access Control. The sublayer of the data link control layer that supports media-dependent functions. It includes the medium-access port. MAC protocols put packets from upper-level protocols into the frame format of the destination network.

Medium Access Control

See MAC.

MIB

Management Information Base. A database of managed objects accessed from a network management protocol.

modem eliminator

A device permitting the connection of two DTE devices without a modem.

MOSPF

Multicast OSPF. A protocol required for use of DLSw group functionality.

N

NAU

Network Accessible Unit. A logical unit (LU), physical unit (PU), system services control point (SSCP) or control point (CP).

Network Accessible Unit

See NAU.

network layer

Layer 3 of the OSI reference model, at which all routers operate.

network name

The symbolic identifier by which end users refer to a network accessible unit, a link, or a link station within a given network.

node type

A designation of a node according to the protocols it supports and the network accessible units that it can contain.

NRZ

Non-return to zero.

NRZI

Non-return to zero inverted.

NSAP

Network Service Access Point. The point at the layer boundary where the communications capability of the network layer is made available to its users. An OSI network address.

O

Open Shortest Path First

See OSPF.

OSI

Open Systems Interconnection. The ISO architecture for internetworking.

OSI reference model

The seven-layer model of computer network architecture and its data functions, specified by ISO.

OSPF

Open Shortest Path First. A link-state protocol that IGPs use to exchange routing information between routers.

P

packet

A self-contained block of data containing control and user information transmitted across a network.

packet switching

A data transfer scheme in which information is broken into individual packets, transferred across a communications link, and reassembled at the receiving end. In a packet-switching system, each node through which the packet travels determines the route to the next receiver with no previously-established communication path.

peer-to-peer communication

Communication between two nodes in an SNA network not requiring explicit mediation by a system services control point.

Physical Unit

See PU.

PLU

Primary Logical Unit. The logical unit that sends a BIND to active a session with its partner LU.

port

The representation of a physical connection to the link hardware.

Primary Logical Unit

See PLU.

PU

Physical Unit. The component that manages and monitors the resources associated with a node, as requested by an SSCP via an SSCP-PU session. This term applies to type 2.0, type 4, and type 5 nodes.

R

RIF

Routing Information Field. A field in the Token Ring 802.5 header generated by a source node and used by a source-route bridge to determine the path a packet must use when passing through a Token Ring network segment.

RIP

Routing Information Protocol. A distance-vector IGP used to exchange routing information between routers.

route

An ordered sequence of nodes that represent a path from an origin node to a destination node traversed by the traffic exchanged between them.

routing

The assignment of a path by which a message can reach its destination.

Routing Information Field

See RIF.

Routing Information Protocol

See RIP.

RS-232

A type of serial interface.

S

SAP

Service Access Point. The interface between a layer in the OSI protocol stack and the layer above. Generally, SAP is preceded by a letter denoting the layer providing the service (for example, network-layer services are NSAPs). Well known services are associated with well known SAP numbers.

SDLC

Synchronous Data Link Control. A link level protocol designed for transfer of information in LAN environments. Transmission exchanges may be duplex or half-duplex over switched or non-switched links. The configuration of the link connection can be point-to-point, multipoint, or looped.

SDLC Relay

A Proteon product that supports exchange of bit-oriented protocols across the wide area.

segment number

A number that identifies an individual LAN, such as a single Token Ring or a serial line.

serial interface

An interface that supports connections via serial line.

Service Access Point

See SAP.

session

A logical connection between two network accessible units that can be activated, tailored to provide various protocols, and deactivated as requested. Each session is uniquely identified in a transmission header accompanying messages exchanged during transmission.

session limit

The maximum number of concurrently active LU-LU sessions that a particular LU can support.

SNA

Systems Network Architecture. A proprietary networking architecture used by IBM and IBM-compatible mainframes.

SNA network

The part of a user-application network that conforms to SNA formats and protocols. It enables reliable transfer of data among end users and provides protocols for controlling the resources of various network configurations. It consists of network accessible units; boundary function, gateway function, intermediate session routing function components, and the transport network.

SRLY

See SDLC Relay.

SSAP

Source SAP.

SSCP

System Services Control Point. A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for end users of an SNA network. Multiple SSCPs can cooperate as peers, dividing the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

SSCP-PU session

A session between a system services control point and a physical unit.

subarea

A portion of the SNA network consisting of a subarea node, any attached peripheral nodes, and their associated resources. Within a subarea node, all network accessible units, links, and adjacent link stations that are addressable within the subarea share a common subarea address and have distinct element addresses.

subarea network

Interconnected subareas, their directly attached peripheral nodes, and the transmission groups that connect them.

subnet

In IP, a distinct network within a network. In OSI, the connection from the IS to the subnetwork.

subnet address

An extension of the IP addressing scheme that allows a site to use a single IP address for multiple physical networks.

Synchronous Data Link Control

See SDLC.

System Services Control Point

See SSCP.

T

TCP

Transmission Control Protocol. A protocol in the TCP/IP suite of protocols that implements transport functions on the internet

TCP/IP

Transmission Control Protocol/Internet Protocol.

token

In a local area network, the symbol of authority passed among data stations to indicate the station temporarily in control of the transmission medium. The token becomes a frame when a station appends data to it.

Token Ring

A network with a ring topology that passes tokens from one attaching device to another. Examples include FDDI networks and the IBM Token Ring network.

transparent bridging

A bridging mechanism implemented by software on bridges and invisible (transparent) to end stations.

type 2.0 node

An SNA peripheral node that requires the services of a PU5 (T5) subarea host in order to communicate. Type 2.0 nodes are known as PU2.0 or T2.0 nodes; the terms are used interchangably. A 3270 terminal cluster controller (for example, an IBM 3174) is an example of a T2.0 node. T2.0 nodes do not perform dynamic link configuration.

type 2.1 node

An SNA peripheral node (T2.1) that has the capability to support communication with another T2.1 node without the mediation of a PU5 (T5) subarea host node. T2.1 nodes come in three basic types with increasing network capabilities: LEN nodes, APPN End Nodes (ENs), and APPN Network Nodes (NN). All three perform dynamic link configuration using XID3's during link activation negotiation. DLSw is capable of carrying SNA traffic between all three T2.1 types. An IBM AS/400 is an example of a T2.1 node.

Index

A

Accessing ELS messages, for BAN, 6–12
Adding an SDLC link station, 2–3, 3–4
APPN, and DLSw, B–2
ASRT, configuring, for BAN, 6–7
ASRT, configuring, 1–16

B

BAN
  adding a DLCI, 6–6
  and bridged Token Ring format frames, 6–3
  assigning a circuit name, 6–6
  boundary node identifier address, 6–8
  bridged configuration, 6–3
  checking configuration, 6–11
  checking initialization, 6–11
  configuring, 6–6
  disabling transparent bridging, 6–7
  DLCI MAC address, adding, 6–8
  DLSw-terminated configuration, 6–3
  ELS messages, 6–11
  enabling source route bridging, 6–7
  filtering, 6–2
  initialization, 7–3
  modes, choosing, 6–5
  networks handled, 6–1
  opening SAPs for, 6–9
  overview, 6–1
  setting up multiple connections, 6–10
  setting-up multiple DLCIs for, 6–10
  specifying bridging or terminated, 6–9
  status messages, 6–12
  using multiple DLCIs, 6–10
  virtual LLC2 connection, 6–4
BAN configuration commands
  add, 7–2
  delete, 7–3
  exit, 7–3
  Help, 7–2
  list, 7–3
BAN monitoring commands
  exit, 8–3
  Help, 8–2
  list, 8–2
Bit-oriented protocols, over WAN links, 9–3
Boundary Access Node
  See also BAN
  configuring. *See* BAN

Bridging
  across the wide area, 1–2
  setting up for DLSw, 1–5
  traditional approach to, 1–2

C

Client/server groups, adding, 2–9, 3–9
Clock speed, SDLC Relay, 9–6
Command summary
  BAN, 7–1, 8–1
  DLSw, 2–2, 3–2
  SDLC, 4–2, 5–4
  SDLC Relay, 10–2, 11–2
Concurrent bridging, configuring, 1–5
Configuration commands
  BAN, 7–1, 8–1
  DLSw, 2–1, 3–1
  SDLC, 4–1, 5–1
  SDLC relay, 10–1, 11–1
Configuration environment
  accessing, 2–1
  SDLC relay, accessing, 10–1
Configuring
  ASRT, 1–5–1–7, 1–16
  BAN, 6–6
  DLSw, 1–4
  IP, for DLSw, 1–6–1–8
  SDLC Relay, 9–3

D

DLSw
  adding an SDLC link station, 2–3, 3–4
  adding SDLC link stations, 1–8
  benefits of, 1–4
  client/server groups, 2–9, 3–9
  configuration environment, 2–1
  configuration requirements, 1–4
  configuring, 1–1, 1–8, 1–19–1–23
  configuring ASRT for, 1–5
  configuring for Token Ring, 1–5
  configuring IP for, 1–6, 1–12–1–14
  configuring OSPF or RIP for, 1–14
  configuring protocols for, 1–12–1–18
  configuring SDLC interfaces for, 1–7
  enabling dynamic routing for, 1–6
  enabling OSPF for, 1–6
  enabling RIP for, 1–7
  group functionality, and OSPF, 1–14
  groups, configuring, 1–19, 1–20
  Interoperability issues, B–1–B–7
  interoperability with IBM 6611, bridge configuration, B–1
  LLC2 termination, 1–3
  MIB support, A–1
  miscellaneous interoperability issues, B–4
  monitoring, 2–1, 3–1
  multicast addresses, 2–9, 3–10
  multicast OSPF, enabling, 1–14
  on-demand TCP sessions, 1–22
  OSPF interfaces, defining, 1–15
  OSPF restrictions, B–2
  OSPF, enabling, 1–14
  over Ethernet or FDDI, 1–5
  overview, 1–1–1–5
  peer-to-peer groups, 2–9, 3–9
  RIP restrictions, B–2
  routes, creating, 1–20
  sample configuration, 1–9–1–19
  setting the router’s internal IP address, 1–13
  setting up, 1–4

setting-up groups and static sessions, 1–20
static sessions, configuring, 1–20
TCP interoperability issues, B–3
WAN link, assigning an internet address to, 1–13
DLSw configuration commands
add, 2–3
sdlc, 2–3
tcp, 2–5
close-sap, 2–5
delete, 2–6
sdlc, 2–6
tcp, 2–6
disable, 2–6
auto-tcp-reconnect, 2–7, 3–8
dls, 2–7, 3–7
llc, 2–7, 3–7
sdlc, 2–7, 3–8
enable, 2–8
auto-tcp-reconnect, 2–8, 3–9
dls, 2–8, 3–8
llc, 2–8, 3–9
sdlc, 2–8, 3–9
exit, 2–22
help, 2–3
join-group, 2–9
leave-group, 2–10
list, 2–10
dls, 2–10
groups, 2–12
llc2 sap parameters, 2–13
open llc2 saps, 2–13
sdlc link stations, 2–14
tcp neighbors, 2–15
open-SAP, 2–15
set, 2–16
cache, 2–16
llc2, 2–16
mac, 2–18
maximum, 2–18
memory, 2–18
srb, 2–19
tcp, 2–21
timers, 2–19
DLSw group feature, and IBM 6611, B–2
DLSw monitoring commands
add, 3–4
sdlc, 3–4
tcp, 2–5, 3–5
close-sap, 3–6
delete, 3–6
sdlc, 3–6
tcp, 3–7
disable, 3–7
auto-tcp-reconnect, 2–7, 3–8
dls, 2–7, 3–7
llc, 2–7, 3–7
sdlc, 2–7, 3–8
enable, 3–8
auto-tcp-reconnect, 2–8, 3–9
dls, 2–8, 3–8
llc, 2–8, 3–9
sdlc, 2–8, 3–9
exit, 3–27
help, 3–3
join-group, 3–9
leave-group, 3–10
list, 3–11
dls, 3–11
dls cache all, 3–17

dls cache range, 3–18
dls global, 3–12
dls memory, 3–18
dls session destination, 3–15
dls session detail, 3–15
dls session ip, 3–16
dls session range, 3–16
dls session src, 3–17
dls session state, 3–17
dls sessions all, 3–13
dls sessions ban, 3–15
groups, 3–19
llc2 open, 3–19
llc2 sap parameters, 3–19
llc2 sessions all, 3–20
llc2 sessions range, 3–21
sdlc link, 3–21
sdlc sessions, 3–21
tcp config, 3–21
tcp sessions, 3–22
open-SAP, 3–22
set, 3–23
llc2, 3–23
maximum, 3–24
memory, 3–24
timers, 3–25
Dynamic routing, enabling for DLSw, 1–6

E

ELS messages, for BAN, enabling, 6–12
Encapsulation, using SDLC Relay, 9–2
Ethernet, configuring for DLSw, 1–5

F

Fault-tolerant BAN, configuring, 6–10
FDDI
BAN support for, 6–1
configuring for DLSw, 1–5
Frame Relay, configuring, for BAN, 6–6

G

Group feature, using, 1–8, 2–9, 3–9

I

IBM 6611 router, interoperating with, B–1
IP, configuring for DLSw, 1–6

L

Line parameters, for SDLC Relay, 9–6
Line speed, SDLC Relay, 9–6
List command, using, 1–10
LLC2 frames, bridging, 1–2

M

MIBs, DLSw MIBs supported, A–1
Monitoring commands
BAN, 7–1, 8–1
DLSw, 2–1, 3–1
SDLC, 4–1, 5–1
SDLC relay, 11–1
Monitoring environment, SDLC Relay, accessing, 11–2
Multipoint lines, and remote link stations, 1–24
multipoint links, configuring, 4–14

N

NetBIOS traffic, over DLSw, B–2
Non-volatile configuration memory, 2–1, 3–1

O

On-demand TCP sessions, setting up, 1–22
Opening SAPs, 1–21
  for BAN, 6–9

P

Peer-to-peer groups, adding, 2–9, 3–9
point-to-point links, configuring, 4–14
Primary and secondary data links, assigning, 9–6
Protocol spoofing, 1–3

R

Remote link station, role of, 4–9
Remote link stations, on multipoint lines, 1–24
RIP, enabling, 1–6
RIP/OSPF restrictions, on DLSw, B–2

S

Sample configuration
  DLSw, 1–9
    context diagram, 1–10
  SDLC Relay, 9–4
SAP filters
  creating, 1–6
  for LLC2 interfaces, 1–8
  implementing, 1–18
SAPs, commonly used, 2–15, 3–22
SDLC, used in the wide area, 1–1
SDLC commands
  clear
    link, 5–6
    remote-secondary, 5–6
  list
    link configuration, 5–8
    link counters, 5–8
    remote-secondary, name or address counters, 5–10
  set
    link role, 4–12
    link rts-hold, 5–14
    link snrm(e), 5–14
    remote-secondary max–packet, 4–15
    remote-secondary name, 4–15, 5–15
    remote-secondary receive window, 4–15
    remote-secondary receive-window, 5–15
    remote-secondary transmit window, 4–15
    remote-secondary transmit-window, 5–15
SDLC configuration commands
  add, 4–3
  exit, 4–15–4–17
  help, 4–3
  list
    link, 4–6
    remote-secondary, 4–8
  set, 4–9
    link clocking, 4–10

link duplex, 4–10
link encoding, 4–10
link frame-size, 4–11
link idle flag, 4–11
link idle mark, 4–11
link modulo, 4–11
link name, 4–12
link poll delay, 4–12
link poll retry, 4–12
link poll timeout, 4–12
link role, 4–12
link rts-hold, 4–13
link snrm, 4–13
link speed, 4–13
link transmit-delay, 4–13
link type, 4–14
link xid/test retry, 4–14
link xid/test timeout, 4–14
remote-secondary, 4–14–4–16
SDLC connections, support for, 4–2, 5–4
SDLC data links, and SRLY, 9–6
SDLC Interfaces, Configuring, 1–7
SDLC link role, setting, 4–12
SDLC link stations, adding, 1–8
SDLC monitoring commands
add, 5–5
clear, 5–6
delete, 4–4, 5–6
disable, 4–4, 5–7
enable, 4–5, 5–7
exit, 5–16–5–18
help, 5–5
list, 4–6, 5–8
remote-secondary, all, address or link station, 5–9
set, 5–12
link modulo, 5–12, 5–13
link poll delay, 5–13
link poll retry, 5–13
link poll timeout, 5–13
link role primary/negotiable, 5–13
link snrm, 5–14
link type, 5–14
link xid/test retry, 5–15
link xid/test timeout, 5–14
remote-secondary, 5–15–5–17
test, 5–16–5–18
SDLC Relay
adding a local port, 9–7
adding a remote port, 9–8
assigning group number, 9–6
cable type, 9–6
configuring, 9–3, 9–4
configuring second router for, 9–8
context diagram for, 9–4
diagram, 9–3, 9–5
end-station roles, 9–2
overview, 9–1
ports and groups, 9–1
primary and secondary stations, 9–2
protocols handled, 9–1
router roles, 9–5
sample configuration, 9–4
setting data-links, 9–5
setting serial line parameters, 9–6
SDLC Relay configuration commands
add
group, 10–3
local-port, 10–3
remote-port, 10–4

delete
group, 10–4
local-port, 10–5
remote-port, 10–5
disable, group, 10–5
enable, group, 10–6
exit, 10–8
help, 10–3
list
all, 10–7, 11–5
group, 10–8, 11–6
SDLC Relay monitoring commands
clear-port-statistics, 11–3
disable, group, 11–3
enable, group, 11–4
exit, 11–6
help, 11–3
list
all, 10–7, 11–5
group, 10–8, 11–6
SDLC secondary, limitations, 9–3
SDLC stations, defining, 1–21
Service Access Points, opening for BAN. *See* SAPs
Setting-up DLSw groups, 1–23
SRLY. *See* SDLC Relay
Statistics, displaying, 5–2
Status messages, BAN, 6–12

T

TCP, interoperability issues with DLSw, B–3
Terminated and bridged BAN, 6–9
Token Ring, configuring for DLSw, 1–5
Token Ring interfaces, adding, to DLSw configuration, 1–10

U

Using multiple BAN DLCIs, 6–10

W

WAN link
adding, for DLSw, 1–11
LAP-B over SDLC Relay, 9–3
shipping bit-oriented protocols over, 9–3

HOW TO ORDER ADDITIONAL DOCUMENTATION

DIRECT TELEPHONE ORDERS

In Continental USA
call 800–DIGITAL

In Canada
call 800–267–6215

In New Hampshire
Alaska or Hawaii
call 603–884–6660

In Puerto Rico
call 809–754–7575 x2012

ELECTRONIC ORDERS (U.S. ONLY)

Dial 800–234–1998 with any VT100 or VT200
compatible terminal and a 1200 baud modem.
If you need assistance, call 1–800–DIGITAL.

DIRECT MAIL ORDERS (U.S. AND PUERTO RICO*)

U. S. SOFTWARE SUPPLY BUSINESS
DIGITAL EQUIPMENT CORPORATION
10 Cotton Road
Nashua, New Hampshire 03063–1260

DIRECT MAIL ORDERS (Canada)

DIGITAL EQUIPMENT OF CANADA LTD.
940 Belfast Road
Ottawa, Ontario, Canada K1G 4C2
Attn: A&SG Business Manager

INTERNATIONAL

DIGITAL
EQUIPMENT CORPORATION
A&SG Business Manager
c/o Digital's local subsidiary
or approved distributor

Internal orders should be placed through the Software Services Business (SSB)
Digital Equipment Corporation, Westminster, Massachusetts 01473

*Any prepaid order from Puerto Rico must be placed
with the Local Digital Subsidiary:
809–754–7575 x2012

Distributed Routing Software
System Networks Architecture Guide
XX–XXXXX–XX

READER'S COMMENTS

What do you think of this manual? Your comments and suggestions will help us to improve the quality and usefulness of our publications.

Please rate this manual:

	Poor				Excellent
Accuracy	1	2	3	4	5
Readability	1	2	3	4	5
Examples	1	2	3	4	5
Organization	1	2	3	4	5
Completeness	1	2	3	4	5

Did you find errors in this manual? If so, please specify the error(s) and page number(s).

General comments:

Suggestions for improvement:

Name _____ Date _____

Title _____ Department _____

Company _____ Street _____

City _____ State/Country _____ Zip Code _____

DO NOT CUT – FOLD HERE AND TAPE

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY LABEL
FIRST CLASS PERMIT NO. 33 MAYNARD MASS.

POSTAGE WILL BE PAID BY ADDRESSEE

digital™

Shared Engineering Services

550 King Street
Littleton, MA 01460–1289

DO NOT CUT – FOLD HERE