Teldat Router

Data Link Switching (DLSw) Protocol

Doc. *DM516-I* Rev. *8.30*

April, 2000

INDEX

Chapter 1
Using the DLSw Protocol

1. About DLSw

The Data Link Switching (DLSw) protocol is 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.

1.1. How DLSw Works

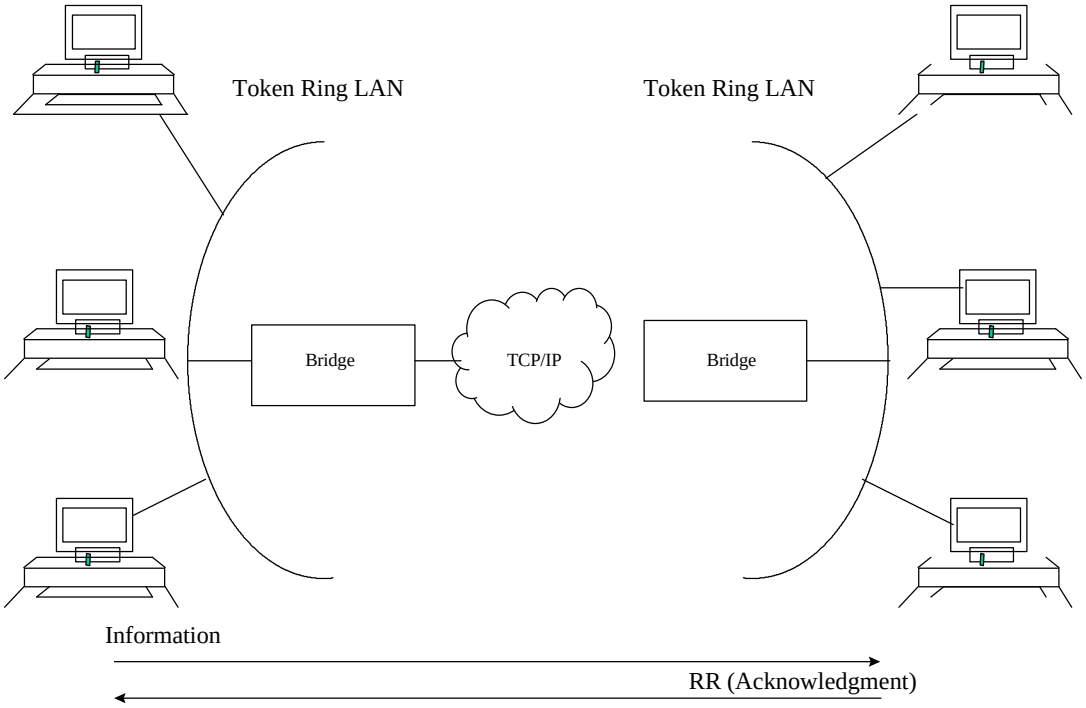
LLC2 and SDLC are connection-oriented protocols, designed to function well on LANs. DLSw gives these protocols the dynamic characteristics of routable protocols. Equally important, DLSw preserves the end-to-end reliability and control features that make LLC2 and SDLC effective for communication on the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

a) Problems Inherent in the Bridging Solution

The following Figure illustrates the traditional approach to bridging LLC2 and SDLC frames across WAN links. The problem with this approach is that network delays occur much more frequently in the WAN 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 WAN. 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 re-transmits data that is not lost, but delayed, LLC2 end stations may end up receiving duplicate data. While this would seem 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 WAN link.

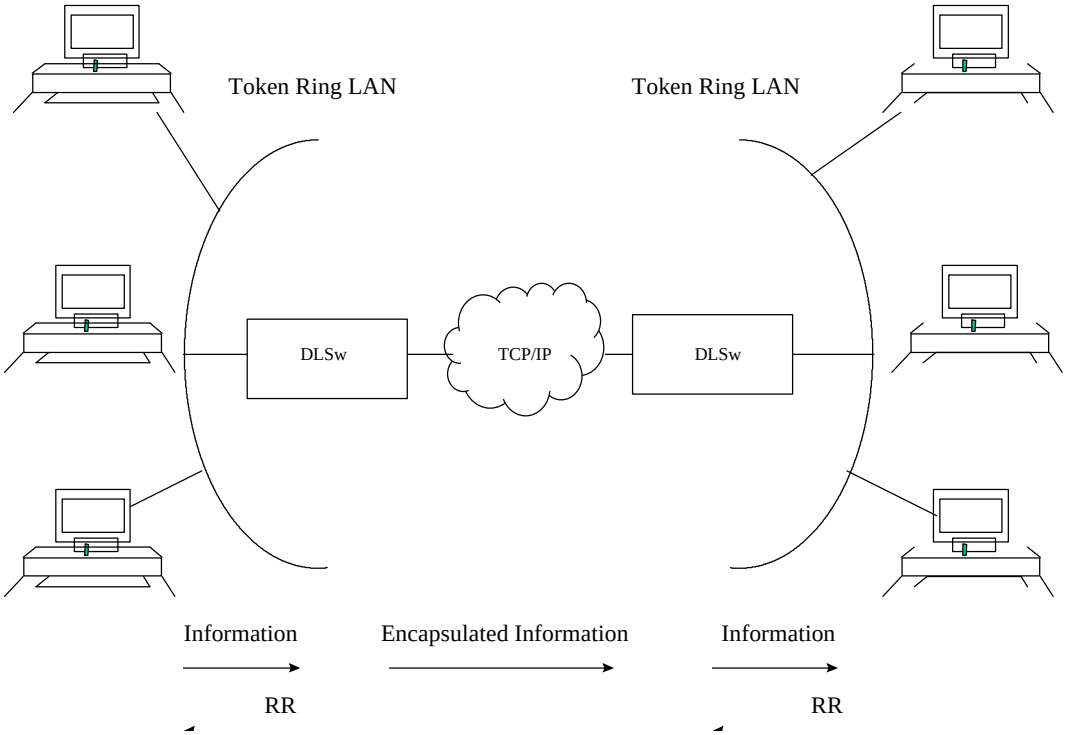


Traditional Approach to Bridging Across WAN Links

b) 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 acknowledgments to the sending station. This acknowledgment tells the sender that data previously transmitted have been received, and prevents the station from re-transmitting.

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 frame headers, determines the address of data's intended recipient, and establishes a new LLC2 connection with that end station. The following figure illustrates this relationship between two DLSw neighbor routers.

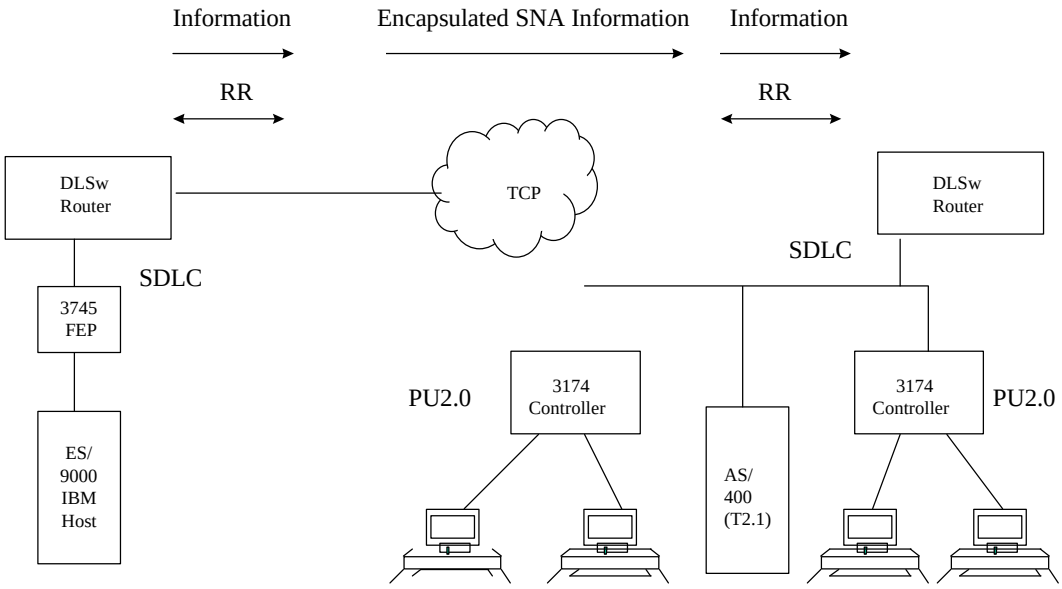


Data Link Switching Over the Wide Area Network

1.2. SDLC Data Link Support

In addition to LAN data link support for SNA (LLC2) and NetBIOS, DLSw supports SDLC data link termination for SDLC-attached SNA devices. You can configure the router to act in either a primary or a secondary local link role. Support for SNA data link type is independent of the corresponding neighbor DLSw router; that is, the local router can have SDLC devices attached and the remote router's SNA devices can be on a Token Ring (LLC2).

> ***WARNING!!***
>
> ***Consult the SDLC link features in the Dm506-I manual.***



SDLC Support

a) *Primary and Secondary Link Roles*

In section 1.2 figure, if the DLSw router is in the primary link role, the router polls downstream SNA PU2.0 or T2.1 devices such as IBM 3174 cluster controllers or the AS/400, respectively. If the router is in the secondary link role, the adjacent (primary) station polls the router. An example of a local secondary link configuration is where the SDLC link connects the router to a Front End Processor (FEP), such as 3745. Another example is where the router is SDLC-attached to a T2.1/APPN device, such as an AS/400, and the T2.1 device acts as a primary link station.

You can configure the type of SNA node (PU2 or T2.1) for each SDLC link station. In addition to the link role consideration, the router uses the node type to determine whether or not to forward XID frames to the adjacent physical device.

For example, a local station configured with a PU2 node type on a local primary link does not forward NXID frames it receives to the actual attached device. Instead, the router generates the appropriate XID0 response using the configured IDNUM and IDBLK values directly. This feature isolates the actual physical device configuration from the IBM host's configuration parameters, and permits, for example, transparent substitution of a remote SDLC device for an existing local Token Ring configuration.

With T2.1 SDLC devices, on the other hand, the router explicitly forwards all XID frames end-to-end, allowing XID3 parameter negotiation support. Mixed node types may be supported on a single multidrop physical link.

b) *Negotiable Link Role*

In addition, you can configure SDLC link role as negotiable. In section 1.2 figure, the router allows SDLC XID frames to flow in both directions until the router determines the role of its adjacent link station, after which the local role dynamically resolves to the appropriate value. This feature is intended to primarily support end-to-end T2.1/APPN traffic, where the respective end station resolves its role dynamically, using XID3 frames. The router does not support dynamic role negotiation on multipoint links or dynamic T2.1 link station address resolution.

If you configure respective SNA T2.1 end stations for role negotiation, but configure the router with a non-negotiable link role (the role is primary or secondary), the router attempts to "bias" the role negotiation protocol such that the local link station role is resolved accordingly.

1.3. 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 QLLC, LLC2, NetBIOS and SDLC traffic at the local LAN.
- DLSw reduces WAN network overhead by eliminating the need to transmit Receive Ready (RRs) acknowledgments over the WAN. DLSw confines the RRs to the LANs that are local to each DLSw router.
- DLSw provides flow and congestion control, and broadcast control, and broadcast control of search packets, between DLSw routers and their attached end stations.
- DLSw increases Source Routing Bridging (SRB) hop-count limits.
- DLSw allows QLLC, LLC2 and SDLC protocol conversion.
- DLSw supports NetBIOS traffic.

2. Setting Up DLSw

The following sections explain the procedures to follow to set up DLSw and cover the following subjects.

- Configuration Requirements
- Configuring Adaptive Source Route Bridging (ASRT)
- Configuring IP
- Configuring X.25 node (QLLC)
- Configuring SDLC Interfaces
- Configuring QLLC links
- Configuring DLSw protocol

In addition, a sample DLSw protocol configuration with explanatory notes is also included.

2.1. Configuration Requirements

Teldat Router supports DLSw over IEEE 802.5 Token Ring, SDLC, QLLC, Ethernet, and FDDI. To use DLSw, you must perform the following actions:

- Configure ASRT
- Configure IP
- Configure OSPF and MOSPF, as needed
- Configure X.25 node (QLLC)
- Configure SDLC devices
- Configure QLLC links
- 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.

a) Configuring Adaptive Source Bridging (ASRT) for DLSw

Since the DLSw router appears as a bridge to attached end stations, you need to configure source route bridging. Note that in SDLC-only and/or QLLC-only configurations, you do not need to set up ASRT. 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 that DLSw will use. 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 will be prompted for an SRB segment number.

- For Ethernet or FDDI interfaces:

Enter the **ENABLE TRANSPARENT** command to enable transparent bridging on the bridging 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 will both bridge and forward the packets it receives.

   To create a SAP filter, enter the **ADD PROT-FILTER DSAP 4** command at the ASRT config> prompt.

   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 using the **LIST BRIDGE** command. You do not have to do this, but is a good idea to check the bridge configuration before proceeding.
7. Enable the DLSw protocol using the **ENABLE DLS** command.

b) *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.

   - To enable RIP:

   Enter the **PROTOCOL RIP** command from the Config> prompt. This brings you to the RIP Config> prompt. Enter **ENABLE RIP** command to enable rip.

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.***

c) 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 will be prompted for an interface number.
2. Use the **NETWORK** command at the Config> prompt to enter the SDLC configuration process. The router prompts you for an interface number.
3. Set the link speed (optional). If you are using internal clocking, use the **SET LINK SPEED** command to choose the clock speed for this line.
4. Set the encoding (NZR/NRZI) to match the attached end station's configuration.
5. Set duplex to full or half to match the attached end station's configuration.
6. When you have finished, use the **LIST LINK** command to verify the SDLC interface configuration.
7. Use the SDLC stations that you configure in DLSw or use the **ADD REMOTE** command to explicitly set up SDLC stations in the following situations:
   - The following defaults for SDLC stations are not satisfactory:

     ⇒ Maximum BTU is maximum allowable by interface.

     ⇒ Tx and Rx Windows are 7 for MOD 8, 127 for MOD 128.
   - The SNA devices on the interface are of mixed node types.

     If you do not explicitly add SDLC, the router assumes the following:
   - The stations are of type PU2 if the router's link role is primary.
   - The stations are of type T2.1 if the routers link role is NEGOTIABLE.
8. Change the link role using the **SET LINK ROLE** command if PRIMARY is not satisfactory.

d) Configuring QLLC links

So the DLSw configuration can support QLLC links, you have to configure the X.25 node.

e) 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. If your configuration is handling LLC2 or NetBIOS traffic, enter 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 (SRB) 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. To open commonly used SNA SAPs (0, 4, 8, and C), specify

SNA. To open the NetBIOS SAP, specify NB or F0. To open the LNM SAP, specify LNM or F4.

5. Use the **ADD TCP** command to add the IP address of each DLSw neighbor. You can also make this connection using multicast OSPF using the **JOIN-GROUP** command.

> ***Note: A router can only participate in a group if its neighbor router is a 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. For your DLSw configuration to support SDLC, you must add an SDLC link station using the **ADD SDLC** command.

   Adding SDLC link stations requires knowledge of the device link station address, the optional Node ID field information (IDNUM and IDBLK), and the source and destination MAC addresses and SAPs for mapping to the corresponding remote SNA device.

7. So the DLSw configuration supports QLLC you have to aggregate a station by using the **ADD QLLC** command. You also must configure the X.25 node.

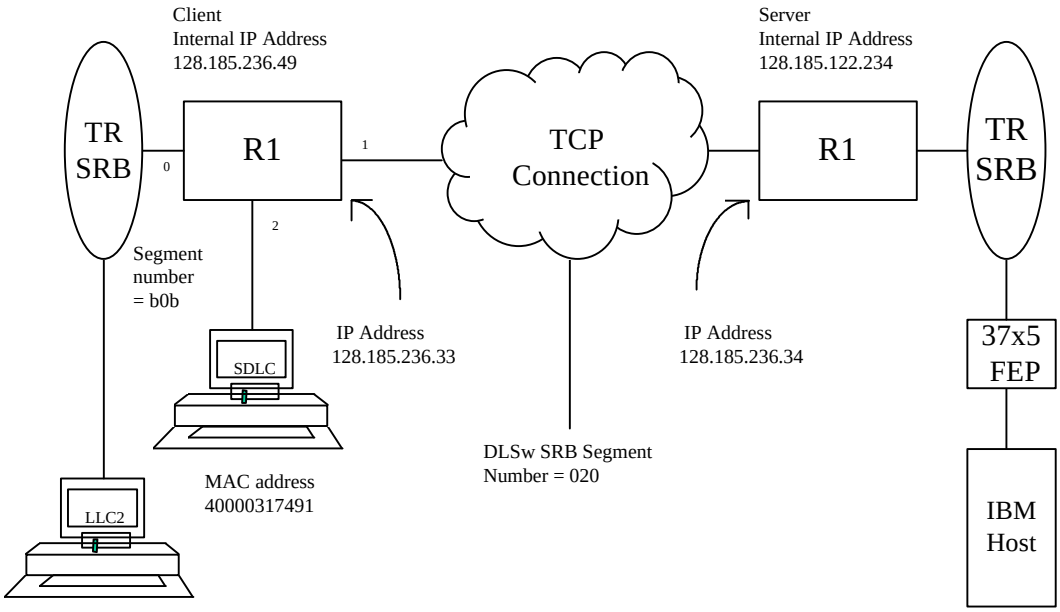
3. Sample DLSw Configuration

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

3.1. Context Diagram

The example is based on the Information shown in the following figure.

Context diagram for DLSw Configuration



The DLSw router being configured (R1 in the diagram) will support one LLC and one SDLC connection to its DLSw neighbor (R2). The TCP connection between the two routers is over a Frame Relay line.

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.

3.2. Adding Physical Devices

The example that follows shows the default configuration for routers. Notice that in the sample screen output shown here, a Token Ring device is added as interface 0, and an SDLC device is added as interface 2. Interface 1 is configured for the TCP connection with a DLSw neighbor router (R2 in the figure).

```
Config>SET DATA-LINK FRAME-RELAY 1
Config>SET DATA-LINK SDLC 2
```

After adding devices, using the **LIST DEVICE** command you can list the devices to verify that they are assigned to the appropriate router interfaces.

Once you have checked the interface list, you need to save the configuration and restart the router.

```
Config>SAVE
Save Configuration [n]? yes
Saving Configuration…OK
Config>                                                    (Push Control-P)
* RESTART
Are you sure to restart the system? (Yes/No)?y
Read disk configuration
*
```

a) Add a Token Ring Device

Next, configure Token Ring. The **LIST** command shown here is not required at this point, or at any other time during configuration of the router.

```
Config (only)>NETWORK 0
Token-Ring interface configuration
TKR config>

TKR config>SPEED 16
TKR config>MEDIA STP

TKR config>LIST
Token-Ring configuration
Packet size (INFO field):     2052
Speed:                        16 Mb/sec
Media:                        Shielded

RIF Aging Timer:              120
Source Routing:               Enabled
MAC Address:                  00:00:00:00:00:00
TKR config>

TKR config>EXIT
```

The first port (interface 1) is used for the WAN (TCP/IP) link (see the figure of 3.1 Context Diagram section). The data link selected for the WAN is Frame Relay. Other possibilities are PPP and X.25.

b) Add Frame Relay interface

In order to support TCP/IP over Frame Relay you need to configure the Frame Relay devices in the DLSw configuration.

The Frame Relay configuration is accessed through the **NETWORK** command and the interface number that the Frame Relay devices has been assigned to (case 1).

```
Config>NETWORK 1
Frame Relay interface configuration.
FR Config>
```

In this example, a permanent channel will be configured for the traffic (in this case it is 16).

```
FR Config>ADD PVC-PERMANENT-CIRCUIT
Circuit number [16]?16
Outgoing Committed Information Rate (CIR) in bps [16000]?
Outgoing Committed Burst Size (Bc) in bits [16000]?
Outgoing Excess Burst Size (Be) in bits [0]?
Envrypt Information? [No]:(Yes/No)?
Assign circuit name[]? EJEMPLO1
Inverse ARP (0-Default, 1-Off, 2-On): [0]?
FR Config>
```

Following this, the IP address from the other end of the channel will be configured which in this case is the R2 router. In this example, we assume that the devices are connected without any other routers in between.

```
FR Config>ADD PROTOCOL-ADDRESS
IP Address [0.0.0.0]?128.185.236.34
Circuit number [16]?16
FR Config>
```

You can consult the Frame Relay link configuration through the **LIST ALL** command.

c) *Add an SDLC Device*

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 has been assigned (in this case, 2).

```
Config (only)>NETWORK 2
SDLC user configuration
SDLC 2 Config>
```

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:                 INTERNAL   Frame Size:   2048
Speed:                    19200      Cable:        DCE

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
SDLC 2 Config>
```

Similarly, when you wish to configure a WAN link, you must modify the clock type and the link speed for the SDLC device.

```
SDLC 2 Config>SET LINK SPEED 9600
SDLC 2 Config>EXIT
```

Note: You can use the SDLC ADD REMOTE command in order to ignore any of the configured SDLC default link stations.

3.3. Configuring Protocols

In order to execute DLSw you must configure the IP, OSPF (or RIP), ASRT and DLSw protocols.

a) Configure IP protocol

This example shows the creation of a minimal IP configuration.
To configure IP, begin by entering the **PROTOCOL IP** command at the Config> prompt.

```
Config>PROTOCOL IP
Internet protocol user configuration
IP config>
```

The **LIST** command displays the default IP configuration.

```
IP config>LIST ALL
Interface addresses
IP addresses for each interface:
   Intf   0                                        IP disabled on this interface
   Intf   1                                        IP disabled on this interface
   Intf   2                                        IP disabled on this interface
   Intf   3                                        IP disabled on this interface
Routing
Protocols

Directed broadcasts: enabled
RIP: enabled
OSPF: disabled
Per-packet-multipath: disabled
IP-classless: disabled

IP config>
```

- *Assign an Internet address to a WAN link*

Add an Internet address through the **ADD ADDRESS** command, and assign it to one of the interfaces associated to 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
IP config>
```

- *Configure an Internal IP Address*

The internal IP address must be configured. This is the address that remote DLSw routers use to connect to the router you are configuring.

```
IP config>SET INTERNAL-IP-ADDRESS
Internal IP address [0.0.0.0]?128.185.236.49
IP config>
```

By using the **LIST** command again, the newly added information can be displayed.

```
IP config>LIST ALL
Interface adresses
IP addresses for each interface:
   Intf   0                                        IP disabled on this interface
   Intf   1   128.185.236.49   255.255.255.0   NETWORK broadcast, fill 0
   Intf   2                                        IP disabled on this interface
   Intf   3                                        IP disabled on this interface
Internal IP address: 128.185.236.49
Routing
Protocols

Directed broadcasts: enabled
RIP: enabled
OSPF: disabled
Per-packet-multipath: disabled
IP-classless: disabled
IP config>
```

Finally you can return to the previous prompt level through the **EXIT** command.

```
IP config>EXIT
Config>
```

b) Configuring OSPF or RIP protocol

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

To configure the OSPF protocol, begin by entering the **PROTOCOL OSPF** command at the Config> prompt.

```
Config>PROTOCOL OSPF
Open SPF-Based Routing Protocol configuration console
OSPF Config>
```

The **LIST ALL** command displays the default OSPF configuration.

```
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
OSPF Config>
```

- *Enable OSPF*

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

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

- *Enable Multicast OSPF as needed*

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

```
OSPF Config> ENABLE MULTICAST
Inter-area multicasting enabled? [No]?No
OSPF Config>
```

- *Define the Interfaces that use OSPF*

You must execute the **SET INTERFACE** command for every physical IP interface that will use OSPF. This example assumes that the backbone is the OSPF area (0.0.0.0). At this point, only one IP interface has been defined.

```
OSPF Config>SET INTERFACE 128.185.236.33
Attaches to area [0.0.0.0]? 0.0.0.1
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 unicast? [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 has been configured. To see what has changed in the configuration, compare this display with the display of the default OSPF configuration shown in section 3.3.b) Configuring OSPF or RIP protocol.

```
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:     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   Trns Dly   Pri   Hello  Dead
0.0.0.0      0.0.0.0   1      5       1          1     10     40

          --Multicast parameters--
IP address       MCForward   DLUnicast   IGMPPoll   IGMPtimeout
128.185.236.33   ENA         DIS         60         180
OSPF Config>
```

Finally you can return to the previous prompt level through the **EXIT** command.

```
OSPF Config>EXIT
Config>
```

c) Configuring ASRT protocol

DLSw requires SRB (Source Route Bridging) to run correctly 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 on a Token Ring connection to the DLSw router. Begin by enabling the bridge as shown:

```
Config>PROTOCOL ASRT
-- ASRT Bridge user configuration --
ASRT config>ENABLE BRIDGE
```

Disable Transparent Bridging

The **LIST PORT** command shows that the default port is configured for Transparent Bridging.

```
ASRT config>LIST PORT
Port Number[-1]?
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
-------------------------------------------------------------------------------
ASRT config>
```

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 Token Ring (see figure in section 3.1 Context Diagram).

```
ASRT config>DISABLE TRANSPARENT
Port Number [1]?
ASRT config>
```

Enable SRB (Source Route Bridging)

Next, enable SRB (Source Route Bridging) for the Token Ring port as shown:

```
ASRT config>ENABLE SOURCE-ROUTING
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 SRB (Source Route Bridging) device, such as Token Ring. In this example (see figure in section 3.1 Context Diagram) 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
```

Through the **LIST BRIDGE** command you can confirm that you have configured the ASRT protocol correctly.

```
ASRT config>LIST BRIDGE

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

Bridge:            Enabled      Bridge behavior:   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:   1470
      +-------------------------------------------------------------------+
------------------|    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   Behavior:   SRB Only   STP:   Enabled
ASRT config>
```

d) *Implementing Protocol Filtering*

This is an important step that is often neglected when configuring DLSw.

Since DLSw, rather than bridging, forwards traffic on SAPs (Service Access Points) 04, 08, 0C, add a special protocol filter to the bridging set up.

> ***Note: You only need to implement the filter described here if you configure parallel bridging and DLSw. Such is not the case in this example. The procedure for creating an SAP filter is provided for reference purposes only.***

The idea of the filter is to prevent the bridge from forwarding, on other ports, packets that only DLSw should handle.

The **ADD PROT-FILTER DSAP 4** command 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/No)? Y
ASRT config>LIST PROT-FILTER
Protocol Class:DSAP
Protocol Type:   04
Protocol State:  FILTERED
Port Map:        1
=========================
No ETHER type Filter Records Associated
No SNAP Filter Records Associated
ASRT config>
```

Once the filtering you need is in place, exit the ASRT configuration module using the **EXIT** command.

```
ASRT config>EXIT
```

e) Configuring DLSw protocol

The final step involves configuring the DLSw protocol.

To do this you begin by entering the **PROTOCOL DLSW** command from the Config> prompt.

```
Config> PROTOCOL DLSW
DLSw protocol user configuration
DLSw config>
```

The **LIST** DLSW command shows the default configuration.

```
DLSw config>LIST DLSW
DLSw is                              ENABLED
LLC2 send Disconnect is              ENABLED
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
NetBIOS UI-frame memory allotment    40960

Database age timer                   1200   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
Neighbor priority wait timer         2.0    seconds
DLSw config>
```

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 DLSW
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 a neighbor DLSw router. This example defines both a group and a static (explicitly configured) TCP session.

- *Using the JOIN-GROUP command*

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

This command executed for R1 (see section 3.1 Context Diagram), designates this DLSw router as a Client in group 1. To join this group, R2 has to be added as a Server in group 1.

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

```
DLSw config>LIST GROUPS
Group   Role     Xmit Bufsize   Rcv Bufsize   Max Segsize   Keepalive   Priority
1       CLIENT   5120           5120          1024          DISABLED    MEDIUM
DLSw config>
```

- *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 section 3.1 Context Diagram). 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]?
Receive Buffer Size (Decimal)[5120]?
Maximum Segment Size (Decimal)[1024]?
Enable/Disable Keepalive (E/D)[D]?
Neighbor Priority (H/M/L)[M]?
DLSw config>
```

```
DLSw config>LIST TCP
Neighbor          Xmit Bufsize   Rcv Bufsize   Max Segsize   Keepalive   Priority
---------------   ------------   -----------   -----------   ---------   ---------
128.185.122.234   5120           5120          1024          DISABLED    MEDIUM
DLSw config>
```

- *Define each SDLC link station*

You must define each SDLC link station as shown:

```
DLSw config>ADD SDLC
Interface #[0]? 2
SDLC Address[c1]?
Local MAC Address [40:23:11:12:02:c1]? 40:00:00:31:74:91
Idblk in Hex (0-0xfff)[0]? 017
Idnum in Hex (0-0xfffff)[0]? A0021
LLC Local SAP in hex[4]?
LLC Remote SAP in hex[0]? 4
Remote MAC Address [00:00:00:00:00:00]? 40:00:00:00:00:02
DLSw config>
```

```
DLSw config>LIST SDLC
Interface #, or 'ALL'[0]? ALL
Net   Addr   Status    Idblk   Idnum   Local SAP/MAC          Remote SAP/MAC
2     C1     Enabled   017     A0021   04/40:00:00:31:74:91   04/40:00:00:00:00:02
DLSw config>
```

- *Open SAPs*

Next, open SAPs on each bridging interface that performs DLSw switching. SAP numbers 0, 4, 8 and C are commonly used SNA SAPs.

```
DLSw config>OPEN-SAP
Interface # [0]?
Enter SAP in hex (range 0-F4), 'SNA', 'NB' or 'LNM' [4]? SNA
SAPs 0 4 8 c opened on interface 0
DLSw config>
```

```
DLSw config>LIST OPEN
Interface   SAP
0           0
0           4
0           8
0           c
DLSw config>
```

Following is the DLSw display after configuring. Please note that the router automatically configures the SDLC MAC address when the first SDLC link station is added.

```
DLSw config>LIST DLSW
DLSw is                              ENABLED
LLC2 send Disconnect is              ENABLED
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
NetBIOS UI-frame memory allotment    40960

Database age timer                   1200   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
Neighbor priority wait timer         2.0    seconds
DLSw config>
```

When you have finished configuring DLSw, exit the DLSw configuration environment through the **EXIT** command and restart the router.

```
DLSw config>EXIT
Config>SAVE
Save Configuration [n]? Yes
Saving Configuration…OK
Config> (Pulsar Ctrl-P)
*RESTART
Are you sure to restart the system? (Yes/No)? yes
Read disk configuration
*
```

Chapter 2
Configuring the DLSw Protocol

1. About DLSw Configuration 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.

2. Accessing the DLSw Configuration Environment

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

To enter the configuration environment, type **PROCESS 4**, or just **P 4**. This brings you to the Config> prompt as shown here:

Example:

```
*PROCESS 4
User configuration
Config>
```

If the Config> prompt does not appear immediately, press Ctrl-P again.

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

Example:

```
Config>PROTOCOL DLS
DLSw protocol user configuration
DLSw config>
```

3. DLSw Configuration Commands

Enter DLSw configuration commands at the DLSw config> prompt.

Command	Function
?(HELP)	Lists the configuration commands or lists any parameters associated with that command
ADD	Adds an SDLC link station, QLLC or a TCP neighbor IP address.
BAN	Displays the BAN prompt (Boundary Access Node).
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 or QLLC link stations and TCP connections.
DISABLE	Disables the DLSw protocol, Auto-TCP-Reconnect, SDLC, QLLC 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, QLLC, SAPs, TCP connections, and DLSw groups.
NETBIOS	Displays the NetBIOS prompt.
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.

The letters written in **bold** are the minimum number of characters that can be written in order to make the command effective.

3.1. ? (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:

```
DLSw config>?
```

Example:

```
DLSw config>?
ADD
BAN
CLOSE-SAP
DELETE
DISABLE
ENABLE
JOIN-GROUP
LEAVE-GROUP
LIST
NETBIOS
OPEN-SAP
SET
EXIT
DLSw config>
```

3.2. ADD

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

Syntax:

```
DLSw config>ADD
QLLC
SDLC
TCP
```

a) *ADD QLLC*

Adds information specifically for adding a QLLC link station. For each QLLC session you must add a QLLC station.

Example:

```
DLSw config>ADD QLLC
Local MAC Address []? 40:10:00:20:00:01
LLC Local SAP in hex[4]?
LLC Remote SAP in hex[0]? 4
Remote MAC Address [00:00:00:00:00:00]? 40:00:00:00:00:02
QLLC Address[ff]?
Local NUA ('X' admitted)?
Remote station NUA ('X' admitted)? 12341234
Remote station alternate NUA ('X' no alternate)?
DLSw config>
```

This meaning of each field is the following:

Local MAC Address	MAC address for the QLLC physical unit.
LLC Local SAP in hex	Identifies the station in the DLSw domain.
LLC Remote SAP in hex	Defines the Service Access Port (SAP) to be used when on activating the QLLC connection a connection is automatically tried.
Remote MAC Address	This is the remote station's MAC address you wish to connect to. The MAC address is in Token Ring format (non canonical format). This holds true even if the remote is in Ethernet. Leaving this address with all "0"'s means that outgoing calls are permitted from all the stations which wish to connect to the source address programmed in this station. Incoming X.25 calls are not admitted in this station.

QLLC Address	Address to use in the QLLC messages. This is a hexadecimal value between 00 and FE. If FF is programmed the session will use FF and learn the address from the remote QLLC station.
Local NUA	X.25 network number identifying the local station. This number discriminates the possible connections in the incoming calls. In outgoing calls this is sent in the call packets, should there be any wildcards ('X') it is not sent.
Remote station NUA	X.25 network number identifying the remote QLLC station. This number discriminates the possible connections in the incoming calls. Should there be any wildcards outgoing calls are not permitted.
Remote station alt. NUA	If there is a remote network number without 'X', an alternative NUA is requested for outgoing calls. If there are any 'X' wildcards, the alternative is not used.

b) ADD SDLC

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

The source and destination MAC addresses and SAPs are mandatory and must be correct for a DLSw connection to take place. If the local devices are to communicate with remote SNA devices on an SNA LAN, such as Token Ring, then the SAPs must correspond to those in use on the remote LAN. However, if the local SDLC devices are to communicate with remote SNA devices that are attached by an SDLC data link, then the MAC addresses and SAPs are arbitrary, provided they are legal values. In this case, the MAC addresses and SAPs must logically map to the reverse source and destination addresses at the remote router.

In SDLC-to-SDLC configurations, the destination SAP (DSAP) of the primary link role router has special significance. If you set it to zero, it designates that a successful SDLC protocol handshake with the adjacent devices should not generate a DLSw connection (CANUREACH). For PU2 (non-negotiable) links with each router connected via an SDLC interface, set the DSAP of the local primary router to zero. This prevents unnecessary DLSw circuit startups from occurring. Otherwise, the local primary router attempts a DLSw CANUREACH connection to the local secondary router, but since the secondary router cannot itself activate the data link to the adjacent SDLC primary station, the connection is guaranteed to fail.

Example:

```
DLSw config>ADD SDLC
Interface #[0]? 2
SDLC Address[c1]?
Local MAC Address [40:23:11:12:02:c1]? 40:00:00:31:74:91
Idblk in Hex (0-0xfff)[0]? 017
Idnum in Hex (0-0xfffff)[0]? A0021
LLC Local SAP in hex[4]?
LLC Remote SAP in hex[0]? 4
Remote MAC Address [00:00:00:00:00:00]? 40:00:00:00:00:02
DLSw config>
```

The meaning of each field is:

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.
Local 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 will use Idblk for PUs on switches 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 will 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 Local SAP in hex	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 Remote SAP in hex	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.
Remote 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.

c) ADD 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:

```
DLSw config>ADD TCP
Enter the DLSw neighbor IP Address [0.0.0.0]?128.185.14.1
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive ? (E/D) - [D] ?
Neighbor Priority (H/M/L) [M]?
DLSw config>
```

The meaning of each field is:

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.
Receive Buffer Size	The size of the packet receive buffer between 1024 and 32768. The default size if 5120.

Maximum Segment Size	The maximum size of the TCP segment between 1024 and 16384. The default size is 1024.
Enable/Disable Keepalive (A/D)	Indicates whether you want the DLSw neighbor to send link keepalive messages. The default is D (Disable).
Neighbor Priority	Allows you to specify the neighbor priority as either High, Medium or Low. DLSw uses this parameter to determine which DLSw neighbor to choose when multiple neighbors can reach a target station.

3.3. BAN

Use the **BAN** command to display the Boundary Access Node configuration prompt.

Syntax:

```
DLSw config>BAN
```

Example:

```
DLSw config>BAN
Boundary Access Node user Configuration
BAN config>
```

3.4. 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:

```
DLSw config>CLOSE-SAP
```

Example:

```
DLSw config>CLOSE-SAP
Interface # [0]?
Enter SAP in hex (range 0-F4), 'SNA', 'NB' or 'LNM' [4]? SNA
SAPs 0 4 8 c closed on interface 0
Closing SAP 0 disables all SNA DLSw function on interface 0
DLSw config>
```

The meaning of each field is:

Interface #	The interface number used by the open SAP.
SAP in hex	You can enter SAPs individually in hexadecimal (with values ranging between 0 and F4). The SAP must be an EVEN number. You can also enter SNA, NB (NetBIOS) or LNM. • SNA closes SAPs 0, 4, 8 and C • NB closes SAP F0 for NetBIOS • LNM closes SAP F4

3.5. DELETE

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

Syntax:

```
DLSw config>DELETE ?
QLLC
SDLC
TCP
```

a) DELETE QLLC

Deletes a specified QLLC station from the list of stations to which the DLSw can connect.

Example:

```
DLSw config>DELETE QLLC
Local MAC Address []? 11:11:11:11:11:11
Record deleted
DLSw config>
```

Local MAC Address MAC address assigned to the station you wish to delete.

b) DELETE SDLC

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

Example:

```
DLSw config>DELETE SDLC
Interface # [0]? 2
SDLC Address [C1]?
Record deleted
DLSw config>
```

The meaning of each field is:

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.

c) DELETE TCP

Removes the IP address of the DLSw neighbor to which you are making the TCP connection.

Example:

```
DLSw config>DELETE TCP
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.14.1
DLSw config>
```

3.6. DISABLE

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

Syntax:

```
DLSw config>DISABLE ?
AUTO-TCP-RECONNECT
DLSW
LLC
QLLC
SDLC
```

a) DISABLE AUTO-TCP-RECONNECT

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

Example:

```
DLSw config>DISABLE AUTO-TCP-RECONNECT
DLSw config>
```

b) DISABLE DLSW

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

Example:

```
DLSw config>DISABLE DLSW
DLSw config>
```

c) DISABLE 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:

```
DLSw config>DISABLE LLC
DLSw config>
```

d) DISABLE QLLC

Prevents DLSw connections to the specified QLLC link station.

Example:

```
DLSw config>DISABLE QLLC
Local MAC Address []? 40:11:11:10:00:00
Record updated
DLSw config>
```

e) DISABLE SDLC

Prevents DLSw connections to the specified SDLC link station.

Example:

```
DLSw config>DISABLE SDLC
Interface # [0]? 2
SDLC Address [C1]?
Record updated
DLSw config>
```

3.7. ENABLE

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

Syntax:

```
DLSw config>ENABLE ?
AUTO-TCP-RECONNECT
DLSW
LLC
QLLC
SDLC
```

a) ENABLE AUTO-TCP-RECONNECT

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

Example:

```
DLSw config>ENABLE AUTO-TCP-RECONNECT
DLSw>
```

b) ENABLE DLSW

Enables DLSw operation on the router.

Example:

```
DLSw config>ENABLE DLSW
DLSw config>
```

c) ENABLE LLC

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

Example:

```
DLSw config>ENABLE LLC
DLSw config>
```

d) ENABLE QLLC

Enables DLSw connections for specified QLLC station.

Example:

```
DLSw config>ENABLE QLLC
Local MAC Address []? 40:11:11:10:00:00
Record updated
DLSw config>
```

e) ENABLE SDLC

Enables DLSw connections to the specified SDLC link station.

Example:

```
DLSw config>ENABLE SDLC
Interface # [0]? 1
SDLC Address [C1]?
Record updated
DLSw config>
```

3.8. 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 would be 225.0.1.2.

Syntax:

```
DLSw config>JOIN-GROUP
```

Example:

```
DLSw config>JOIN-GROUP
Group ID (1-64 Decimal)[1]? 2
Client/Server or Peer Group Member (C/S/P)-[C]?
Transmit Buffer Size (Decimal)[5120]?
Receive Buffer Size (Decimal)[5120]?
Maximum Segment Size (Decimal)[1024]?
Enable/Disable Keepalive (E/D)[D]?
Neighbor Priority (H/M/L)[M]?
DLSw config>
```

The meaning of each field is:

Group ID	The number of the group that you want this router to join.
Client/Server or Peer 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.
Receive Buffer size	The size of the packet receive buffer between 1024 and 32768. The default size is 5.120.
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)
Neighbor Priority	Specifies the neighbor priority as High, Medium or Low. DLSw uses this parameter to determine which DLSw neighbor to choose when multiple neighbors can reach a target station.

3.9. LEAVE-GROUP

Use the **LEAVE-GROUP** command to remove the router from any specified DLSw groups that were configured with the **JOIN-GROUP** command. This command do not affect existing TCP connections belonging to the specified group.

Syntax:

```
DLSw config>LEAVE-GROUP <group#>
```

Example:

```
DLSw config>LEAVE-GROUP 2
DLSw config>
```

3.10. LIST

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

Syntax:

```
DLSw config>LIST ?
DLSW
GROUPS
LLC2
OPEN LLC2
PRIORITY
QLLC
SDLC
TCP
```

a) LIST DLSW

Displays the information configured with the **ENABLE** and **SET** commands.

Example:

```
DLSw config>LIST DLSW
DLSw protocol user configuration
DLSw config>LIST DLS
DLSw is                              ENABLED
LLC2 send Disconnect is              ENABLED
Automatic TCP connection             ALWAYS CONNECT

SRB Segment number                   030
MAC <-> IP mapping cache size        128
Max DLSw sessions                    3000
DLSw global memory allotment         141312
LLC per-session memory allotment     8192
SDLC per-session memory allotment    4096
NetBIOS UI-frame memory allotment    40960

Database age timer                   1200  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
Neighbor priority wait timer         2.0   seconds
DLSw config>
```

The meaning of each field is:

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.
MAC <-> IP mapping cache size	Maximum number of entries in MAC <-> mapping cache.
Max DLSw Sessions	The maximum number of DLSw sessions that the router will 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.
NetBIOS UI-frame memory allotment	The number of bytes the router allocates as a buffer for NetBIOS UI frames.
Database age timer	The maximum time to hold active database entries.
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 re-transmitting an LLC TEST frame.
Wait timer for SDLC response	The maximum amount of time (in seconds) the router waits for an SDLC TEST response before re-transmitting an SDLC TEST frame.
Join Group Interval	Amount of time (in seconds) between DLSw group advertisement broadcast.
Neighbor priority wait timer	Amount of time DLSw waits before selecting a neighbor.

b) LIST GROUPS

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

Example:

```
DLSw config>LIST GROUPS
Group Role   Xmit Bufsize  Rcv Bufsize   Max Segsize   Keepalive   Priority
1     CLIENT 5120          5120          1024          DISABLED    MEDIU
DLSw config>
```

The meaning of each field is:

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.
Rcv Bufsize	The size of the TCP receive buffer in the range of 1024 and 32768. The default 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.
Priority	Displays the priority of the neighbor router in the selection process. Neighbor priority is either HIGH, MEDIUM or LOW.

c) LIST LLC2

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 will be generated.

Example:

```
DLSw config>LIST LLC2
SAP   t1   t2   ti   n2   n3   tw   rw   nw   acc
0     1    1    30   8    1    2    2    1    0
DLSw config>
```

The meaning of each field is:

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.

d) LIST OPEN LLC2

Displays all open SAPs and their associated interfaces.

Example:

```
DLSw config>LIST OPEN
Interface   SAP
 0          0
 0          4
 1          4
DLSw config>
```

e) LIST PRIORITY

Lists the circuit priorities selected for SNA and NetBIOS circuits, the transmit ratios between the various circuit priorities and the largest frame size.

Example:

```
DLSw config>LIST PRIORITY
Priority for SNA DLSw sessions is           MEDIUM
Priority for NetBIOS DLSw sessions is       CRITICAL
Message allocation by C/H/M/L priority is   4/3/2/1
Maximum frame size for NetBIOS is           2052
DLSw config>
```

Circuit priorities are CRITICAL, HIGH, MEDIUM or LOW. The router uses the priority value you assign to selectively limit the burst-length of specific types of traffic. For example, if you assign SNA traffic a priority of CRITICAL and NetBIOS traffic a priority of MEDIUM, with a message allocation

of C/H/M/L 4/3/2/1, the router processes 4 SNA frames before it processes 2 NetBIOS frames. After the router processes 2 NetBIOS frames, it processes 4 SNA frames and so on.

In this scenario, two thirds of available bandwidth is dedicated to SNA traffic (a ratio of 4 to 2). Note that the router counts frames, rather than bytes, when allocating bandwidth according to the priorities you assign.

f) LIST QLLC

Displays the QLLC link station information configured with the **ADD QLLC** command.

Example:

```
DLSw config>LIST QLLC
Remote NUA              Local NUA     Local SAP/MAC          Remote SAP/MAC
Remote Alt. NUA         QLLC Address  Status
000000000               111111111     04/40:11:11:10:00:00   04/40:22:22:22:22:22
                        FF            Enabled
DLSw config>
```

The meaning of each field is:

Remote NUA	X.25 network number identifying the remote QLLC station. This number discriminates the incoming calls. Should there be any wildcards ('X') outgoing calls are not permitted from this station.
Local NUA	X.25 network number identifying the local station. This number discriminates the incoming calls. In outgoing calls this is used as NR calling. Should there be any wildcards ('X') this is not used in outgoing calls.
Remote Alt. NUA	Alternative X.25 Network number to which the X.25 call is made should the call to the remote NR fail. This is optional and may not exist in which case this facility is not enabled.
Local SAP/MAC	Identifies the PU in the DLSw domain and the Source MAC address.
Remote SAP/MAC	Identifies the remote PU in the DLSw domain in order to achieve connection with the QLLC station.
QLLC address	Address to use in the QLLC messages. Hexadecimal value between 00 and FE. If FF is programmed, the session will use FF and learn the address from the remote QLLC station.
Status	Indicates the QLLC station's availability status (Active) or inactivity (Inactive) in order to carry out connections.

g) LIST SDLC

Displays the SDLC link station information configured with the **ADD SDLC** command

Example:

```
DLSw config>LIST SDLC ALL
Net  Addr  Status   Idblk   Idnum   Local SAP/MAC          Remote SAP/MAC
5    C1    ENABLED  017     A0021   04/40:00:00:00:00:01   04/40:03:00:00:00:10
DLSw config>
```

Net	The ID number of the network that connects to the SDLC link station.
Addr	The SDLC address, between 01 and FE, of the connecting link station.
Status	The status, enabled or disabled, of the link station.
Idblk	The 3-digit hexadecimal value that identifies the device (PU) that you are connecting. Normally you will 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 will 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 correspond to this PU.
Local SAP/MAC	Identifies the PU link to the DLSw domain and the MAC address of the local link station. 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 flip the MAC address, in such cases.
Remote SAP/MAC	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. 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 flip the MAC address, in such cases.

h) LIST TCP

Displays configured DLSw neighbors that are TCP neighbors. The neighbors were configured with the **ADD TCP** command.

Example:

```
DLSw config>LIST TCP
Neighbor        Xmit Bufsize   Rcv Bufsize   Max Segsize   Keepalive  Priority
--------        ------------   -----------   -----------   ---------  --------
128.185.236.49  5120           5120          1024          Disabled   MEDIU
DLSw config>
```

Neighbor	The IP address of the TCP neighbor.
Xmit Bufsize	The size of the packet transmit buffer between the range of 1024 and 32760. The default is 5120.
Rcv Bufsize	The size of the packet transmit buffer between the range of 1024 and 32760. The default is 5120.
Max Segsize	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.
Priority	The priority of the neighbor router in the selection process, either **HIGH, MEDIUM** or **LOW.**

3.11. NETBIOS

Use the **NETBIOS** command to display the NetBIOS configuration prompt.

Syntax:

```
DLSw config>NETBIOS
```

Example:

```
DLSw config>NETBIOS
NetBIOS Support User Configuration
DLSw config>
```

3.12. 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 . It is recommended that you open 04, 08, and 0C on all participating DLSw routers.

Syntax:

```
DLSw config>OPEN-SAP
```

Example:

```
DLSw config>OPEN-SAP
Interface # [0]?
Enter SAP in hex (range 0-F4), 'SNA', 'NB' or 'LNM' [4]? LNM
SAP f4 opened on interface 0
DLSw config>
```

The meaning of each field is:

Interface # The number of the interface over which you want to open the SAP.

Enter SAP in hex You can enter SAPs individually in hexadecimal with values that range between 0 to F4. The SAP must be an even number. You can also enter SNA, NB (NetBIOS) or LNM.

- SNA opens SAPs 0, 4, 8 and C.
- NB opens SAP F0 for NetBIOS.
- LNM opens SAP F4.

3.13. 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, TCP receive buffer size, circuit priority and necessary memory size.

Syntax:

```
DLSw config>SET ?
CACHE
LLC2
MAXIMUM
MEMORY
PRIORITY
SRB
TIMERS
```

a) SET 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 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 will consume memory in the router. The effect will be a reduction in the number of DLSw sessions the router can handle.

Example:

```
DLSw config>SET CACHE
MAC <-> IP mapping cache size (4 - 65535) [128]?
DLSw config>
```

b) SET LLC2

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

Example:

```
DLSw config>SET LLC2
Enter SAP in hex (range 0 - F0) [0]?
Reply Timer (T1) in sec. [1]?
Receive Ack timer (T2) in 100millisec. [1]?
Inactivity Timer (Ti) in sec. [30]?
Transmit Window (Tw) 1- 127, 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]?
DLSw config>
```

The meaning of each field is

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 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 will continue 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.

c) SET MAXIMUM

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

Example:

```
DLSw config>SET MAXIMUM
Maximum number of DLSw sessions (1-60000) [1000]?
DLSw config>
```

d) SET 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:

```
DLSw config>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]?
Number of bytes to allocate for NetBIOS UI-frames[40960]?
DLSw config>
```

The default 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. 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_memory * total sessions * 75%.

Adjust this number 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 4 K 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 you anticipate many small packets, then

(20*4K*85%)+(80*8K*85%)+(4*512)=628.736 bytes

Bad judgment in determining the DLSw memory allocation may 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, consider increasing the DLSw allocation value.

e) SET PRIORITY

Lets you specify the circuit priorities to use for SNA circuits and NetBIOS circuits. You can use this command to specify circuit priority as Critical, High, Medium and Low. Note that you must assign circuit priorities in descending order from Critical to Low.

The router uses the priority value you assign to selectively limit the burst-length of specific types of traffic. For example, if you assign SNA traffic a priority of Critical and NetBIOS traffic a priority of Medium, with a message allocation of 4/3/2/1, the router processes 4 SNA frames before it processes 2 NetBIOS frames. After the router processes 2 NetBIOS frames, it processes 4 SNA frames and so on. In this scenario, two thirds of available bandwidth is dedicated to SNA traffic (a ratio of 4 to 2). Note that the router counts frames, rather than bytes, when allocating bandwidth according to the priorities you assign.

You can also use this command to set the maximum frame size to use for NetBIOS. Set this parameter to the largest frame size you expect to need, and no larger. Setting the frame size larger than needed reduces the number of available buffers.

Example:

```
DLSw config>SET PRIORITY
Priority for SNA DLSw sessions (C/H/M/L)[M]?
Priority for NetBIOS DLSw sessions (C/H/M/L)[C]?
Message allocation by C/H/M/L priority (4 digits)[4/3/2/1]?
Maximum NetBIOS frame size (516, 1470, 2052, or 4399)[2052]?
DLSw config>
```

f) SET SRB

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

Example:

```
DLSw config>SET SRB
Enter segment number in hex (1-FFF) [5]?
DLSw config>
```

g) SET TIMERS

Sets the DLSw protocol timers.

Example:

```
DLSw config>SET TIMERS
Database age timeout (1-10000 secs. Decimal)[1200]?
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)[900]?
Neighbor priority wait timer (1.0-5.0 secs. Decimal)[5.0]?
DLSw config>
```

The meaning of each field is:

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.
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. The range is 1 to 60000 seconds in decimal. The default is 900 seconds (15 minutes).
Neighbor priority wait timer	Amount of time (in seconds) to wait during exploration before selecting a neighbor.

3.14. EXIT

Use the **EXIT** command to return to the Config> prompt.

Syntax:

```
DLSw config>EXIT
```

Example:

```
DLSw config>EXIT
Config>
```

Chapter 3
Monitoring the DLSw Protocol

1. About DLSw Monitoring Commands

DLSw monitoring commands are available at the DLSw> prompt. Unlike configuration commands, 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.

2. Accessing the DLSw Monitoring Environment

To enter the monitoring environment, enter **PROCESS 3**, or just **P 3.** This brings you to the monitoring environment as shown:

Example:

```
*PROCESS 3
Console Operator
+
```

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

Example:

```
+PROTOCOL DLSW
Data Link Switching Console
DLSw>
```

3. DLSw Monitoring Commands

Enter DLSw monitoring commands at the DLSw> prompt.

Command	Function
?(HELP)	Lists the monitoring commands or lists any parameters associated with that command
ADD	Adds an SDLC, QLLC link station or a TCP neighbor IP address.
BAN	Displays the BAN prompt (Boundary Access Node).
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 or Q LLC link stations and TCP connections.
DISABLE	Disables the DLSw protocol, Auto-TCP-Reconnect, SDLC, QLLC link station, and LLC disconnect functionality.
ENABLE	Enables the DLSw protocol, Auto-TCP-Reconnect, SDLC, QLLC 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, QLLC link stations, SAPs, TCP connections, and DLSw groups. This command also offers you detailed information on the TCP connections aptitudes and statistics.
NETBIOS	Displays the NetBIOS prompt.
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, protocol timers and circuit priority.
EXIT	Exits the DLSw configuration process and returns you to the prompt +.

The letters written in **bold** are the minimum number of characteristics that can be entered in order to make the command effective.

3.1. ? (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:

```
DLSw>?
```

Example:

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

3.2. ADD

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

Syntax:

```
DLSw>ADD ?
QLLC
SDLC
TCP
```

a) ADD QLLC

Add the specific information necessary in order to aggregate a QLLC station. For each QLLC session you need to add a QLLC station.

Example:

```
DLSw>ADD QLLC
Local MAC Address []? 020000000023
LLC Local SAP in hex[4]?
LLC Remote SAP in hex[0]? 4
Remote MAC Address [00:00:00:00:00:00]? 020203030304
QLLC Address[ff]?
Local NUA ('X' admitted)? XXXXXXXXXXXXXX
Remote station NUA ('X' admitted)? XXXXXXXXXXXXXX
Link added and opened
DLSw>
```

This meaning of each field is the following:

Local MAC address	MAC address for the QLLC physical unit.
LLC Local SAP in hex	Identifies the station in the DLSw domain.
LLC Remote SAP in hex	Defines the Service Access Port (SAP) to be used when on activating the QLLC connection a connection is automatically tried.
Remote MAC address	This is the remote station's MAC address you wish to connect to. The MAC address is in Token Ring format (non canonical format). This holds true even if the remote is in Ethernet. Leaving this address with all "0"'s means that outgoing calls are permitted from all the stations

	which wish to connect to the source address programmed in this station. Incoming X.25 calls are not admitted in this station.
QLLC address	Address to use in the QLLC messages. This is a hexadecimal value between 00 and FE. If FF is programmed the session will use FF and learn the address from the remote QLLC station.
Local NUA	X.25 network number identifying the local station. This number discriminates the possible connections in the incoming calls. In outgoing calls this is sent in the call packets, should there be any wildcards ('X') it is not sent.
Remote station NUA	X.25 network number identifying the remote QLLC station. This number discriminates the possible connections in the incoming calls. Should there be any wildcards outgoing calls are not permitted.
Remote alt NUA	If there is a remote network number without 'X', an alternative NUA is requested for outgoing calls. If there are any 'X' wildcards, the alternative is not used.

b) ADD 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.

The source and destination MAC addresses and SAPs are mandatory and must be correct for a DLSw connection to take place. If the local devices are to communicate with remote SNA devices on an SNA LAN, such as Token Ring, then the SAPs must correspond to those in use on the remote LAN. However, if the local SDLC devices are to communicate with remote SNA devices that are attached by an SDLC data link, then the MAC addresses and SAPs are arbitrary, provided they are legal values. In this case, the MAC addresses and SAPs must logically map to the reverse source and destination addresses at the remote router.

In SDLC-to-SDLC configurations, the destination SAP (DSAP) of the primary link role router has special significance. If you set it to zero, it designates that a successful SDLC protocol handshake with the adjacent devices should not generate a DLSw connection (CANUREACH). For PU2 (non-negotiable) links with each router connected via an SDLC interface, set the DSAP of the local primary router to zero. This prevents unnecessary DLSw circuit startups from occurring. Otherwise, the local primary router attempts a DLSw CANUREACH connection to the local secondary router, but since the secondary router cannot itself activate the data link to the adjacent SDLC primary station, the connection is guaranteed to fail.

Example:

```
DLSw>ADD SDLC
Interface #[0]? 2
SDLC Address[c1]?
Local MAC Address [40:00:00:00:02:c1]?
Idblk in Hex (0-0xfff)[0]?
Idnum in Hex (0-0xfffff)[0]?
LLC Local SAP in hex[4]?
LLC Remote SAP in hex[0]? 4
Remote MAC Address [00:00:00:00:00:00]? 40:55:00:00:00:02
Link added and opened
DLSw>
```

The meaning of each field is:

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.
Local 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 will use Idblk for PUs on switches 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 will 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 Local 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 Remote 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.
Remote 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.

c) ADD 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:

```
DLSw>ADD TCP
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.14.1
Transmit Buffer Size (Decimal)[5120]?
Receive Buffer Size (Decimal)[5120]?
Maximum Segment Size (Decimal)[1024]?
Enable/Disable Keepalive (E/D)[D]?
Neighbor Priority (H/M/L)[M]?
DLSw>
```

The meaning of each field is:

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.
Receive Buffer Size	The size of the packet receive 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).
Neighbor Priority (H/M/L)	Allows you to specify the neighbor priority as either High, Medium or Low. DLSw uses this parameter to determine which DLSw neighbor to choose when multiple neighbors can reach a target station.

3.3. BAN

Use the **BAN** command to display the Boundary Access Node console prompt.

Syntax:

```
DLSw>BAN
```

Example:

```
DLSw>BAN
Boundary Access Node Console
BAN>
```

3.4. 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:

```
DLSw>CLOSE-SAP
```

Example:

```
DLSw>CLOSE-SAP
Interface # [0]?
Enter SAP in hex (range 0-F4), 'SNA', 'NB' or 'LNM'  [4]? LNM
DLSw>
```

The meaning of each field is:

Interface #	The interface number used by the open SAP.
Enter SAP in hex	You can enter SAPs individually in hexadecimal (with values ranging between 0 and F4). The SAP must be an EVEN number. You can also enter SNA, NB (NetBIOS) or LNM. • SNA closes SAPs 0, 4, 8 and C • NB closes SAP F0 for NetBIOS • LNM closes SAP F4

3.5. DELETE

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

Syntax:

```
DLSw>DELETE ?
QLLC
SDLC
TCP
```

a) DELETE QLLC

Deletes a specified QLLC station from the list of stations to which the DLSw can connect.

Example:

```
DLSw>DELETE QLLC
Local MAC Address []? 40:11:11:10:00:00
Link closed and deleted
DLSw>
```

Local MAC Address MAC address assigned to the station you wish to delete.

b) DELETE SDLC

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

Example:

```
DLSw>DELETE SDLC
Interface #[0]? 2
SDLC Address[c1]? 1
Link closed and deleted
DLSw>
```

The meaning of each field is:

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.

c) DELETE TCP

Removes the IP address of the DLSw neighbor to which you are making the TCP connection.

Example:

```
DLSw>DELETE TCP
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.14.1
Connection closed
DLSw>
```

3.6. DISABLE

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

Syntax:

```
DLSw>DISABLE ?
AUTO-TCP-RECONNECT
LLC
QLLC
SDLC
```

a) DISABLE AUTO-TCP-RECONNECT

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

Example:

```
DLSw>DISABLE AUTO-TCP-RECONNECT
DLSw>
```

b) DISABLE 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:

```
DLSw>DISABLE LLC
DLSw>
```

c) DISABLE QLLC

Prevents DLSw connections to the specified QLLC link station. This command also ends the existing QLLC connection.

Example:

```
DLSw config>DISABLE QLLC
Local MAC Address []? 40:22:22:20:00:00
Link disabled and closed
DLSw>
```

d) DISABLE SDLC

Prevents DLSw connections to the specified SDLC link station. It also terminates the existing SDLC connection.

Example:

```
DLSw>DISABLE SDLC
Interface #[0]? 2
SDLC Address[c1]? 2
Link disabled and closed
DLSw>
```

3.7. ENABLE

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

Syntax:

```
DLSw>ENABLE ?
AUTO-TCP-RECONNECT
LLC
QLLC
SDLC
```

a) ENABLE AUTO-TCP-RECONNECT

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

Example:

```
DLSw>ENABLE AUTO-TCP-RECONNECT
DLSw>
```

b) ENABLE LLC

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

Example:

```
DLSw>ENABLE LLC
DLSw>
```

c) ENABLE QLLC

Enables DLSw connections to the specified QLLC link station.

Example:

```
DLSw>ENABLE QLLC
Local MAC Address []? 40:22:22:20:00:00
Link enabled and opened
DLSw>
```

d) ENABLE SDLC

Enables DLSw connections to the specified SDLC link station.

Example:

```
DLSw>ENABLE SDLC
Interface #[0]? 2
SDLC Address[c1]? 2
Link enabled and opened
DLSw>
```

3.8. 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 would be 225.0.1.2.

Syntax:

```
DLSw>JOIN-GROUP
```

Example:

```
DLSw>JOIN-GROUP
Group ID (1-64 Decimal)[1]? 2
Client/Server or Peer Group Member (C/S/P)[C]?
Transmit Buffer Size (Decimal)[5120]?
Receive Buffer Size (Decimal)[5120]?
Maximum Segment Size (Decimal)[1024]?
Enable/Disable Keepalive (E/D)[D]?
Neighbor Priority (H/M/L)[M]?
DLSw>
```

The meaning of each field is:

Group ID	The number of the group that you want this router to join.
Client/Server or Peer 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.
Receive Buffer size	The size of the packet receive buffer between 1024 and 32768. The default size is 5.120.
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 (E/D)	Indicates whether you want the DLSw neighbor to send link keepalive messages. Default is **D** (Disable)
Neighbor Priority (H/M/L)	Specifies the neighbor priority as High, Medium or Low. DLSw uses this parameter to determine which DLSw neighbor to choose when multiple neighbors can reach a target station.

3.9. LEAVE-GROUP

Use the **LEAVE-GROUP** command to remove the router from any specified DLSw groups that were configured with the **JOIN-GROUP** command. This command terminate existing TCP connections belonging to the specified group.

Syntax:

```
DLSw>LEAVE-GROUP <group#>
```

Example:

```
DLSw>LEAVE-GROUP 2
DLSw>
```

3.10. LIST

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

Syntax:

```
DLSw>LIST ?
DLSW
GROUPS
LLC2
PRIORITY
SDLC
QLLC
TCP
```

a) LIST DLSW

Displays related information on DLSW.

Syntax:

```
DLSw>LIST DLSW ?
CACHE
GLOBAL Information
MEMORY
SESSIONS
```

- *LIST DLSW CACHE*

Lists the addresses from the DLSw MAC addresses cache.

Syntax:

```
DLSw>LIST DLSW CACHE ?
ALL
RANGE
```

LIST DLSW CACHE ALL

Lists the addresses from the DLSw MAC addresses cache. This cache contains a database with the most recent conversions of IP neighbors to MAC addresses. This also gives the MAC address, the lifetime (in seconds) within the cache and the neighbor IP address.

Example:

```
DLSw>LIST DLSW CACHE ALL
MAC Address          Secs to live   IP Adress(es)    Largest Frame
10:00:5A:F1:81:09    810            128.185.236.84   1470
10:00:5A:F1:81:A4    1170           128.185.236.84   2052
40:00:00:00:00:88    1170           128.185.236.84   2052
DLSw>
```

LIST DLSW CACHE RANGE

Displays information on a specific range of cache entries.

Example:

```
DLSw>LISTAR DLSW CACHE RANGE
Start [2]?
Stop [2]?
MAC Address          Secs to live   IP Adress(es)    Largest Frame
10:00:5A:F1:81:09    810            128.185.236.84   1470
10:00:5A:F1:81:A4    1170           128.185.236.84   2052
40:00:00:00:00:88    1170           128.185.236.84   2052
DLSw>
```

- *LIST DLSW GLOBAL*

Displays global information on DLS parameters.

Example:

```
DLSw>LIST DLSW GLOBAL
DLSw is                              ENABLED
LLC2 send Disconnect is              ENABLED
Automatic TCP connection             ALWAYS CONNECT

SRB Segment number                   100
MAC <-> IP mapping cache size        128
Max DLSw sessions                    1000
DLSw global memory allotment         141312
LLC per-session memory allotment     32768
SDLC per-session memory allotment    4096
NetBIOS UI-frame memory allotment    40960
```

```
Database age timer                   1200  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
Neighbor priority wait timer         5.0   seconds
DLSw>
```

The meaning of each field is:

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.
MAC <-> IP mapping cache size	Maximum number of entries allowed in the MAC <-> IP mapping cache.
Max DLSw Sessions	The maximum number of DLSw sessions that the router will 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.
NetBIOS UI-frame memory allotment	The number of bytes the router allocates as a buffer for NetBIOS UI frames.
Database age timer	The maximum time to hold active database entries.
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 re-transmitting 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 re-transmitting an SDLC TEST frame.
Join Group Interval	Amount of time (in seconds) between DLSw group advertisement broadcast.
Neighbor priority wait timer	Amount of time DLSw waits other ICANREACH response before selecting a neighbor.

- *LIST DLSW MEMORY*

This command lists all the existing DLSw sessions and the amount of memory used by each. It also displays the following flow control status.

READY	The session is not congested.
SESSION	The session has used the majority of its session assignment and has blocked the flow through the data link.
GLOBAL	The session is congested due to lack of memory in the router.

The Currently in use field displays the current amount of memory assigned by DLS. This includes all the session assignations, control messages and the TCP reception buffers.

Note: You need to use the SET MEMORY command to change the memory.

Example:

```
DLSw>LIST DLSW MEMORY
Total DLSw bytes requested:          141312
Global receive pool bytes granted:   84787
  Currently in use:                  0

Global transmit pool bytes granted:  56525
  Currently in use:                  232

NetBIOS UI-frame pool total bytes:   81920
  Currently in use:                  0

No active sessions
DLSw>
```

- *LIST DLSW SESSIONS*

Displays information on a current DLS session, including source, destination, status, flags, destination IP address and ID.

Syntax:

```
DLSw>LIST DLSW SESSIONS ?
ALL
BAN
DEST
DETAIL
IP
NB
RANGE
SRC
STATE
```

LIST DLSW SESSIONS ALL

Displays information on a current DLS session.

Example:

```
DLSw>LIST DLSW SESSIONS ALL
Local  (TKR)     Remote  (TKR)    State      Flags  Rem IP Addr     Id
---------------  ---------------  ---------  -----  --------------  --
400000000003/04  500000000003/04  CONNECTED          128.185.236.51   2
DLSw>
```

The meaning of each field is:

Local The source MAC address of the session.

Remote 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 an SSP_STARTED indication following an SSP_START request.

CIRC_PEND	The target DLSw is waiting an SSP_REACHACK response to an SSP_ICANREACH message.
CIRC_EST	The end-to-end circuit has been established.
CIR_RSTRT	The DLSw that originated the reset is awaiting the restart of the data link and an 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 an 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 the following.

- A- CONTACT MSG PENDING
- B- SAP RESOLVE PENDING
- C- EXIT BUSY EXPECTED
- D- TCP BUSY
- E- DELETE PENDING
- F- CIRCUIT INACTIVE

Rem 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.

LIST DLSW SESSIONS BAN

Displays the current information on BAN sessions.

Example:

```
DLSw>LIST DLSW SESSIONS BAN
BAN Port number (use 0 for all ports)[0]? 2
No active sessions
DLSw>
```

LIST DLSW SESSIONS DEST

Displays DLS session information by destination MAC address.

Example:

```
DLSw>LIST DLSW SESSIONS DEST
Remote MAC Address [50:00:00:00:00:03]?
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/04  500000000003/04   CONNECTED           128.185.236.51  2
DLSw>
```

LIST DLSW SESSIONS DETAIL

Displays detailed DLS session information.

Example:

```
DLSw>LIST DLSW SESSIONS DETAIL
Session Identifier [1]? 1
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/04  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
Local CID:             00564454:56667322
Remote CID:            23443553:36775433
Priority:              MEDIUM
DLSw>
```

The meaning of each field is:

Personality	The ORIGINATOR (initiator) or TARGET (recipient) of the connection.
XIDs sent	XIDs that this DLSw NODE has sent to the remote DLSw peer.
XIDs rcvd	XIDs that this DLSw NODE has received from the remote DLSw peer.
Datagrams sent	Datagrams that this DLSw NODE peer has sent to the remote DLSw peer.
Datagrams rcvd	Datagrams that this DLSw NODE peer has received from the remote DLSw peer.
Info frames sent	I-frames that this DLSw NODE has sent to the DLSw peer.
Info frames rcvd	I-frames that this DLSw NODE has received from the DLSw peer.
RIF	The information that is included in the RIF of the LLC TEST frame.
Local CID	Local node identifier for this session.
Remote CID	Remote node identifier for this session.
Priority	Neighbor priority used.

LIST DLSW SESSIONS IP

Displays session information about the circuits established with a neighbor DLSw.

Example:

```
DLSw>LIST DLSW SESSIONS IP
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.236.51
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/04  500000000003/04   CONNECTED           128.185.236.51  2
DLSw>
```

LIST DLSW SESSIONS NB

Lists information about the current active circuits that support NetBIOS.

Example:

```
DLSw>LIST DLSW SESSIONS NB
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/F0  500000000003/F0   CONNECTED           128.185.236.51  2
DLSw>
```

LIST DLSW SESSIONS RANGE

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

Example:

```
DLSw>LIST DLSW SESSIONS RANGE
Start [1]?
Stop [1]?
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/04  500000000003/04   CONNECTED           128.185.236.51  2
DLSw>
```

LIST DLSW SESSIONS SRC

Displays all the DLSw session information by local MAC Address.

Example:

```
DLSw>LIST DLSW SESSIONS SRC
Local MAC Address [40:00:00:00:00:01]?
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/04  500000000003/04   CONNECTED           128.185.236.51  2
SDLC 01-C1       400000000002/04   CONNECTED           128.185.236.51  1
DLSw>
```

Note: In this example local MAC address 400000000001 maps to the "SDLC 01-C1" name. If you do not know the source MAC address, enter LIST SDLC CONFIGURATION ALL or LIST QLLC CONFIGURATION to obtain it.

LIST DLSW SESSIONS STATE

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

Example:

```
DLSw>LIST DLSW SESSIONS 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,  WAIT_NOACK =11
CIRC_STRT= 2,    HLT_NOACK = 13
Enter state value[7]? 7
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/04  500000000003/04   CONNECTED           128.185.236.51  2
DLSw>
```

b) LIST GROUPS

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

Example:

```
DLSw>LIST GROUPS
Group  Role    Xmit Bufsize  Rcv Bufsize  Max Segsize  Keepalive  Priority
1      CLIENT  5120          5120         1024         DISABLED   MEDIUM
DLSw>
```

The meaning of each field is:

Group	Number of the group.
Role	Type of group.
Xmit Bufsize	Size of the TCP transmit buffer in the range of 1024 and 32768. The transmit buffer size must be at least twice the maximum segment size. Default value is 5120.
Rcv Bufsize	Size of the TCP receive buffer in the range of 1024 and 32768. The receive buffer must be at least twice the maximum segment size. Default is 5120.
Max Segsize	Maximum size of the TCP segment, in the range of 64 and 16384. The default is 1024.
Keepalive	The status of the keepalive functionality, enabled or disabled.
Priority	Displays the priority of the DLSw group as either HIGH, MEDIUM or LOW.

c) LIST LLC2

Displays information that pertains to LLC2. The options (OPEN Saps, SAP Parameters, and SESSIONS) for LLC2 are described in the following sections.

Syntax:

```
DLSw>LIST LLC2 ?
OPEN
SAP
SESSIONS
```

- ***LIST LLC2 OPEN***

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

Example:

```
DLSw>LIST LLC2 OPEN
Interface   SAP
0           0
0           4
DLSw>
```

- *LIST LLC2 SAP*

Displays configuration information on the Saps parameters. It only displays configurations which have changed. If you did not use the SET LLC2 command, no output is generated.

Example:

```
DLSw>LIST LLC2 SAP
SAP   t1  t2  ti   n2   n3   tw   rw   nw   acc
0     1   1   30   8    1    2    2    1    0
DLSw>
```

The meaning of each field is:

SAP SAP number.

t1 Response timer.

t2 Received timer for Acknowledgment.

ti Inactive timer.

n2 Maximum number of retries value.

n3 Number of I frames received before sending Acknowledgment.

tw Transmission window.

rw Receive window.

nw Acknowledgments needed to increase Ww.

acc Current LLC2 implementation does not use access priority. This parameter is always 0 by default.

- *LIST LCC2 SESSIONS*

Syntax:

```
DLSw>LIST LLC2 SESSIONS ?
ALL
BAN
NB
RANGE
```

LIST LLC2 SESSIONS ALL

Displays current information on all LLC2 sessions.

Example:

```
DLSw>LIST LLC2 SESSIONS ALL
     SAP  Int  Remote Ad.(TKR)    Local Ad.(TKR)     State      RIF
1    04   6    40:00:00:00:00:03  50:00:00:00:00:00  CONTACTED  0620 0202 B0B0
DLSw>
```

State Displays the session state. 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 has been 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 has been transmitted or received, or a DLC_HALT has been received from DLSw.

CONTACTED — In an active DLSw session, you can pass data on the session. This is the normal operation state.

LIST LLC2 SESSIONS BAN

Example:

```
DLSw>LIST LLC2 SESSIONS BAN
BAN Port number (use 0 for all ports)[0]?
     SAP  Int  Remote Ad.(TKR)    Local Ad.(TKR)     State      RIF
1    04   6    40:00:00:00:00:03  50:00:00:00:00:00  CONTACTED  0620 0202 B0B0
DLSw>
```

LIST LLC2 SESSIONS NB

Example:

```
DLSw>LIST LLC2 SESSIONS NB
     SAP  Int  Remote Ad.(TKR)    Local Ad.(TKR)     State      RIF
1    FO   6    40:00:00:00:00:03  50:00:00:00:00:00  CONTACTED  0620 0202 B0B0
DLSw>
```

LIST LLC2 SESSIONS RANGE

Displays current information for the selected range of LLC2 sessions.

Example:

```
DLSw>LIST LLC2 SESSIONS RANGE
Start [1]?
Stop [1]?
     SAP  Int  Remote Ad.(TKR)    Local Ad.(TKR)     State      RIF
1    F0   6    40:00:00:00:00:03  50:00:00:00:00:00  CONTACTED  0620 0202 B0B0
DLSw>
```

d) LIST PRIORITY

Syntax:

```
DLSw>LIST PRIORITY
```

Example:

```
DLSw>LIST PRIORITY
Priority for SNA DLSw sessions is             MEDIUM
Priority for NetBIOS DLSw sessions is         CRITICAL
Message allocation by C/H/M/L priority is     4/3/2/1
Maximum frame size for NetBIOS is             2052
DLSw>
```

e) LIST SDLC

Displays information pending to the SDLC stations defined in DLSw.

Syntax:

```
DLSw>LIST SDLC ?
CONFIGURATION
SESSIONS
```

- *LIST SDLC CONFIGURATION*

Displays the parameters configured for the PUs connected by SDLC.

Example:

```
DLSw>LIST SDLC CONFIGURATION
Interface #, or 'ALL'[0]? 5
Net  Addr  Status   Idblk   Idnum  Local SAP/MAC         Remote SAP/MAC
5    C1    Enabled  000     00000  04/40:18:99:7E:05:C1  04/40:1A:AB:92:00:C1
DLSw>
```

- *LIST SDLC SESSIONS*

Displays information on all DLS SDLC sessions in the router.

Example:

```
DLSw>LIST SDLC SESSIONS
Net   Addr  Local SAP/MAC          Remote SAP/MAC        OutQ   State
2     C1    04/40:00:00:00:00:01   04/40:00:00:00:00:02  0      Contacted
DLSw>
```

f) LIST QLLC

Displays information on the QLLC stations defined in DLSw.

Syntax:

```
DLSw>LIST QLLC ?
CONFIGURATION
SESSIONS
```

- *LIST QLLC CONFIGURATION*

Displays the parameters configured for the PUs connected by QLLC.

Example:

```
DLSw>LIST QLLC CONFIGURATION
Remote NUA       Local NUA        Local SAP/MAC         Remote SAP/MAC
Remote Alt. NUA  QLLC Address     Status
xxxxxxxxxxxxxx   xxxxxxxxxxxxxx   04/40:11:11:11:11:11  04/40:22:22:22:22:22
xxxxxxxxxxxxxx   FF               Enabled
DLSw>
```

The meaning of each field is:

Remote NUA	X.25 network number identifying the remote QLLC station. This number discriminates the incoming calls. Should there be any wildcards ('X') outgoing calls are not permitted from this station.
Local NUA	X.25 network number identifying the local station. This number discriminates the incoming calls. In outgoing calls this is used as NUA calling. Should there be any wildcards ('X') this is not used in outgoing calls.
RemoteAlt. NUA	Alternative X.25 Network number to which the X.25 call is made should the call to the remote NUA fail. This is optional and may not exist in which case this facility is not enabled.
Local SAP/MAC	Identifies the PU in the DLSw domain and the Source MAC address.
Remote SAP/MAC	Identifies the remote PU in the DLSw domain in order to achieve connection with the QLLC station.
QLLC address	Address to use in the QLLC messages. Hexadecimal value between 00 and FE. If FF is programmed, the session will use FF and learn the address from the remote QLLC station.
Status	Indicates the QLLC station's availability status (Active) or inactivity (Inactive) in order to carry out connections.

- *LIST QLLC SESSIONS*

Displays information about all QLLC DLSw session in the router.

Example:

```
DLSw>LIST QLLC SESSIONS
     Remote NUA       Local  SAP/MAC        Addr  OutQ  QLLC State
     Local NUA        Remote SAP/MAC
1.   xxxxxxxxxxxxxx   04/40:22:22:22:22:22  FF    0     QLLC_CNX_OFF
     xxxxxxxxxxxxxx   04/40:33:33:33:33:33
DLSw>
```

The meaning of each field is:

Remote NUA	X.25 network number identifying the remote QLLC station. This number discriminates the incoming calls. Should there be any wildcards ('X') outgoing calls are not permitted from this station.
Local NUA	X.25 network number identifying the local station. This number discriminates the incoming calls. In outgoing calls this is used as NUA calling. Should there be any wildcards ('X') this is not used in outgoing calls.
Local SAP/MAC	Identifies the PU in the DLSw domain and the Source MAC address.
Remote SAP/MAC	Identifies the remote PU in the DLSw domain in order to achieve connection with the QLLC station.
QLLC address	Address to use in the QLLC messages. Hexadecimal value between 00 and FE. If FF is programmed, the session will use FF and learn the address from the remote QLLC station.
OutQ	Frames pending to be sent to QLLC.
QLLC state	QLLC session state. The possible states are:

NET_DOWN:	QLLC interface down.
QLLC_CNX_OFF:	X.25 connection disconnected.
QLLC_CNX_PEND:	X.25 connection pending.
DISCONNECTED:	QLLC session disconnected.
RESOLVE_PEND:	Pending on finding remote station.
CONNECTED:	QLLC session open.
CONTACTED:	QLLC session active.
NULL_XID_PEND:	Waiting for empty XID.
DISC_PEND:	Waiting for QLLC session disconnection.
XID_PEND:	Session waiting for XID response.
CONN_REQ_PEND:	QLLC session pending connection.

g) LIST TCP

Displays information pending to the TCP connections in the DLSw router.

Syntax:

```
DLSw>LIST TCP ?
CAPABILITIES
CONFIGURATION
SESSIONS
STATISTICS
```

- ***LIST TCP CAPABILITIES***

Displays the information received from an associated router, in the capabilities exchange message.

Example:

```
DLSw>LIST TCP CAPABILITIES
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.152.14.3

Vendor ID                    000564
Vendor product version:      Teldat, S.A. 8.3.0D
Initial pacing window:       12
Supported SAPs:              00 04 08 0c f0
DLSw>
```

- *LIST TCP CONFIGURATION*

Displays the information in all the configured TCP sessions.

Example:

```
DLSw>LIST TCP CONFIGURATION
Neighbor         Xmit Bufsize  Rcv Bufsize   Max Segsize   Keepalive   Priority
---------------  ------------  -----------   -----------   ---------   --------
128.185.122.234  5120          5120          1024          DISABLED    MEDIUM
DLSw>
```

- *LIST TCP SESSIONS*

Displays version, number of active DLSw sessions which use this TCP session and the number of sessions which at some point have used this session.

Example:

```
DLSw>LIST TCP SESSIONS
Group   IP Address   Conn State   Version    Active Sess   Sess Creates
-----   ----------   ----------   -------    -----------   ------------
        1.1.1.1      ESTABLISHED  AIW V1R0   2             4
DLSw>
```

- *LIST TCP STATISTICS*

Displays the use statistics of the TCP sessions.

Example:

```
DLSw>LIST TCP STATISTICS
Enter the DLSw neighbor IP Address [0.0.0.0]? 1.1.1.2
                                  Transmitted   Received
                                  -----------   --------
Data Messages                     217           314
Data Bytes                        31648         43796
Control Messages                  64            74

CanYouReach Explorer Messages     6             0
ICanReach Explorer Messages       0             4
NameQuery Explorer Messages       0             0
NameRecognized Explorer Messages  0             0
DLSw>
```

3.11. NETBIOS

Use the **NETBIOS** command to display the NetBIOS monitoring prompt.

Syntax:

```
DLSw>NETBIOS
```

Example:

```
DLSw>NETBIOS
NetBIOS Support User Console
NetBIOS>
```

3.12. 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 . It is recommended that you open 04, 08, and 0C on all participating DLSw routers.

Syntax:

```
DLSw>OPEN-SAP
```

Example:

```
DLSw>OPEN-SAP
Interface # [0]?
Enter SAP in hex (range 0-F4), 'SNA', 'NB' or 'LNM' [4]? LNM
SAP f4 opened on interface 0
DLSw>
```

The meaning of each field is:

Interface # — The number of the interface over which you want to open the SAP.

Enter SAP in hex — You can enter SAPs individually in hexadecimal with values that range between 0 to F4. The SAP must be an even number. You can also enter SNA, NB (NetBIOS) or LNM.

- SNA opens SAPs 0, 4, 8 and C.
- NB opens SAP F0 for NetBIOS.
- LNM opens SAP F4.

3.13. SET

Use the **SET** command to configure the LLC2 parameters, protocol timers, TCP receive buffer size, circuit priority and amount of memory needed.

Syntax:

```
DLSw>SET ?
LLC2
MEMORY
PRIORITY
TIMERS
```

a) SET LLC2

Permits you to configure specific LLC2 capabilities for a specified SAP

Example:

```
DLSw>SET LLC2
Enter SAP in hex (range 0-F0) [0]?
Reply Timer(T1) in sec. [1]?
Receive Ack timer(T2) in 100millisec.[1]?
Inactivity Timer(Ti) in sec.[30]?
Transmit Window(Tw) 1-127, 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]?
DLSw>
```

The meaning of each field is:

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 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 will

	continue 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 …(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.

b) SET 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 will only affect the new DLSw sessions.

Example:

```
DLSw>SET MEMORY
Number of bytes to allocate for DLSw (at least 26624)[141312]?
Number of bytes to allocate per LLC session[8192]?
Number of bytes to allocate per SDLC session[4096]?
Number of bytes to allocate for NetBIOS UI-frames[40960]?
The SDLC and LLC allocations will affect new sessions only
DLSw>
```

Note that the default for the number of bytes to allocate to DLSw is probably too low to be useful for more than three or four DLSw sessions. 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_memory * total_sessions * 75%.

Adjust this number 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 4 K 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 you anticipate many small packets, then

(20*4K*85%)+(80*8K*85%)+(4*512)=628.736 bytes

Bad judgment in determining the DLSw memory allocation may 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, consider increasing the DLSw allocation value.

c) SET PRIORITY

Lets you specify the circuit priorities to use for SNA circuits and NetBIOS circuits. You can use this command to specify circuit priority as Critical, High, Medium and Low. Note that you must assign circuit priorities in descending order from Critical to Low.

The router uses the priority value you assign to selectively limit the burst-length of specific types of traffic. For example, if you assign SNA traffic a priority of Critical and NetBIOS traffic a priority of Medium, with a message allocation of 4/3/2/1, the router processes 4 SNA frames before it processes 2 NetBIOS frames. After the router processes 2 NetBIOS frames, it processes 4 SNA frames and so on. In this scenario, two thirds of available bandwidth is dedicated to SNA traffic (a ratio of 4 to 2). Note that the router counts frames, rather than bytes, when allocating bandwidth according to the priorities you assign.

You can also use this command to set the maximum frame size to use for NetBIOS. Set this parameter to the largest frame size you expect to need, and no larger. Setting the frame size larger than needed reduces the number of available buffers.

Example:

```
DLSw>SET PRIORITY
Priority for SNA DLSw sessions (C/H/M/L)[M]?
Priority for NetBIOS DLSw sessions (C/H/M/L)[M]?
Message allocation by C/H/M/L priority (4 digits)[4/3/2/1]?
Maximum NetBIOS frame size (516, 1470, 2052, or 4399)[2052]?
DLSw>
```

d) SET TIMERS

Sets the DLSw protocol timers.

Example:

```
DLSw>SET TIMERS
Database age timeout (1-10000 secs. Decimal)[1200]?
Max wait timer ICANREACH (1-1000 secs. Decimal)[30]?
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)[900]?
Neighbor priority wait timer (1.0-5.0 secs. Decimal)[5.0]?
DLSw>
```

The meaning of each field is:

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.
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-GROUP** command, rather than statically configuring each

router with the adjacent IP address of its DLS neighbor using the **ADD TCP** command. When you use **SET TIMERS** 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 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 (15 minutes).

Neighbor priority wait timer — Amount of time (in seconds) to wait during exploration before selecting a neighbor.

3.14. EXIT

Use the **EXIT** command to return to the + prompt.

Syntax:

```
DLSw>EXIT
```

Example:

```
DLSw>EXIT
+
```

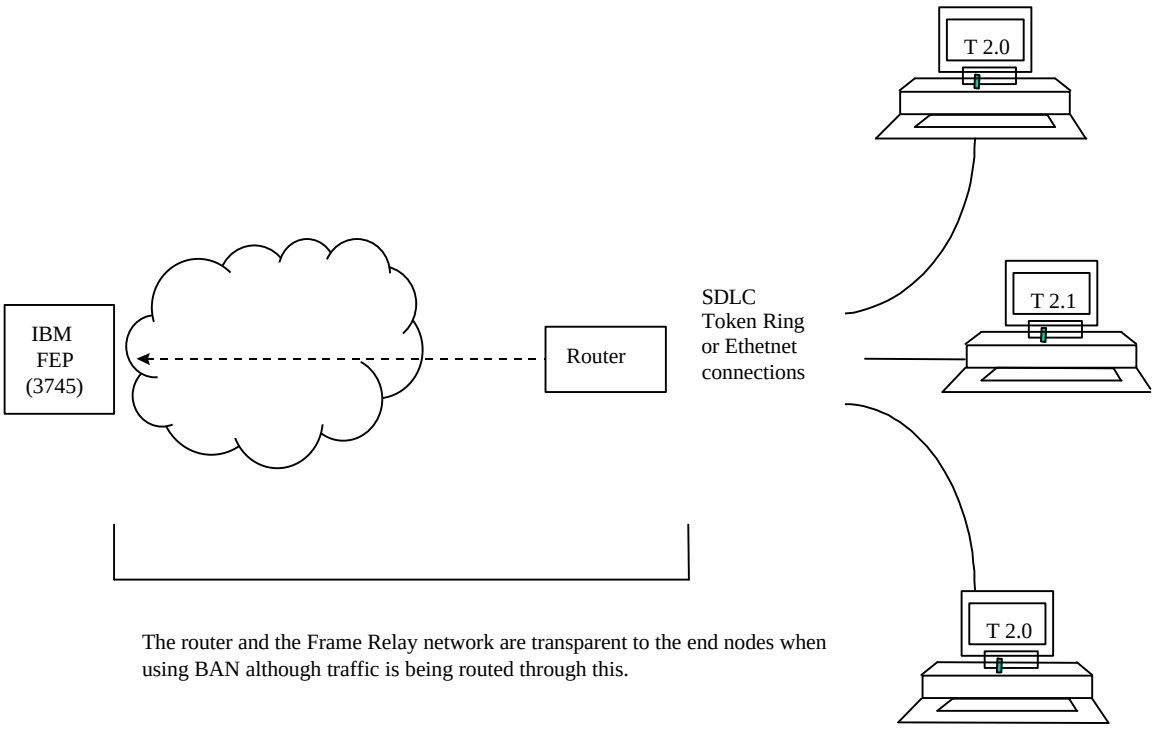
Chapter 4
Using Boundary Access Node

1. 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 the **Teldat Router**.

BAN is designed to meet the business goals of customers who do not 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 **Teldat Router** to make direct connection via Frame Relay with the front end processor (FEP) attached to an IBM mainframe.



Direct Connection of End Nodes to IBM FEP Using BAN.

1.1. How BAN Works

Ban works by filtering the frames that Type 2.0 or 2.1 end stations send. The **Teldat Router** modifies each BAN frame to comply with Bridge 802.5 (Token Ring) Frame format. The **Teldat 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.

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.

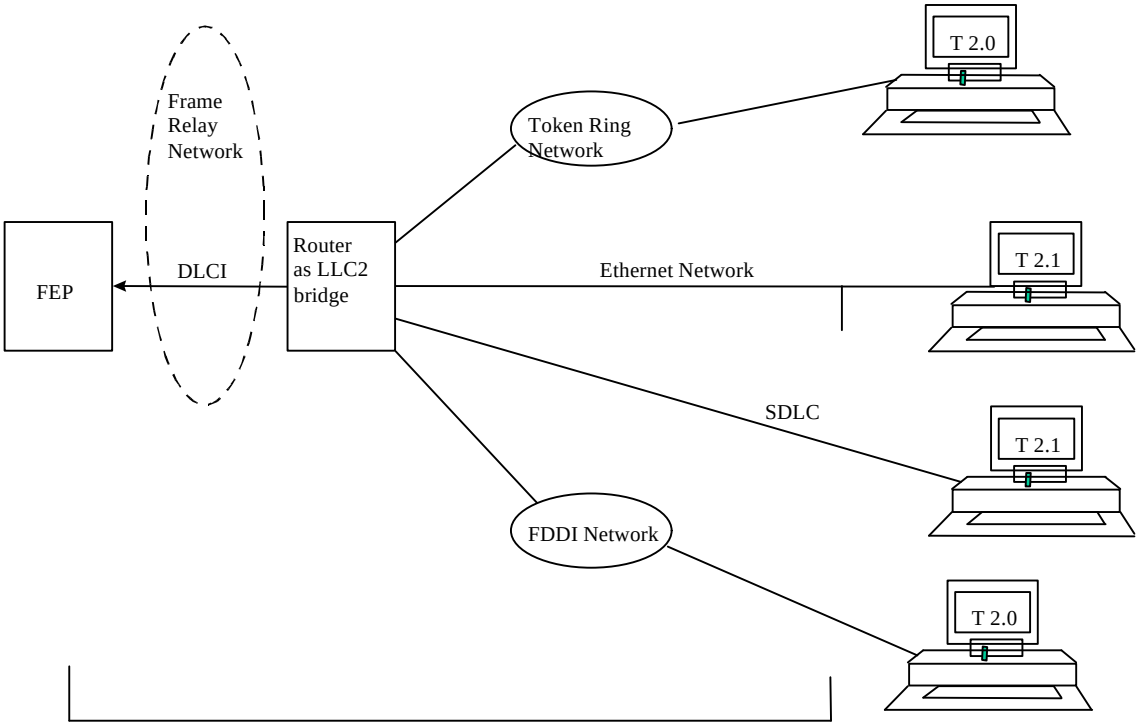
There are two ways to use BAN: straight bridging, using the router's bridging capability, and DLSw terminated. In the majority of cases, you should choose the bridging option. However you may consider choosing the terminated option if you want to reduce session timeouts on the DLCI.

1.2. Bridged and DLSw-terminated BAN

The **Teldat Router** enables you to implement BAN in two ways. With the straight bridging method, you configure BAN to bridge LLC2 frame from Type 2.0 or Type 2.1 end stations straight into the NCP. With 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.

The figure show a BAN Type 1 (bridged) connection. In this illustration, the router does not terminate the LLC2 traffic it receives from attached end nodes. Instead, the router converts the whatever frames it receives to bridged Token Ring format (RFC 1490) frames, and bridges directly to the NCP.



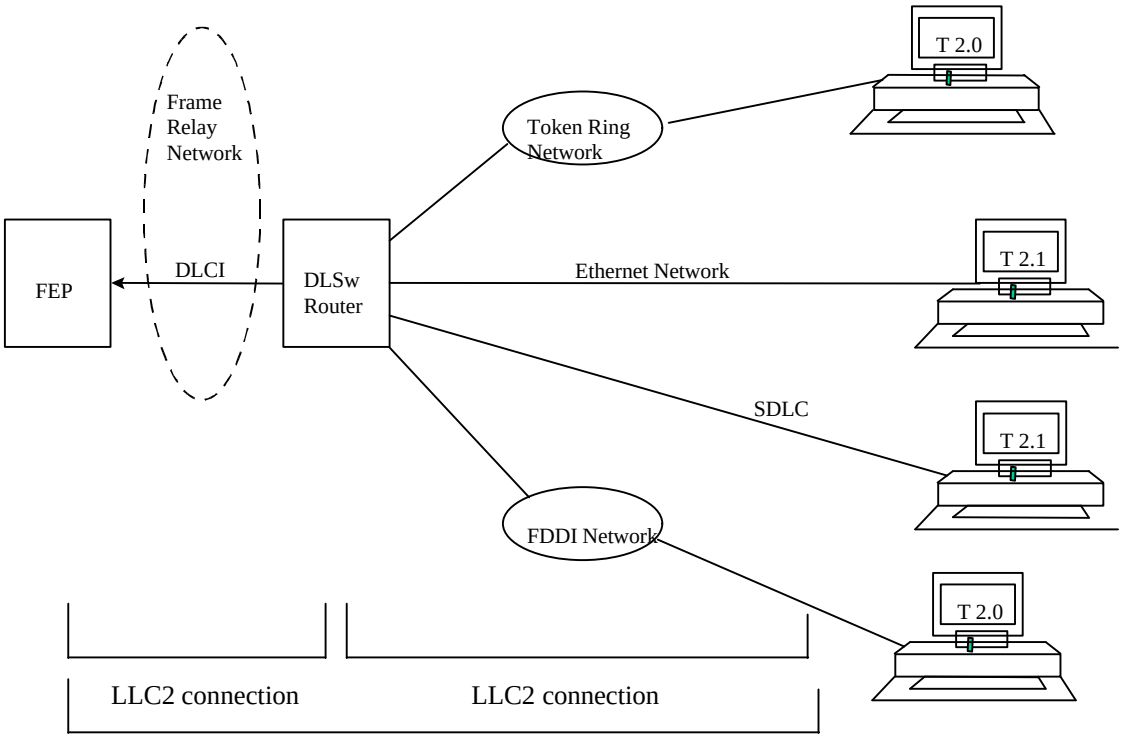
Bridged LLC2 connection with BAN

BAN Type 1: The Router as an LLC2 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 or Ethernet.

The figure shows a BAN Type 2 (Virtual BAN DLSw) connection. In this illustration, 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.



Virtual BAN DLSw LLC2 connection

BAN type 2.

1.3. Which Method Should 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 want to use DLSw-terminated BAN in situations where reducing the possibility of session timeouts is a 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.

2. Using BAN

To configure BAN, follow these steps:

1. Configure the router for Frame-Relay (FR).
2. Configure the router for Adaptive Source Routing Bridging (ASRT)
3. Configure the router for BAN
4. Open the 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.

2.1. Configuring Frame Relay

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

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

At the *FR Config>* prompt, add a permanent circuit. The router prompts you for a circuit number, which 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 PVC-PERMANENT-CIRCUIT
Circuit number[16]? 20
Outgoing Committed Information Rate (CIR) in bps[16000]?
Outgoing Committed Burst Size (Bc) in bits[16000]?
Outgoing Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)?
Assign circuit name[]? 20-ncp10
Inverse ARP (0-Default, 1-Off, 2-On): [0]?
FR Config>
```

You should 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). You should 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 the **Teldat 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.

2.2. Configuring Adaptive Source Route Bridging

Next, configure the PVC as a bridge port. To do this, enter **PROTOCOL ASRT** at the *Config>* prompt.

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

At the *ASRT config>* prompt, add a port. 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. You must assign the same circuit name as you did when configuring the router for bridging over FR in step 1.

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

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

```
ASRT config>ENABLE SOURCE-ROUTING
Port Number[2]? 5
Segment Number for the port in hex(1 - FFF)[1]? 456
ASRT  config>
```

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

```
ASRT config>DISABLE TRANSPARENT
Port Number[2]? 5
ASRT  config>
```

2.3. Configuring the Router for BAN

You configure 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
Boundary Access Node user 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

```
BAN config>ADD 5
Enter the BAN DLCI MAC Address  []? 40:00:00:00:00:01
Enter the Boundary Node Identifier MAC Address  [4f:ff:00:00:00:00]?
```

In this example, 40:00:00:00:00:01 is the MAC address of the DLCI: this is the address to which attached end stations send data. The other address, 4F:FF:00:00:00:00, is the default Boundary Node Identifier. To accept it, press Intro.

Note: You should always choose the default Boundary Node Identifier address unless the Boundary Node Identifier address of the receiving FEP has 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.

a) 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 (Type2). Type 1, straight bridging, is the default. You should accept the default unless you want inbound traffic to be terminated at the router.

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

b) Specifying the BAN mode used

Once you have defined the type of BAN to use, the router prompts you for the mode of BAN you want to use. The mode indicates the area where the router is placed. Two functional modes exist, normal and inverse. Normal mode is used in the router which connects to the NCP. The inverse mode is used if the router is going to be placed in the NCP area instead of this.

The **Teldat Router** only supports inverse mode when BAN Type 1 is used. If you choose BAN Type 2 then the router selects normal mode.

```
Do you want normal (n) or inverse (i) (n/i) [n]?
BAN port record added
BAN config>
```

2.4. Opening Service Access Points (SAPs)

To use terminated BAN, or BAN over SDLC-LLC or QLLC-LLC conversions, 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 will not be able to use BAN. Failure to open all SAPs is often the cause of configuration problems.

Open the SAPs from the *DLSw config>* prompt as follows:

```
DLSw config>OPEN-SAP
Interface # [0]?
Enter SAP in hex (range 0-F4), 'SNA', 'NB' or 'LNM' [4]? SNA
SAPs 0 4 8 c opened on interface 0
DLSw config>
```

Issuing the **OPEN-SAP** command for interface 0 opens the SAP on the LAN interface. You issue the same command to open the SAP on the FR interface.

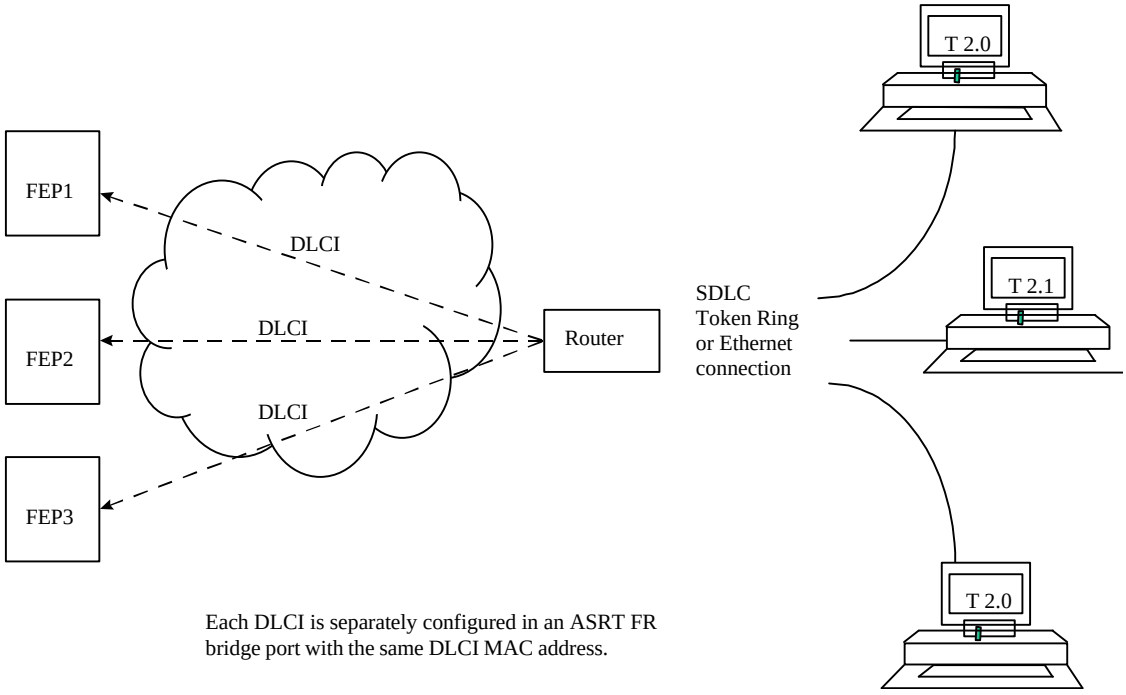
```
DLSw config>OPEN-SAP
Interface # [0]? 2
Enter SAP in hex (range 0-F4), 'SNA', 'NB' or 'LNM' [4]? SNA
SAPs 0 4 8 c opened on interface 0
DLSw config>
```

3. Using Multiple DLCIs for BAN Traffic

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.

3.1. 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 the figure.



BAN Configuration with Multiple DLCIs.

3.2. Setting up multiple DLCIs

Setting up multiple DLCIs is a simple matter, particularly if you do it 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 the 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 you must:

1. (FR configuration). Define another Frame Relay DLCI on a new bridge port.
2. (ASRT configuration). Add a bridge port for that DLCI.
3. (BAN configuration). Configure the bridge port for BAN.

4. 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 term.  Mode
5        40:00:00:00:00:01  4F:FF:00:00:00:00   bridged     direct
BAN config>
```

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, the type of BAN and if the mode is normal or inverse.

To check to see that BAN has initialized properly on startup, you can use the routers monitoring environment (at **P 3**) as follows:

```
+PROTOCOL ASRT
ASRT>BAN
BAN>LIST
Bridge   BAN                Boundary            bridged or
Port     DLCI MAC Address   Node Identifier     DLSw term.  Mode    Status
5        40:00:00:00:00:01  4F:FF:00:00:00:00   bridged     direct  Init Fail
BAN>
```

BAN has three associated status messages:

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

If you receive a status other than **Up** you should check the router's ELS messages to diagnose the problem.

5. BAN configuration

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, enter **PROCESS 4**, or simply **P 4**. This brings you to the Config> prompt as shown:

Example:

```
*PROCESS 4
User Configuration
Config>
```

If the Config> prompt does not appear immediately, press the ◴ key again.

Enter all BAN configuration commands at the *BAN config>* prompt.

Access this prompt by entering **BAN** at either the *DLSw config>* or *ASRT config>* prompt as shown:

Example:

```
Config>PROTOCOL DLSW
DLSw protocol user configuration
DLSw config>BAN
Boundary Access Node user Configuration
BAN config>
```

5.1. Configuration commands

Enter the BAN configuration commands at the *BAN config>* prompt.

Command	Function
? (HELP)	Lists all configuration commands or associated parameters.
ADD	Adds 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>* prompt.

a) ?(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:

```
BAN config>?
```

Example:

```
BAN config>?
ADD
DELETE
LIST
EXIT
BAN config>
```

b) ADD

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

Syntax:

```
BAN config>ADD <port #>
```

Example:

```
BAN config>ADD 2
Enter the BAN DLCI MAC Address  []? 40:00:00:00:00:01
Enter the Boundary Node Identifier MAC Address  [4f:ff:00:00:00:00]?
Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) [b]?
Do you want normal (n) or inverse (i) (n/i) [n]?
BAN port record added
BAN config>
```

c) DELETE

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

Syntax:

```
BAN config>DELETE <port #>
```

Example:

```
BAN config>DELETE 2
Record deleted
BAN config>
```

d) LIST

Use the **LIST** command to display information on the existing BAN configuration or to assess whether the DLCI is functioning properly. When the BAN configuration module is active, the **LIST** command provides general information on the BAN configuration.

Syntax:

```
BAN config>LIST
```

Example:

```
BAN config>LIST
Bridge   BAN                Boundary           bridged or
Port     DLCI MAC Address   Node Identifier    DLSw term.  Mode
5        40:00:00:00:00:01  4F:FF:00:00:00:00  bridged     direct
BAN config>
```

e) EXIT

Use the **EXIT** command to exit the configuration module. If you exit this it returns you to the *DLSw config>* or the *ASRT config>* prompt.

Syntax:

```
BAN config>EXIT
```

Example:

```
BAN config>EXIT
DLSw config>
```

6. BAN Monitoring

To enter the monitoring environment, enter **PROCESS 3**, or simply **P 3**. This brings you to the + prompt as shown:

Example:

```
*PROCESS 3
+
```

The BAN monitoring commands are entered at the *BAN>* prompt. Access this prompt by entering the **BAN** command at the *DLSw>* or the *ASRT>* prompt:

Example:

```
+PROTOCOL DLSW
DLSw>BAN
BAN>
```

6.1. Monitoring Commands

The monitoring commands are entered at the BAN> prompt.

Command	Function
? (HELP)	Lists all configuration 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>* or *ASRT>* prompt.

a) ?(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:

```
BAN>?
```

Example:

```
BAN>?
LIST
EXIT
BAN>
```

b) LIST

Use the **LIST** command to display information on the existing BAN configuration or to assess whether the DLCI is functioning properly. When the BAN monitoring module is active, the **LIST** command

provides general information on the BAN monitoring. This command also informs you if each BAN port has been initialized correctly.

Syntax:

```
BAN>LIST
```

Example:

```
BAN>LIST
Bridge   BAN                Boundary            bridged or
Port     DLCI MAC Address   Node Identifier     DLSw term.  Mode    Status
5        40:00:00:00:00:01  4F:FF:00:00:00:00   bridged     direct  Up
BAN>
```

Up: BAN Port is active.

c) EXIT

Use the **EXIT** command to exit the monitoring module. If you exit this it returns you to the *DLSw>* or *ASRT>* prompt.

Syntax:

```
BAN>EXIT
```

Example:

```
BAN>EXIT
DLSw>
```

or

```
BAN>EXIT
ASRT>
```