# DLSw Protocol

bintec-Dm 716-I

## Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

# Table of Contents

# I Related Documents

bintec-Dm 706-I SDLC

# Chapter 1 Using the DLSw Protocol

## 1.1 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 provides 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.

### 1.1.1 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. Moreover, DLSw preserves the end-to-end reliability and control features that make LLC2 and SDLC effective for communication on the LAN.

#### 1.1.1.1 Inherent problems 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 intended to be used 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 an inefficient use of the WAN link.

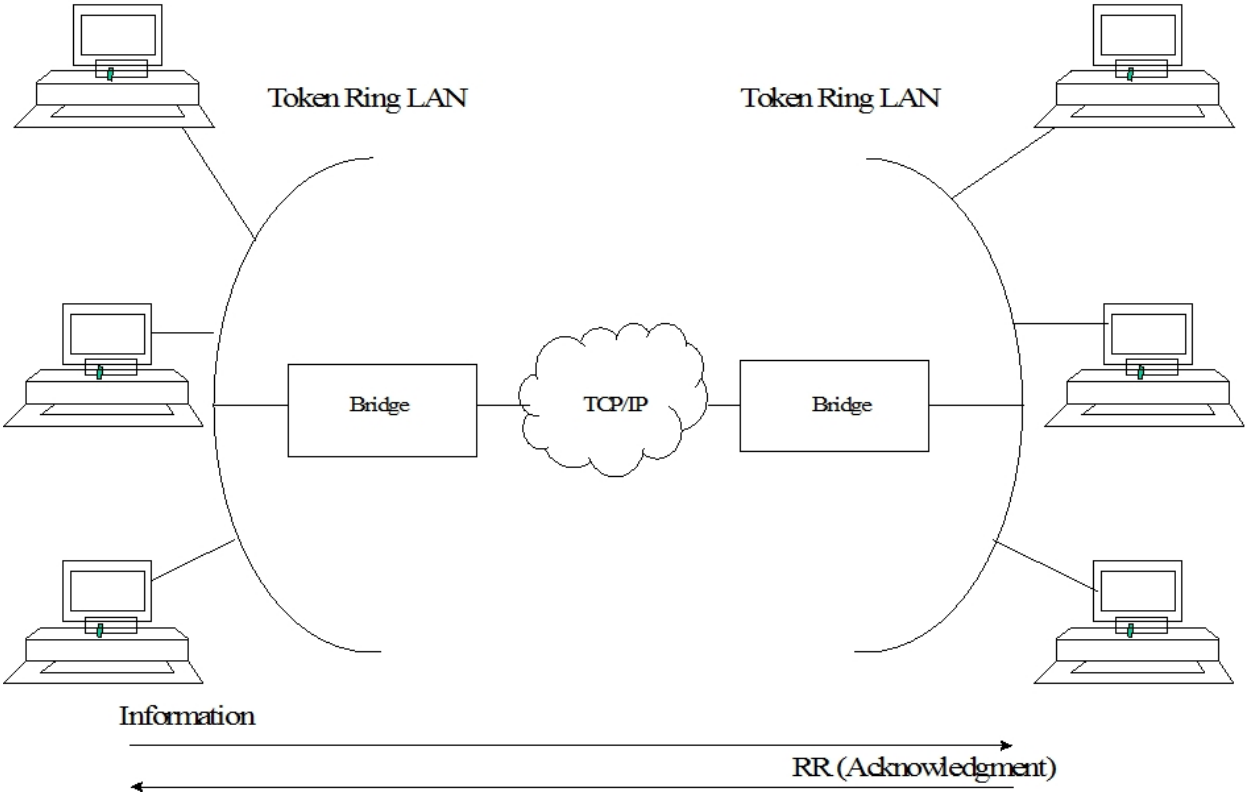


*Fig. 1: Traditional Approach to Bridging Across Internet.*

#### 1.1.1.2 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 onwards, the DLSw software is responsible for making sure the data gets through. This is accomplished by encapsulating the data in routable IP frames, then transporting them (via TCP) to another DLSw node. 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.

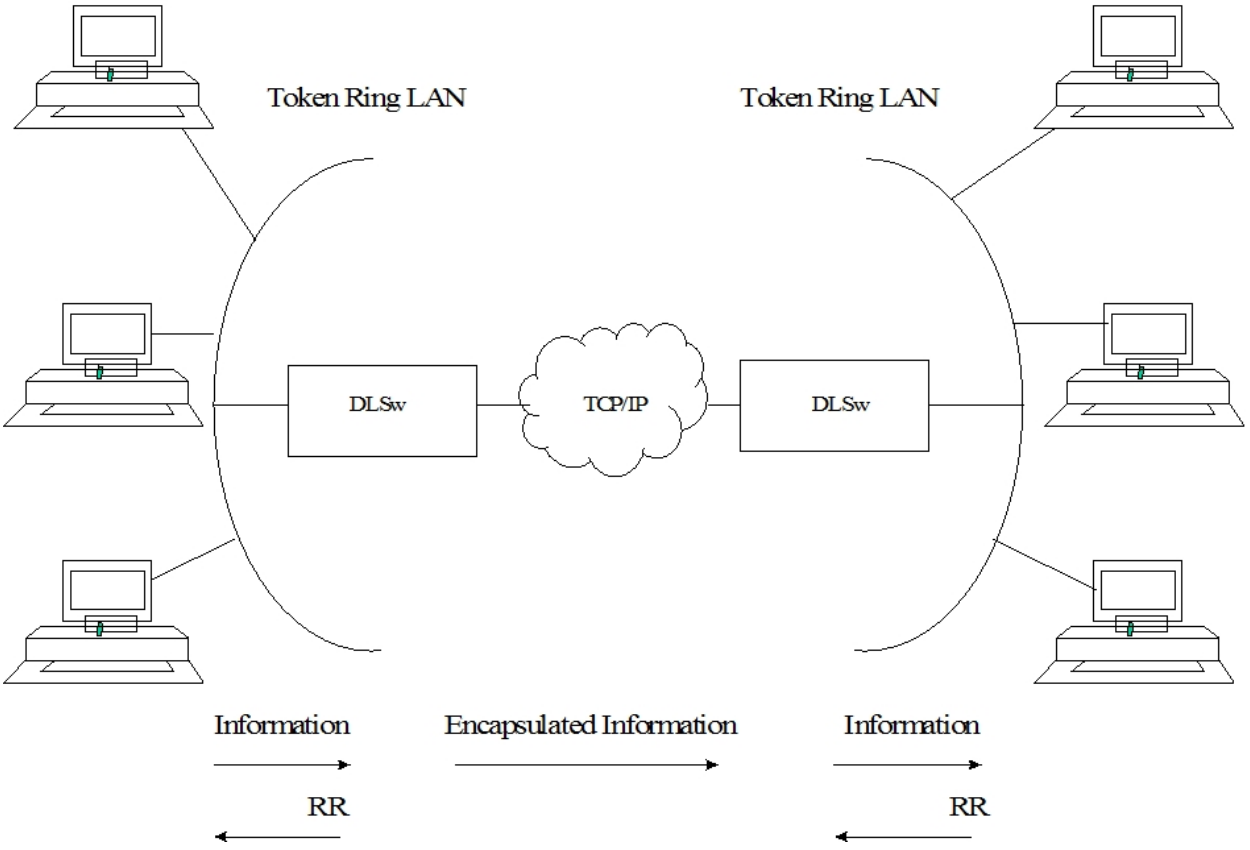


*Fig. 2: DLSw over WAN*

### 1.1.2 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. As a result, 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 bintec-Dm706-I SDLC manual.

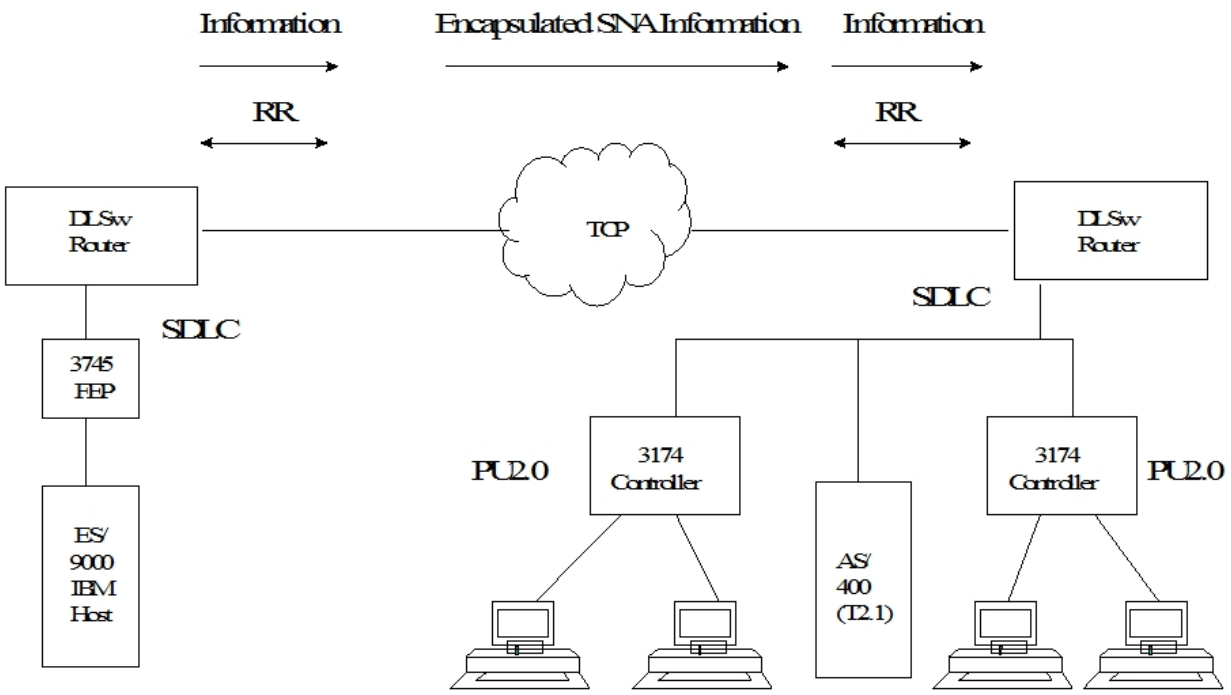


*Fig. 3: SDLC Support*

#### 1.1.2.1 Primary and Secondary Link Roles

In the above 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 allows, 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.

#### 1.1.2.2 Negotiable Link Role

In addition, you can configure SDLC link role as negotiable. In the previous figure 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 so that the local link station role is resolved accordingly.

### 1.1.3 DLSw Benefits

Since 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 main benefits of the protocol are as follows:

- 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, 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.

## 1.2 Setting Up DLSw

The following sections explain what procedures to follow to set up DLSw.

- 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.

### 1.2.1 Configuration Requirements

Our 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 following sections detail how to carry out these actions in a step-by-step fashion. An annotated example of an actual DLSw configuration follows these procedures.

#### 1.2.1.1 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 **BRIDGE** command to enable bridging on the router. Each bridge must have a unique bridge address.

(3) Enter the **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 **NO TRANSPARENT** command to disable transparent bridging. Then, enter the **BRIDGE-NUMBER** and **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 **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 Service Access Points (SAPs) you want DLSw to use. This is essential if the router is performing bridging operations and forwarding packets via DLSw.
To create a SAP filter, enter the **PROTOCOL-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 4 on a designated port. (Note that this assumes you have chosen a SAP 4 for DLSw traffic. Assigning a SAP is something you do while configuring DLSw).

(6) Next, verify the ASRT configuration using the **LIST BRIDGE** command. Although it isn't mandatory, checking the bridge configuration before proceeding is always a good idea.

(7) Enable the DLSw protocol using the **DLS** command.

### 1.2.1.2 Configuring the Internet Protocol for DLSw

The IP needs to be configured so that the local DLSw router can form a TCP connection with its DLSw neighbor. To do this:

(1) Enter the **NETWORK** command at the Config> prompt to access the interface used to connect to the DLSw neighbors available.

(2) Use the **IP ADDRESS** command to assign the IP address to the hardware interface used to connect to the other DLSw peer.

(3) Access the IP configuration process by entering the **PROTOCOL IP** command at the Config> prompt.

(4) Next, use the **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 to its DLSw peer via TCP.

(5) 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 the **ENABLE** command to activate rip.

**Note**

If you are using RIP, the router's Internal IP address MUST match the IP address assigned to a physical interface.

### 1.2.1.3 Configuring SDLC Interfaces

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 line speed (optional). If you are using internal clocking, use the **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 **STATION** command to explicitly set up SDLC stations in the following situations:

- The following defaults for SDLC stations are not satisfactory:

  - Maximum BTU is the maximum value allowable by interface.

  - Tx and Rx Windows are 7 for MOD 8 or 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 **ROLE** command if PRIMARY is not satisfactory.

#### 1.2.1.4 Configuring QLLC links

For the DLSw configuration to support QLLC links, configure the X.25 node.

#### 1.2.1.5 Configuring DLSw

Before you begin configuring DLSw, use the **LIST DEVICE** command at the Config> prompt to list the interface names for the 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 **DLS-ENABLED** command to enable DLSw in the router.

(3) If your configuration is handling LLC2 or NetBIOS traffic, enter the **DLS-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 prevent 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 **TCP-NEIGHBOR** command to add the IP address of each DLSw neighbor. You can also make this connection using multicast OSPF via the **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 **SDLC-STATION** 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 to be able to map to the corresponding remote SNA device.

(7) For the DLSw configuration to support QLLC, you have to aggregate a station using the QLLC **-STATION** command. You must also configure the X.25 node.

## 1.3 Sample DLSw Configuration

Here you can find a complete DLSw configuration. The example assumes that the router has not been configured for any other protocols or data links.

### 1.3.1 Context Diagram

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

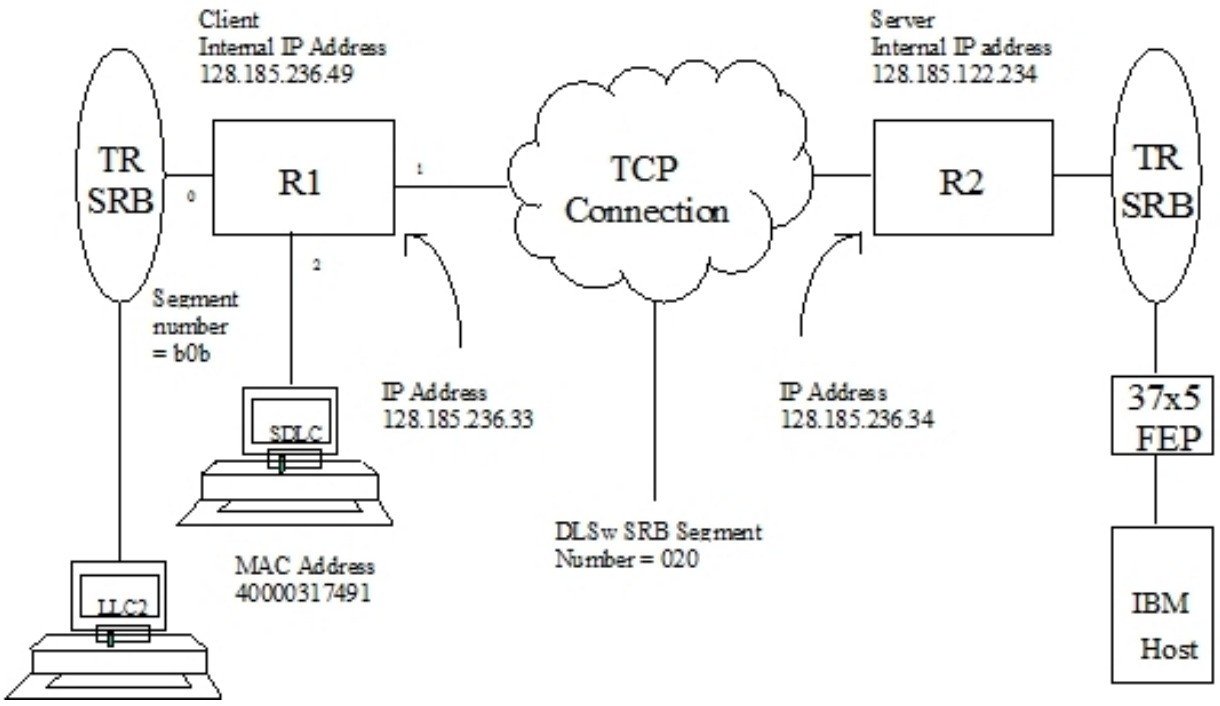


*Fig. 4: Context diagram for DLSw Configuration*

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 those used for the TCP connection.
- The source route bridge segment number of the attached Token Ring.

## 1.3.2 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 or token-ring0/0, and an SDLC device is added as interface 2 or serial0/1. Interface 1 or serial0/0 is configured for the TCP connection with a DLSw neighbor router (R2 in the figure).

```
Config> set data-link frame-relay seril0/0
Config>set data-link sdlc serial0/1
```

Once devices have been added, you can use the **LIST DEVICE** command to verify that they are assigned to the appropriate router interfaces.

### 1.3.2.1 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>network token-ring0/0
Token-Ring interface configuration
TKR config>

TKR config>speed 16

TKR config>list
Token-Ring configuration
Packet size:                    2052
Speed:                          16 Mbps
RIF Aging:                      120
Source Routing:                 Enabled
MAC Address:                    00:00:00:00:00:00
TKR config>
```

```
TKR config>exit
```

The first port (interface 1 or serial0/0) is used for the WAN (TCP/IP) link (see the figure in section *Context Diagram* on page 7). The data link selected for the WAN is Frame Relay.

### 1.3.2.2 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 or name that the Frame Relay device has been assigned (in this case 1 or serial0/0).

```
Config>network serial0/0
-- Frame Relay user configuration --
serial0/0 FR Config>
```

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

```
serial0/0 FR Config>pvc 16 default
serial0/0 FR Config>
```

Following this, the IP address from the other end of the channel will be configured (in this case, this is the R2 router). In this example, we assume that the devices are connected with no other routers in between.

```
serial0/0 FR Config>protocol-address 128.185.236.34 16
serial0/0 FR Config>
```

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

### 1.3.2.3 Add an SDLC Device

When 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 or the name of the interface to which an SDLC device has been assigned (in this case, 2 or serial0/1).

```
Config>network serial0/1
-- 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
            Slow poll    :      5.0 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>speed 9600
```

```
SDLC 2 Config>exit
```

**Note**

You can use the SDLC-STATION command in order to ignore any of the configured SDLC default link stations.

## 1.3.3 Configuring Protocols

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

### 1.3.3.1 Assigning an Internet Address to a WAN link

Select the corresponding WAN link and assign an Internet address through the **IP ADDRESS** command.

```
Config>network serial0/0
-- Frame Relay user configuration --
serial0/0 FR Config>ip address 128.185.236.33 255.255.255.0
serial0/0 FR Config>exit
Config>
```

### 1.3.3.2 Configuring IP protocol

This example shows how to create 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:
 tokenring0/0                                  IP disabled on this interface
 serial0/0       128.185.236.33  255.255.255.0   NETWORK broadcast,  fill 0
 serial0/1                                     IP disabled on this interface
 bri0/0                                        IP disabled on this interface
 x25-node                                      IP disabled on this interface
 bvi0                                          IP disabled on this ifc

Ip policy routing: disabled
Directed broadcasts: enabled
RIP: enabled
OSPF: disabled
Multipath: disabled
Ip classless: disabled
Icmp redirects: enabled
Icmp unreachables: enabled

Pool                    Begin           End
 (default)              192.168.0.0     192.168.255.255

No ip connection rules configured

No access-group configured

Local access-group: none

IP config>
```

#### 1.3.3.2.1 Configuring 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>internal-ip-address 128.185.236.49
IP config>
```

Entering the LIST command again displays newly added information.

```
IP config>list all
Interface addresses
IP addresses for each interface:
 tokenring0/0                                  IP disabled on this interface
 serial0/0       128.185.236.33  255.255.255.0   NETWORK broadcast,  fill 0
 serial0/1                                     IP disabled on this interface
 bri0/0                                        IP disabled on this interface
 x25-node                                      IP disabled on this interface
 bvi0                                          IP disabled on this ifc
Internal IP address: 128.185.236.49

Ip policy routing: disabled
Directed broadcasts: enabled
RIP: enabled
OSPF: disabled
Multipath: disabled
Ip classless: disabled
Icmp redirects: enabled
Icmp unreachables: enabled

Pool                      Begin           End
 (default)                192.168.0.0     192.168.255.255

No ip connection rules configured

No access-group configured

Local access-group: none

IP config>
```

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

```
IP config>exit
Config>
```

### 1.3.3.3 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>
```

#### 1.3.3.3.1 Enable OSPF

The first step is to enable the OSPF protocol and estimate the number of external routes and OSPF routers.

```
OSPF Config>enable ospf
OSPF Config>
```

#### 1.3.3.3.2 Define the Interfaces that use OSPF

You must execute the 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>interface 128.185.236.33 default
OSPF Config>interface 128.185.236.33 area 0.0.0.1
OSPF Config>
```

#### 1.3.3.3.3 Check the OSPF Configuration

The OSPF display configured is shown. To see changes in the configuration, compare this display with the display of the default OSPF configuration shown in section *Configuring OSPF or RIP protocol* on page 11.

```
OSPF config>list all

                        --Global configuration--
                OSPF Protocol:          Enabled
                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  TrnsDly  Pri  Hello  Dead
128.185.236.33    0.0.0.1              1      5       1     1     10    40
OSPF config>
```

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

```
OSPF Config>exit
Config>
```

### 1.3.3.4 Configuring the ASRT protocol

DLSw requires Source Route Bridging (SRB) 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>bridge
ASRT config>port tokenring0/0 1
ASRT config>
```

**Transparent Bridging Deactivation**

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

```
ASRT config>list port
Port Id (dec)          : 128: 1, (hex): 80-01
Port State             : Enabled
STP Participation      : Enabled
Port Supports          : Transparent Bridging Only
Assoc Interface        : tokenring0/0
Path Cost              : 0
-------------------------------------------------------------------------------
ASRT config>
```

Begin by disabling transparent bridging on the Token Ring port. Port number one is port 1 on interface tokenring0/0. In other words, port 1 is the logical bridge port for the physical interface set up for Token Ring (see figure in section *Context Diagram* on page 7).

```
ASRT config>no transparent 1
```

```
ASRT config>
```

**Active Source Route Bridging (SRB)**

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

**Assign a Port Segment Number and Active DLSw**

You need to 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 *Context Diagram* on page 7) b0b is the hexadecimal number assigned to the Token Ring device. You must have previously configured the bridge number in the source routing domain. In this case, this is 1.

```
ASRT config>bridge number 1
ASRT config>source-routing 1 B0B
ASRT config>
```

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

```
ASRT config>dls
ASRT config>
```

Via the LIST BRIDGE command, you can confirm that you have configured the ASRT protocol correctly.

```
ASRT config>list bridge

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

Virtual Bridge ID: 0
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:   tokenring0/0   Behavior:   SRB Only   STP:   Enabled
ASRT config>
```

### 1.3.3.5 Implementing protocol filtering

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

Since, rather than bridging, DLSw forwards traffic on SAPs (Service Access Points) 04, 08, 0C, we recommend adding 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. This is not the case in this example. The process of creating an SAP filter is provided for reference purposes only.

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

The **PROTOCOL**-FILTER DSAP 4 command creates a filter that works on all packets with a SAP 4 destination. The LIST command displays the filter characteristics.

```
ASRT config>protocol-filter dsap 4 1
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
```

### 1.3.3.6 Configuring DLSw protocol

The final step involves configuring the DLSw protocol.

To do this, begin by entering the PROTOCOL DLSW command at 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                           DISABLED
LLC2 send Disconnect is           ENABLED
Default TCP cnx mode is           ALWAYS
Promiscuous mode is               DISABLED
MAC Exclusivity mode is           DISABLED
NetBIOS Exclusivity mode is       DISABLED

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>dls-enabled
DLSw config>dls-srb 020
DLSw config>
```

#### 1.3.3.6.1 Configuring DLSw Groups and Static Sessions

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

#### 1.3.3.6.2 Using the -GROUP command

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

When executed for R1 (see section *Context Diagram* on page 7), this command defines the DLSw router as Client in group 1. To join this group, R2 must be added as a Server in group 1.

```
DLSw config>group 1 default
DLSw config>
```

```
DLSw config>list groups
Group  Role      Xmit Bufsize   Rcv Bufsize   Max Segsize   Keepalive   Priority
Inact. Time      Max cnx.       Min cnx.      Retries       Timeout
1      CLIENT    5120           5120          1024          DISABLED    MEDIUM
        0           0              0             0               0
DLSw config>
```

#### 1.3.3.6.3 Using the TCP-NEIGHBOR command

The **TCP-NEIGHBOR** 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 *Context Diagram* on page 7). You must also configure R2 with the neighbor IP address of R1.

```
DLSw config>tcp-neighbor 128.185.122.234 default
DLSw config>
```

```
DLSw config>list tcp-neighbors
Neighbor      Xmit Buf    Rcv Buf    Max Seg    Kalive   Conn Mode  Priority
Inact. time   Max cnx.    Min. cnx   Retries    Timeout
--------      ---------   --------   --------   -------  ---------  --------
128.185.122.234   5120       5120       1024    DISABLED DEFAULT     MEDIUM
        0            0          0          0          0
DLSw config>
```

#### 1.3.3.6.4 Define each SDLC link station

You must define each SDLC link station as shown:

```
DLSw config>sdlc-station serial0/1 C1 local-mac 40:00:00:31:74:91
DLSw config>sdlc-station serial0/1 C1 local-sap 4
DLSw config>sdlc-station serial0/1 C1 remote-mac 40:00:00:00:00:02
DLSw config>sdlc-station serial0/1 C1 remote-sap 4
DLSw config>sdlc-station serial0/1 C1 idblk 017
DLSw config>sdlc-station serial0/1 C1 idnum A0021
DLSw config>
```

```
DLSw config>list sdlc-stations all
Net        Addr  Status   Idblk  Idnum   Local SAP/MAC         Remote SAP/MAC
Serial0/1  C1    Enabled  017    A0021   04/40:00:00:31:74:91  04/40:00:00:00:00:02
DLSw config>
```

#### 1.3.3.6.5 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 tokenring0/0 sna
DLSw config>
```

```
DLSw config>list open-llc2
Interface      SAP
tokenring0/0    0
tokenring0/0    4
tokenring0/0    8
tokenring0/0    c
```

```
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> (Press Ctrl-P)

*RESTART
Are you sure to restart the system? (Yes/No)? yes
Read disk configuration
*
```

# Chapter 2 Configuring the DLSw Protocol

## 2.1 Accessing the DLSw Configuration Environment

To enter the static configuration environment, enter **PROCESS 4** or just **P 4**. This takes you to the Config> prompt. The changes made do not execute until they have been saved and the device restarted.

To enter the dynamic configuration environment, enter **PROCESS 5** or just **P 5**. This takes you to the Config> prompt. Changes take immediate effect or, in the case of some commands, they execute when a non-related command is entered or you exit the menu. This is shown below:

*Example:*

```
*PROCESS 4
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 DLS** command as shown:

*Example:*

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

## 2.2 DLSw Configuration Commands

Enter DLSw configuration commands at the DLSw config> prompt.

| Command | Function |
|---|---|
| *? (HELP)* | Lists the configuration commands and/or any associated parameters. |
| *BAN* | Displays the Boundary Access Node (BAN) prompt. |
| *CACHE-MAC-IP* | Configures the size of the MAC <-> IP cache. |
| *CONNECTION* | Defines the default connection mode with other DLSw nodes. |
| *DATABASE-TIMER* | Configures the life timer for the cache entries. |
| *DLS-ENABLED* | Enables the DLSw protocol. |
| *DLS-GLOBAL-MEMORY* | Configures the size of the global memory for DLSw. |
| *DLS-QUEUES* | Defines the queue procedure depending on priority. |
| *DLS-SRB* | Configures the SRB Segment for DLSw. |
| *GROUP* | Defines groups to dynamically search for DLSw nodes. |
| *ICANREACH-STATION* | Configures the list of local stations accessible from the current node to prioritize and filter exploration traffic. |
| *ICANREACH-TIMER* | Configures the response wait timer for the Icanreach messages. |
| *JOIN-GROUP-TIMER* | Configures the DLSw nodes dynamic search interval. |
| *LIST* | Displays information on the SDLC, QLLC, SAPs link stations, TCP connections and DLS groups. |
| *LLC-SAP* | Configures the parameters for each SAP LLC2. |
| *LLC-SESSION-MEMORY* | Configures the memory size reserved for each LLC session. |
| *LLC-TEST-TIMER* | Configures the wait timer for responses to the TEST LLC frames. |
| *MAX-DLS-SESSIONS* | Configures the maximum number of DLSw sessions allowed. |
| *NBS-GLOBAL-MEMORY* | Configures the storage space for NetBIOS UI frames. |
| *NBS-MTU-UI-FRAMES* | Configures the maximum size allowed for NetBIOS UI frames. |
| *NBS-PRIORITY* | Configures the NetBIOS traffic priority. |
| *NEIGHBOR-TIMER* | Configures the nodes priority wait timer. |
| *NETBIOS* | Displays the NetBIOS prompt. |
| *NO* | Deactivates certain protocol parameters. |

| | |
|---|---|
| *OPEN-SAP* | Allows DLSw to transmit data over the specified SAP. |
| *PROMISCUOUS* | Allows TCP connections to be accepted from any DLSw neighbor. |
| *QLLC-STATION* | Aggregates a QLLC link station. |
| *REMOTE-STATION* | Allows remote station lists to be configured to prioritize exploration traffic. |
| *SDLC-SESSION-MEMORY* | Configures the memory size reserved for each SDLC/QLLC session. |
| *SDLC-STATION* | Aggregates an SDLC link station. |
| *SDLC-TEST-TIMER* | Configures the wait timer for responses to the SDLC TEST frames. |
| *SEND-LLC-DISC* | Activates the sending of DISC frames in LLC disconnections. |
| *SNA-PRIORITY* | Configures the SNA traffic priority. |
| *TCP-NEIGHBOR* | Aggregates a TCP connection to another DLSw node. |
| *EXIT* | Exits the DLSw configuration process and returns to the Config> prompt. |

### 2.2.1 ? (HELP)

Lists the commands available at the current prompt level. You can also enter ? after a specific command name to list its options.

*Syntax:*

```
DLSw config>?
```

*Example:*

```
DLSw config>?
  ban                    Ban menu
  cache-mac-ip           MAC <-> IP cache size
  connection             Default transport connection activation mode
  database-timer         Database age time
  dls-enabled            Enable dlsw
  dls-global-memory      Global dlsw memory space
  dls-queues             Priority buffer queues process
  dls-srb                DLSW SRB segment
  group                  Configure groups
  icanreach-station      Configure reachability lists
  icanreach-timer        Icanreach message wait time
  join-group-timer       Join group interval
  list                   List configuration
  llc-sap                LLC2 SAP tunable parameters
  llc-session-memory     LLC per session memory space
  llc-test-timer         LLC test response wait time
  max-dls-sessions       Maximum DLSw Sessions
  nbs-global-memory      Netbios UI-Frames memory space
  nbs-mtu-ui-frames      Max size Netbios UI-Frames (576,1470,2052,4399)
  nbs-priority           Netbios traffic priority
  neighbor-timer         Neighbor priority wait time
  netbios                Netbios menu
  no                     Negate a command or set its defaults
  open-sap               Open llc2 saps
  promiscuous            Enable promiscuous connection mode
  qllc-station           QLLC Link Station
  remote-station         Configure local priorization lists
  sdlc-session-memory    SDLC/QLLC per session memory space
  sdlc-station           SDLC Link Station
  sdlc-test-timer        SDLC test response wait time
  send-llc-disc          Enable send llc DISC frames
  sna-priority           SNA traffic priority
  tcp-neighbor           Neighbor IP Address
  exit
DLSw config>
```

### 2.2.2 BAN

Displays the Boundary Access Node configuration prompt.

*Syntax:*

```
DLSw config>ban
```

*Example:*

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

### 2.2.3 CACHE-MAC-IP

Allows you to specify the cache size for the association of MAC addresses with IP addresses.

DLSw uses information saved in this cache memory to discover routes to remote stations. The DLSw has more possibilities of finding the required remote station without having to retransmit CANUREACH frames to all known TCP/IP neighbors if the cache is large.

However, configuring a very big cache length can prove harmful. Router memory is used and the number of DLSw sessions the router can handle drops. The default value for this parameter is 128 elements.

*Syntax:*

```
DLSw config>cache-mac-ip <cache-size>
```

*Example:*

```
DLSw config>cache-mac-ip 300
DLSw config>
```

### 2.2.4 CONNECTION

Defines the behavior to be carried out in order to execute the connection with other configured DLSw nodes or neighbors. There are various types of behavior.

*Syntax:*

```
DLSw config>connection ?
  always       Connect transport connections always
  on-demand    Connect transport connections when needed
  passive      Only accept incoming transport connections
```

#### 2.2.4.1 CONNECTION ALWAYS

Under this mode, the connection with the remote node is always established. In cases where the connection is lost, it is re-established immediately.

*Example:*

```
DLSw config>connection always
DLSw config>
```

#### 2.2.4.2 CONNECTION ON-DEMAND

Under this mode, the connection with the remote node is established when necessary (i.e. when a local station tries to establish connection with another remote station or when traffic not orientated to the connection is sent). Whenever the connection is lost, reestablishment is performed when necessary.

*Example:*

```
DLSw config>connection on-demand
DLSw config>
```

#### 2.2.4.3 CONNECTION PASSIVE

Under this passive mode, connection with the remote DLSw node does not establish unless the remote node requests it. Whenever the connection is lost, reestablishment is performed when necessary.

*Example:*

```
DLSw config>connection passive
DLSw config>
```

### 2.2.5 DATABASE-TIMER

Indicates how long the DLSw database entries are maintained without being used. Database entries assign destination MAC addresses within the group of DLSw neighbors that can reach them. The time is expressed in seconds. The default value is 1200 seconds.

*Syntax:*

```
DLSw config>database-timer <time>
```

*Example:*

```
DLSw config>database-timer 500
DLSw config>
```

### 2.2.6 DLS-ENABLED

Allows the router to transmit DLSw functions over all the DLSw interfaces configured (or prevents it altogether). This option is disabled by default.

*Syntax:*

```
DLSw config>[no] dls-enabled
```

#### 2.2.6.1 DLS-ENABLED

Activates DLSw operation in the router.

*Example:*

```
DLSw config>dls-enabled
DLSw config>
```

#### 2.2.6.2 NO DLS-ENABLED

Deactivates DLSw operation in the router.

*Example:*

```
DLSw config>no dls-enabled
DLSw config>
```

### 2.2.7 DLS-GLOBAL-MEMORY

Allows you to specify the total amount of memory allocated to DLSw. This is expressed in bytes.

The default for the number of bytes assigned to DLSw is probably too low to be useful for more than a small number of DLSw sessions. You need to increase the memory value depending on the number of anticipated DLSw sessions, TCP neighbors and the amount of memory available in the router.

The maximum memory required by a single session is estimated using the following formula: session_memory * number_of_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 is generated (the message number is DLS.161: Entering GLOBAL congestion on global DLS poll). It is perfectly normal for these messages to appear occasionally. If they appear very often, consider increasing the DLSw allocation value.

*Syntax:*

```
DLSw config>dls-global-memory <size>
```

*Example:*

```
DLSw config>dls-global-memory 200000
DLSw config>
```

### 2.2.8 DLS-QUEUES

Allows you to specify the circuit queue priorities when using SNA and NetBIOS circuits. You can use this command to specify circuit priority as Critical, High, Medium or Low. Please note that you must assign the circuit priority in descending order from Critical to Low.

Routers use the assigned priority values 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 through priority 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 the available bandwidth are devoted 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. The default value is CRITICAL 4, HIGH 3, MEDIUM 2 and LOW 1.

*Syntax:*

```
DLSw config>dls-queues ?
  critical    Configure critical queue priority
  high        Configure high queue priority
  medium      Configure medium queue priority
  low         Configure low queue priority
```

#### 2.2.8.1 DLS-QUEUES CRITICAL

Defines the number of critical priority messages to be sent before switching to a lower priority. Values range from 1 to 4.

*Example:*

```
DLSw config>dls-queues critical 4
DLSw config>
```

#### 2.2.8.2 DLS-QUEUES HIGH

Defines the number of high priority messages to be sent before switching to a lower priority.

*Example:*

```
DLSw config>dls-queues high 3
DLSw config>
```

#### 2.2.8.3 DLS-QUEUES MEDIUM

Defines the number of medium priority messages to be sent before switching to a lower priority.

*Example:*

```
DLSw config>dls-queues medium 2
DLSw config>
```

#### 2.2.8.4 DLS-QUEUES LOW

Defines the number of low priority messages to be sent before switching to a higher priority.

*Example:*

```
DLSw config>dls-queues low 1
DLSw config>
```

### 2.2.9 DLS-SRB

Sets the Source Routing Bridge (SRB) segment number that identifies DLSw on Source Routing networks. Specify the segment number with a 3-digit hexadecimal value. **The default value is 0, which implies DLSw will not boot unless programmed and LLC connections will be used**.

*Syntax:*

```
DLSw config>dls-srb <srb-segment>
```

*Example:*

```
DLSw config>dls-srb 100
DLSw config>
```

### 2.2.10 GROUP

The **GROUP** command allows you to automatically and dynamically control the automatic search and session connections between neighbors. This eliminates the need to define TCP neighbors with the **TCP-NEIGHBOR** command. Group numbers allowed are decimals between 1 and 64.

DLSw groups alleviate the need for long lists of static IP addresses and avoid the costs associated to their maintenance. The internet IP used must support multicast routing.

A DLSw router can be a member of a maximum of 64 groups. Members of DLSw groups use the MOSPF protocol. To use the **GROUP** command functionality, 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 before other group members and to transmit packets to them. 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.

*Syntax:*

```
DLSw config>[no] group <group-number> ?
  default       Join a new group
  inactivity    Inactivity time to disconnect from neighbor
  keepalive     dls keepalive
  low-priority  Go to low priority parameters
    max-connections  Maximum number of simultaneous connections to loose priority
    min-connections  Minimum number of simultaneous connections to recover lost
                     priority
    retries          Failed circuit connections before to go to low priority
    timeout          Time to wait before recover configured priority
  max-sgsize    Maximum segment size
  no            Negate a command or set its defaults
    keepalive     dls keepalive
  role          Role in group
    client        Join as a client
    peer          Join as a peer
    server        Join as a server
  priority      Neighbour priority
    high          High priority
    low           Low priority
    medium        Medium priority
  rx-bfsize     Teception buffer size
  tx-bfsize     Transmission buffer size
```

#### 2.2.10.1 GROUP <group-num> DEFAULT

Registers the router in a group so that the device initializes with the default values. You must specify the group number with a decimal ranging from 1 to 64.

*Syntax:*

```
DLSw config>group <group-num> default
```

*Example:*

```
DLSw config>group 3 default
```

```
DLSw config>
```

#### 2.2.10.2 NO GROUP <group-num>

Deletes any specified DLSw group configured through the **GROUP** command. This command does not affect the existing TCP connections which pertain to the specific group.

*Syntax:*

```
DLSw config>no group <group-num>
```

*Example:*

```
DLSw config>no group 5
DLSw config>
```

#### 2.2.10.3 GROUP <group-num> KEEPALIVE

Triggers the transmission of keepalive SSP messages (IAMOKAY) in order to check, periodically, that the TCP links established with other group DLSw neighbors are still active. This is deactivated by default.

*Syntax:*

```
DLSw config>group <group-num> keepalive
```

*Example:*

```
DLSw config>group 5 keepalive
DLSw config>
```

#### 2.2.10.4 GROUP <group-num> NO KEEPALIVE

Deactivates the transmission of keepalive SSP messages (IAMOKAY) for TCP links established with other DLSw neighbors pertaining to the group.

*Syntax:*

```
DLSw config>group <group-num> no keepalive
```

*Example:*

```
DLSw config>group 5 no keepalive
DLSw config>
```

#### 2.2.10.5 GROUP <group-num> MAX-SGSIZE <max-size>

Configures the maximum TCP segment length to be sent by the links established with the neighbors pertaining to the group. These values are between 64 and 16.384 bytes. The default value is 1.024.

*Syntax:*

```
DLSw config>group <group-num> max-sgsize <max-size>
```

*Example:*

```
DLSw config>group 5 max-sgsize 576
DLSw config>
```

#### 2.2.10.6 GROUP <group-num> PRIORITY HIGH

Configures the priority that TCP links established with group neighbors will have. In this case, this is configured as High. DLSw uses this parameter to determine which DLSw neighbor to select when several can reach a destination station.

*Syntax:*

```
DLSw config>group <group-num> priority high
```

*Example:*

```
DLSw config>group 5 priority high
DLSw config>
```

#### 2.2.10.7 GROUP <group-num> PRIORITY MEDIUM

Configures the priority that TCP links established with group neighbors will have. In this case, this is configured as Medium. DLSw uses this parameter to determine which DLSw neighbor to select when several can reach a destination station. The default value is Medium.

*Syntax:*

```
DLSw config>group <group-num> priority medium
```

*Example:*

```
DLSw config>group 5 priority medium
DLSw config>
```

#### 2.2.10.8 GROUP <group-num> PRIORITY LOW

Configures the priority that TCP links established with group neighbors will have. In this case, this is configured as Low. DLSw uses this parameter to determine which DLSw neighbor to select when several can reach a destination station.

*Syntax:*

```
DLSw config>group <group-num> priority low
```

*Example:*

```
DLSw config>group 5 priority low
DLSw config>
```

#### 2.2.10.9 GROUP <group-num> ROLE CLIENT

Configures the behavior of the device within the group. In this case, it is configured as Client. This type of devices can only establish transport connections with group devices that act as Servers. The default value is Client.

*Syntax:*

```
DLSw config>group <group-num> role client
```

*Example:*

```
DLSw config>group 5 role client
DLSw config>
```

#### 2.2.10.10 GROUP <group-num> ROLE PEER

Configures the behavior of the device within the group. In this case, it is configured as Peer. This type of devices can only establish transport connections with Server and Peer devices.

*Syntax:*

```
DLSw config>group <group-num> role peer
```

*Example:*

```
DLSw config>group 5 role peer
DLSw config>
```

#### 2.2.10.11 GROUP <group-num> ROLE SERVER

Configures the behavior of the device within the group. In this case this is configured as Server. This type of devices can establish transport connections with devices of a group with any type of behavior.

*Syntax:*

```
DLSw config>group <group-num> role server
```

*Example:*

```
DLSw config>group 5 role server
DLSw config>
```

#### 2.2.10.12 GROUP <group-num> RX-BFSIZE <rx-size>

Configures the reception buffer size for links established with other group neighbors. These values range between 1.024 and 32.768. Default is 5.120.

*Syntax:*

```
DLSw config>group <group-num> rx-bfsize <rx-size>
```

*Example:*

```
DLSw config>group 5 rx-bfsize 8192
DLSw config>
```

#### 2.2.10.13 GROUP <group-num> TX-BFSIZE <tx-size>

Configures the transmission buffer size for links established with other group neighbors. These values range between 1.024 and 32.768. Default is 5.120.

*Syntax:*

```
DLSw config>group <group-num> tx-bfsize <tx-size>
```

*Example:*

```
DLSw config>group 5 tx-bfsize 8192
DLSw config>
```

### 2.2.11 ICANREACH-STATION

Allows you to define the list of local stations that can reach or access the DLSw node. This also defines the access behavior. The resulting lists are announced when executing the CAPEX negotiation with the remote node. The functionality allows the remote node to optimize its exploration proceedings and station connections. In cases where active TCP links are modified, the CAPEX phase is renegotiated for each one.

*Syntax:*

```
DLSw config> [no] icanreach-station ?
  mac             Configure reachability MAC Address List
    exclusive       Exclusive MAC Address List Reachability
    mac-address     Configure MAC Address List Address & Mask
  netbios         Configure reachability NetBIOS Name List
    exclusive       Exclusive NetBIOS Name List Reachability
    name            Configure NetBIOS Name List
      group           Group name type
      individual      Individual name type
```

#### 2.2.11.1 ICANREACH-STATION MAC EXCLUSIVE

Marks the accessible MAC address list as Exclusive. This function tells the remote node that the local node has exclusive access to the stations declared on the list and will drop traffic addressed to other stations. This also allows the remote node to optimize, if required, its station exploration procedures through the various links it establishes.

**Caution**

If the EXCLUSIVE function is activated and the list of MAC addresses is left empty, the node will drop all exploration traffic that comes through the TCP links. In this case, connections between stations can only be established if the local node requests this, meaning remote stations cannot take the initiative.

*Example:*

```
DLSw config>icanreach-station mac exclusive
DLSw config>
```

#### 2.2.11.2 NO ICANREACH-STATION MAC EXCLUSIVE

Marks the accessible MAC address list as non exclusive, i.e. the announced MAC address list only tells the remote node about the stations that are accessible through the link with the local node so it can optimize, if required, its station exploration procedures in the different links that it establishes.

*Example:*

```
DLSw config>no icanreach-station mac exclusive
DLSw config>
```

### 2.2.11.3 ICANREACH-STATION MAC MAC-ADDRESS <mac> [<mask>]

Defines an entry on the MAC addresses list that is accessible from the local node. In order to avoid huge lists, you can define a mask to create a single group of stations using only one entry.

Both the MAC address and the mask are in Token Ring format (non canonic format). This is applied even though the final remote station is located in Ethernet. The mask is optional, default being ff:ff:ff:ff:ff:ff. Each mask bit set to 1 indicates that this MAC address bit must be taken into account. The stored MAC address is calculated by executing the AND between the MAC address introduced and the mask.

**Note**

In EXCLUSIVE mode, the only accepted traffic is that received through the TCP link and that is directed to local stations whose MAC address fulfills the following algorithm:

<mac-received> AND <mask introduced> = <mac-introduced>

*Syntax:*

```
DLSw config>icanreach-station mac mac-address <mac> [<mask>]
```

*Example:*

```
DLSw config>icanreach-station mac mac-address 40:00:00:00:00:01
DLSw config>icanreach-station mac mac-address 50:00:00:00:00:00 F0:00:00:00:00:00
DLSw config>icanreach-station mac mac-address 00:05:64:00:00:00 FF:FF:FF:00:00:00
DLSw config>
```

### 2.2.11.4 NO ICANREACH-STATION MAC MAC-ADDRESS <mac> [<mask>]

Deletes an entry from the list of MAC addresses that are accessible from the local node.

Both the MAC address and the mask are in Token Ring format (non-canonic format). This is applied even though the final remote station is located in Ethernet.

**Caution**

If the EXCLUSIVE function is activated and the list of MAC addresses is left empty, the node will drop all exploration traffic that comes through the TCP links. In this case, connections between stations can only be established if the local node requests this, meaning remote stations cannot take the initiative.

*Syntax:*

```
DLSw config>no icanreach-station mac mac-address <mac> [<mask>]
```

*Example:*

```
DLSw config>no icanreach-station mac mac-address 40:00:00:00:00:01
DLSw config>no icanreach-station mac mac-address 50:00:00:00:00:00 F0:00:00:00:00:00
DLSw config>no icanreach-station mac mac-address 00:05:64:00:00:00 FF:FF:FF:00:00:00
DLSw config>
```

### 2.2.11.5 ICANREACH-STATION NETBIOS EXCLUSIVE

Marks the accessible NetBIOS names list as Exclusive. This function tells the remote node that the local node has exclusive access to the stations listed and will drop non-connection NetBIOS traffic directed to other stations. This also allows the remote node to optimize, if required, its station exploration procedures through the various links that it establishes.

**Caution**

If the EXCLUSIVE function is activated and the list of NetBIOS names is left empty, the node will drop all non-connection NetBIOS traffic that comes through the TCP links.

*Example:*

```
DLSw config>icanreach-station netbios exclusive
DLSw config>
```

### 2.2.11.6 NO ICANREACH-STATION NETBIOS EXCLUSIVE

Marks the accessible NetBIOS names list as non exclusive. As a result, the announced NetBIOS names list tells the remote node about stations that are accessible through the link with the local node. This way, it can optimize (if required) its procedures for sending non-connection NetBIOS traffic through the different links it establishes.

*Example:*

```
DLSw config>no icanreach-station netbios exclusive
DLSw config>
```

### 2.2.11.7 ICANREACH-STATION NETBIOS NAME INDIVIDUAL <name>

Defines an entry on the individual NetBIOS names list accessible from the local node. In order to avoid huge lists, you can enter wildcard characters so that, through a single entry, a single group of stations can be defined. The following special characters are allowed:

| | |
|---|---|
| “?” | The corresponding character is not taken into account. |
| “*” | Subsequent characters are not taken into account (this is only permitted if it is the last one). |
| “<” | Changes to hexadecimal mode. |
| “>” | Exits the hexadecimal mode. |

*Syntax:*

```
DLSw config>icanreach-station netbios name individual <name>
```

*Example:*

```
DLSw config>icanreach-station netbios name individual “STATION-1”
DLSw config>icanreach-station netbios name individual “STATION-?”
DLSw config>icanreach-station netbios name individual “ZONE<20>-<20>*”
DLSw config>
```

### 2.2.11.8 NO ICANREACH-STATION NETBIOS NAME INDIVIDUAL <name>

Deletes an entry from the list of individual NetBIOS names accessible from the local node.

**Caution**

If the EXCLUSIVE function is activated and the list of NetBIOS names is left empty, the node will drop all NetBIOS traffic not oriented to the connection that comes through the TCP links.

*Syntax:*

```
DLSw config>no icanreach-station netbios name individual <name>
```

*Example:*

```
DLSw config>no icanreach-station netbios name individual “STATION-1”
DLSw config>no icanreach-station netbios name individual “STATION-?”
DLSw config>no icanreach-station netbios name individual “ZONE<20>-<20>*”
DLSw config>
```

### 2.2.11.9 ICANREACH-STATION NETBIOS NAME GROUP <name>

Defines an entry on the group NetBIOS names list accessible from the local node. This type of name is only applied to ADD-GROUP-NAME-QUERY NetBIOS messages. Please see INDIVIDUAL.

*Syntax:*

```
DLSw config>icanreach-station netbios name group <name>
```

*Example:*

```
DLSw config>icanreach-station netbios name group “INPUTS-1”
DLSw config>icanreach-station netbios name group “INPUTS-?”
```

```
DLSw config>icanreach-station netbios name group "OUTPUTS<20>-<20>*"
DLSw config>
```

#### 2.2.11.10 NO ICANREACH-STATION NETBIOS NAME GROUP <name>

Deletes an entry from the list of group NetBIOS names accessible from the local node. Please see INDIVIDUAL.

**Caution**

If the EXCLUSIVE function is activated and the list of NetBIOS names is left empty, the node will drop all NetBIOS traffic not oriented to the connection that comes through the TCP links.

*Syntax:*

```
DLSw config>icanreach-station netbios name group <name>
```

*Example:*

```
DLSw config>no icanreach-station netbios name group "INPUTS-1"
DLSw config>no icanreach-station netbios name group "INPUTS-?"
DLSw config>no icanreach-station netbios name group "OUTPUTS<20>-<20>*"
DLSw config>
```

### 2.2.12 ICANREACH-TIMER

Indicates how much time is spent waiting for an ICANREACH response originated by a previously transmitted CANUREACH. This time is expressed in seconds. The default value is 20 seconds.

If there are several TCP links and the exploration traffic is prioritized in some of them, either by announcing the station lists from the remote node or by configuring the local node, non-priority links start sending exploration messages when this timer times out for the first time. In this case, after the second time out, the exploration attempt is considered unsuccessful.

*Syntax:*

```
DLSw config>icanreach-timer <time>
```

*Example:*

```
DLSw config>icanreach-timer 30
DLSw config>
```

### 2.2.13 JOIN-GROUP-TIMER

This timer is important when configuring a pair of DLSw routers to use a TCP group together with the **GROUP** command, instead of statically configuring each router with the IP address next to its DLS neighbor using the **TCP-NEIGHBOR** command. This value is expressed in seconds. Default is 900 seconds (15 minutes).

*Syntax:*

```
DLSw config>join-group-timer <time>
```

*Example:*

```
DLSw config>join-group-timer 3000
DLSw config>
```

### 2.2.14 LIST

Displays DLSw information on SDLC, QLLC stations, SAPs, TCP Neighbors, groups and priorities.

*Syntax:*

```
DLSw config>list ?
  dlsw                 List DLS global configuration
  groups               List groups configuration
  icanreach-station    List Icanreach Lists
    mac                  List Icanreach MAC Address List
    netbios              List Icanreach NetBIOS Name List
  open-llc2            List all open SAPs and their associated interfaces
```

```
  priority             List priority information
  qllc-stations        List QLLC link stations configuration
  remote-stations      List local priorization information
  sap                  List LLC2 parameters configuration
  sdlc-stations        List SDLC link stations configuration
    <interface>          List stations of one interface
    all                  List stations of all interfaces
  tcp-neighbors        List TCP neighbors configurationDLSW Global Information
```

### 2.2.14.1 LIST DLSW (Global Information)

Displays the information configured through various commands.

*Example:*

```
DLSw config>list dls
DLSw is                             ENABLED
LLC2 send Disconnect is             ENABLED
Default TCP cnx mode is             ALWAYS
Promiscuous mode is                 ENABLED
MAC Exclusivity mode is             DISABLED
NetBIOS Exclusivity mode is         ENABLED

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 as follows:

| | |
|---|---|
| *DLSw is* | Status of the DLSw protocol, enabled or disabled. |
| *LLC2 send Disconnect is* | Status preventing the router from terminating an LLC2 connection upon the loss of the TCP connection. Values are enabled or disabled. |
| *Default TCP cnx mode is* | Indicates the default behavior mode for the local node in order to connect to the remote nodes. The modes are always, on-demand and passive. |
| *Promiscuous mode is* | Indicates whether the promiscuous mode is activated or not. This mode allows the local node to accept connections from remote nodes not configured in the TCP neighbors list. |
| *MAC Exclusivity mode is* | Indicates if the MAC address lists announced in the CAPEX phase are Exclusive. |
| *NetBIOS Exclusivity mode is* | Indicates if the NetBIOS name lists announced in the CAPEX phase are Exclusive. |
| *SRB Segment number* | The SRB segment that identifies DLSw in the RIF. |
| *MAC <-> IP mapping cache size* | Size of the MAC <->IP mapping cache to reduce exploration traffic. |
| *Max DLSw Sessions* | Maximum number of DLSw sessions that the router will support. |
| *DLSw global memory allotment* | Maximum amount of memory that can be used by DLSw. |
| *LLC per-session memory allotment* | Maximum amount of memory that can be used by each LLC session. |
| *SDLC per-session memory allotment* | Maximum amount of memory that can be used by each SDLC session. |
| *NetBIOS UI-frame memory allotment* | Number of bytes the router allocates as a buffer for NetBIOS UI frames. |

| | |
|---|---|
| *Database age timer* | Maximum time to hold active database entries. |
| *Max wait timer for ICANREACH* | Maximum waiting time for a response to a CANUREACH query before giving up. |
| *Wait timer for LLC response* | Maximum time (in seconds) the router waits for an LLC TEST response before re-transmitting an LLC TEST frame. |
| *Wait timer for SDLC response* | Maximum 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. |

### 2.2.14.2 LIST GROUPS

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

*Example:*

```
DLSw config>list groups
Group  Role      Xmit Bufsize   Rcv Bufsize   Max Segsize   Keepalive   Priority
Inact. Time      Max cnx.       Min cnx.      Retries       Timeout
1      CLIENT    5120           5120          1024          DISABLED    MEDIUM
        0           0              0             0               0
DLSw config>
```

The meaning of each field is:

| | |
|---|---|
| *Group* | The group number. |
| *Role* | The type of group: CLIENT, SERVER, and PEER. |
| *Xmit Bufsize* | The size of the TCP transmit buffer ranging between 1.024 and 32.768. The default size is 5.120. |
| *Rcv Bufsize* | The size of the TCP receive buffer ranging between 1.024 and 32.768. Default is 5.120. |
| *Max Segsize* | Maximum size of the TCP segment ranging between 64 and 16.384. The default size is 1.024. |
| *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. |
| *Inact. Time* | Displays the time during which the link should not have circuits established in order to deactivate it. Default is 0 which deactivates this functionality. |
| *Max cnx.* | Displays the maximum number of connections which if surpassed penalizes the link by dropping its priority to LOW. Default is 0 which deactivates this functionality. |
| *Min cnx.* | Displays the minimum number of connections which if reached or is below this value, the link then recovers its priority. Default is 0. |
| *Retries* | Displays the maximum number of unsuccessful connection attempts, which if surpassed penalizes the link by dropping its value to LOW. Default is 0 which deactivates this functionality. |
| *Timeout* | Displays the time that the link must remain with LOW priority due to an excess of unsuccessful connection attempts before recovering its priority. Default is 0 which prevents priority recovery if the link is lost for this reason. |

### 2.2.14.3 LIST ICANREACH-STATIO MAC

Displays information on the list of stations announced to the remote nodes, previously configured through the **ICANREACH-STATION MAC** command.

*Example:*

```
DLSw config>list icanreach-station mac

MAC Address List Exclusivity mode: ENABLED

  MAC Address          Mask
--------------------------------------
40:37:45:ff:01:00    ff:ff:ff:ff:ff:fc
40:00:00:00:00:00    ff:ff:ff:ff:ff:ff
50:00:00:00:00:00    f0:00:00:00:00:00
```

```
DLSw config>
```

### 2.2.14.4 LIST ICANREACH-STATION NETBIOS

Displays information on the list of stations announced to the remote nodes, previously configured through the **ICANREACH-STATION NETBIOS** command.

*Example:*

```
DLSw config>list icanreach-station netbios

NetBIOS Name List Exclusivity mode: DISABLED

  I/G  NetBIOS Name
-------------------------------------------------
   I    "STATION-1"
   I    "<0102>MSBROWSE<0201>"
   I    "STATION-R??"
   I    "STATION-S*"
   G    "GROUP-1"
   I    "<0102>__MSBROWSE__<02><01>"

DLSw config>
```

### 2.2.14.5 LIST OPEN-LLC2 (Open Saps)

Displays all open SAPs and their associated interfaces.

*Example:*

```
DLSw config>list open-llc2
Interface      SAP
ethernet0/0     0
ethernet0/0     4
ethernet0/1    f0
DLSw config>
```

### 2.2.14.6 LIST PRIORITY

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

*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 the bandwidth available is devoted 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.

### 2.2.14.7 LIST QLLC-STATIONS (QLLC Link Stations)

Displays information on QLLC link stations configured with the **QLLC-STATION** command.

*Example:*

```
DLSw config>list qllc-stations
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 as follows:

| | |
|---|---|
| *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 QLLC 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 in case the call to the remote NR fails. 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 (Enabled) or inactivity (Disabled) in order to carry out connections. |

### 2.2.14.8 LIST REMOTE-STATIONS

Displays information on the list of remote stations that allow exploration traffic prioritization, sent to the remote nodes and previously configured through the **REMOTE –STATION** command.

*Example:*

```
DLSw config>list remote-stations

    Neighbor          MAC Address            Mask
-------------------------------------------------------------
172.24.73.1         50:37:45:00:00:00    ff:ff:ff:ff:ff:00
128.185.236.49      50:37:45:00:00:00    ff:ff:ff:ff:ff:00
128.185.236.49      40:37:45:00:00:01    ff:ff:ff:ff:ff:ff
10.0.12.1           00:00:00:00:00:00    00:00:00:00:00:00

DLSw config>
```

### 2.2.14.9 LIST SAP (Parameters)

Displays the LLC2 parameters configured with the **LLC-SAP** command.

*Example:*

```
DLSw config>list sap
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 as follows:

| | |
|---|---|
| *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. |

### 2.2.14.10 LIST SDLC-STATIONS (SDLC Link Stations)

Displays the SDLC link stations information configured with the **SDLC-STATION** command.

*Example:*

```
DLSw config>list sdlc-stations all
Net        Addr  Status   Idblk   Idnum    Local SAP/MAC         Remote SAP/MAC
serial0/2   C1   ENABLED   017    A0021  04/40:00:00:00:00:01  04/40:03:00:00:00:10
DLSw config>
```

The meaning of each field is as follows:

| | |
|---|---|
| *Net* | The interface 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* | 3-digit hexadecimal value that identifies the connected device (PU). 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* | 5-digit hexadecimal value that identifies the specific SDLC PU type (2.0) connected. 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 corresponds to this PU. |
| *Local SAP/MAC* | Identifies the PU link to the DLSw domain and the MAC address of the local 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. In such cases, use the ASRT monitoring FLIP command to flip the MAC address. |
| *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 try to establish a circuit. 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. In such cases, use the ASRT monitoring FLIP command to flip the MAC address. |

### 2.2.14.11 LIST TCP-NEIGHBORS (Remote Neighbors)

Displays configured DLSw neighbors that are TCP neighbors. The neighbors were configured using the **TCP-NEIGHBOR** command.

*Example:*

```
DLSw config>list tcp-neighbors
Neighbor      Xmit Buf    Rcv Buf    Max Seg    Kalive   Conn Mode  Priority
Inact. Time      Max cnx.       Min cnx.      Retries       Timeout
--------      ---------   --------   --------   -------  ---------  --------
128.185.122.234   5120       5120       1024    DISABLED DEFAULT     MEDIUM
        0           0              0             0                0
DLSw config>
```

The meaning of each field is as follows:

| | |
|---|---|
| *Neighbor* | IP address of the TCP neighbor. |
| *Xmit Bufsize* | Size of the TCP transmit buffer ranging between 1.024 and 32760. Default is 5.120. |
| *Rcv Bufsize* | Size of the TCP receive buffer ranging between 1.024 and 32760. Default is 5.120. |
| *Max Segsize* | Maximum size of the TCP segment ranging between 64 and 16.384. Default is 1.024. |
| *Keepalive* | Displays the status of the keepalive functionality, Enabled or Disabled. |
| *Conn Mode* | Indicates the connection mode for the remote node. The values can be: Default (global configuration), Always, On-demand, or Passive. |
| *Priority* | Priority of the neighbor router in the selection process, either HIGH, MEDIUM or LOW. |
| *Inact. Time* | Displays the time during which the link should not have circuits established in order to deactivate it. Default is 0 which deactivates this functionality. |
| *Max cnx.* | Displays the maximum number of connections which if surpassed penalizes the link by dropping its priority to LOW. Default is 0 which deactivates this functionality. |
| *Min cnx.* | Displays the minimum number of connections which if reached or is below this value, the link then recovers its priority. Default is 0. |
| *Retries* | Displays the maximum number of unsuccessful connection attempts, which if surpassed penalizes the link by dropping its value to LOW. Default is 0 which deactivates this function- |

| | |
|---|---|
| | ality. |
| *Timeout* | Displays the time that the link must remain with LOW priority due to an excess of unsuccessful connection attempts before recovering its priority. Default is 0 which prevents priority recovery if the link is lost for this reason. |

## 2.2.15 LLC-SAP

Allows you to configure specific LLC2 attributes for a given SAP. Num-sap must be an even hexadecimal number between 0 and F0.

*Syntax:*

```
DLSw config>llc-sap <num-sap> ?
  default    Set default values
  T1         Reply Timer
  T2         Receive Ack timer (in 100millisec)
  Ti         Inactivity Timer
  N2         Max Retry value
  N3         Number I-frames received before sending ACK
  Tw         Transmit Window
  Rw         Receive Window
  Nw         Acks needed to increment Ww
```

### 2.2.15.1 LLC-SAP <num-sap> DEFAULT

Configures the SAP parameters with the default values. Additionally, any parameter can be configured with its default value by introducing the value 0 in the corresponding option.

*Syntax:*

```
DLSw config>llc-sap <num-sap> default
```

*Example:*

```
DLSw config>llc-sap 4 default
DLSw config>
```

### 2.2.15.2 LLC-SAP <num-sap> T1 <val-T1>

Configures the T1 timer (Reply Timer) that times out when the end LLC2 fails to send a requested acknowledgement or a response. This is expressed in seconds. The default value is 1 second.

*Syntax:*

```
DLSw config>llc-sap <num-sap> t1 <val-T1>
```

*Example:*

```
DLSw config>llc-sap 4 t1 10
DLSw config>
```

### 2.2.15.3 LLC-SAP <num-sap> T2 <val-T2>

Sets the T2 timer (Receive Ack Timer), which indicates how much time to wait before sending an acknowledgement for a frame received with format-I. This is expressed in tenths of seconds. The default value is 1 tenth of a second.

*Syntax:*

```
DLSw config>llc-sap <num-sap> t2 <val-T2>
```

*Example:*

```
DLSw config>llc-sap 4 t2 10
DLSw config>
```

### 2.2.15.4 LLC-SAP <num-sap> Ti <val-Ti>

Sets the Ti timer (Inactivity Timer). This times out when an LLC frame has not been received for a specified period of time. When this timer times out, the neighbor transmits an RR until the LLLC2 end responds or the N2 maximum retries counter is exceeded. This is expressed in seconds. The default value is 30 seconds.

*Syntax:*

```
DLSw config>llc-sap <num-sap> Ti <val-Ti>
```

*Example:*

```
DLSw config>llc-sap 4 Ti 8
DLSw config>
```

### 2.2.15.5 LLC-SAP <num-sap> Tw <val-Tw>

Configures the Tw counter (Transmit Window). This counter indicates the number of I-frames that can be sent before receiving an RR. Values range between 1 and 127. The default value is 2 frames.

*Syntax:*

```
DLSw config>llc-sap <num-sap> Tw <val-Tw>
```

*Example:*

```
DLSw config>llc-sap 4 Tw 10
DLSw config>
```

### 2.2.15.6 LLC-SAP <num-sap> Rw <val-Rw>

Configures the Rw counter (Receive Window). This counter indicates the number of I-frames that can be received before sending an RR. Values range between 1 and 127. The default value is 2 frames.

*Syntax:*

```
DLSw config>llc-sap <num-sap> Rw <val-Rw>
```

*Example:*

```
DLSw config>llc-sap 4 Rw 10
DLSw config>
```

### 2.2.15.7 LLC-SAP <num-sap> Nw <val-Nw>

Configures the Nw counter (Acks needed to increment Window). The working window (Ww) is a dynamically changing copy 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 increasing Ww by 1. Ww shall be increased in this fashion until Ww=Tw. The default value is 1 Ack (RR).

*Syntax:*

```
DLSw config>llc-sap <num-sap> Nw <val-Nw>
```

*Example:*

```
DLSw config>llc-sap 4 Nw 3
DLSw config>
```

### 2.2.15.8 LLC-SAP <num-sap> N2 <val-N2>

Sets the N2 counter (Max Retry Value). This counter indicates the maximum number of times the LLC2 neighbor will transmit a frame without receiving acknowledgement when the inactivity timer (Ti) times out. The default value is 8.

*Syntax:*

```
DLSw config>llc-sap <num-sap> N2 <val-N2>
```

*Example:*

```
DLSw config>llc-sap 4 N2 10
DLSw config>
```

### 2.2.15.9 LLC-SAP <num-sap> N3 <val-N3>

Configures the N3 counter (Number I-Frames to Ack). This counter is used, together with the T2 timer, to reduce the acknowledgement traffic for the received I-frames. This counter is configured with an initial value and decreases each time an I-frame is received. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. To ensure good performance, N3 should be set to a value that is lower than the remote LLC's Tw. Default is 1.

*Syntax:*

```
DLSw config>llc-sap <num-sap> N3 <val-N3>
```

*Example:*

```
DLSw config>llc-sap 4 N3 2
DLSw config>
```

### 2.2.16 LLC-SESSION-MEMORY

Allows you to configure the amount of memory assigned to each LLC connection established in order to cope with congestion situations. This value is expressed in bytes. The default value is 8192.

*Syntax:*

```
DLSw config>llc-session-memory <size>
```

*Example:*

```
DLSw config>llc-session-memory 16384
DLSw config>
```

### 2.2.17 LLC-TEST-TIMER

Time waited for an LLC test response before giving up. This value is expressed in seconds. The default value is 15 seconds.

*Syntax:*

```
DLSw config>llc-test-timer <time>
```

*Example:*

```
DLSw config>llc-test-timer 10
DLSw config>
```

### 2.2.18 MAX-DLS-SESSIONS

Configures the maximum number of DLSw sessions that the DLSw protocol can support. No further sessions will be permitted once the maximum number of connected sessions has been reached. The default value is 1000.

*Syntax:*

```
DLSw config>max-dls-sessions <number>
```

*Example:*

```
DLSw config>max-dls-sessions 500
DLSw config>
```

### 2.2.19 NBS-GLOBAL-MEMORY

Allows you to configure the total amount of memory assigned to store LLC UI frames corresponding to NetBIOS messages in order to cope with congestions situations. This value is expressed in bytes. The default value is 40960.

*Syntax:*

```
DLSw config>nbs-global-memory <size>
```

*Example:*

```
DLSw config>nbs-global-memory 20480
DLSw config>
```

### 2.2.20 NBS-MTU-UI-FRAMES

Configures the maximum frame length to be used by NetBIOS. This parameter should be adjusted to the longest frame length you expect to need, but not further. Configuring a frame length beyond what is needed reduces the number of available buffers. This value is expressed in bytes. The default value is 2052 bytes.

*Syntax:*

```
DLSw config>nbs-mtu-ui-frames <size>
```

*Example:*

```
DLSw config>nbs-mtu-ui-frames 1470
DLSw config>
```

## 2.2.21 NBS-PRIORITY

Allows you to specify circuit priority when managing NetBIOS traffic. The default value is MEDIUM.

*Syntax:*

```
DLSw config>nbs-priority ?
  critical
  high
  low
  medium
```

### 2.2.21.1 NBS-PRIORITY CRITICAL

Specifies the NetBIOS circuit priority as critical or the highest.

*Example:*

```
DLSw config>nbs-priority critical
DLSw config>
```

### 2.2.21.2 NBS-PRIORITY HIGH

Specifies the NetBIOS circuit priority as high.

*Example:*

```
DLSw config>nbs-priority high
DLSw config>
```

### 2.2.21.3 NBS-PRIORITY MEDIUM

Specifies the NetBIOS circuit priority as medium.

*Example:*

```
DLSw config>nbs-priority medium
DLSw config>
```

### 2.2.21.4 NBS-PRIORITY LOW

Specifies the NetBIOS circuit priority as low.

*Example:*

```
DLSw config>nbs-priority low
DLSw config>
```

## 2.2.22 NEIGHBOR-TIMER

Allows you to configure the amount of wait time from the reception of the first ICANREACH response to a CANUREACH message before selecting a path to establish the circuit. This value is expressed in seconds (introducing tenths of seconds is also allowed). The default value is 2.0 seconds.

*Syntax:*

```
DLSw config>neighbor-timer <time>
```

*Example:*

```
DLSw config>neighbor-timer 3.0
DLSw config>
```

### 2.2.23 NETBIOS

Displays the NetBIOS configuration prompt.

*Syntax:*

```
DLSw config>netbios
```

*Example:*

```
DLSw config>netbios
-- NetBIOS Support User Configuration --
NetBIOS config>
```

### 2.2.24 OPEN-SAP

Activates or deactivates LLC data transmission for the SAP link specified by the DLSw protocol. The interface must support LLC traffic and can be defined by a number or by a name. The SAP number is an even number in hexadecimal. You can also introduce SNA, NB (NetBIOS) or LNM. By default, the SAP LLC are closed.

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

*Syntax:*

```
DLSw config>[no] open-sap <interface> ?
  <hex 0..fe>    SAP number
  sna            Open SNA SAPs
  nb             Open NB SAP
  lnm            Open LNM SAP
```

#### 2.2.24.1 OPEN-SAP

The **OPEN-SAP** command should be executed on the router that is located on the session-initiator side of the connection. For example, if the client is always the sessions initiator, then you only need to open the SAPs on the router at the client's side. 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. We recommend that you open 04, 08, and 0C on all participating DLSw routers.

*Example:*

```
DLSw config>open-sap ethernet0/0 sna
DLSw config>
```

#### 2.2.24.2 NO OPEN-SAP

Closes the corresponding SAPs.

*Example:*

```
DLSw config>no open-sap ethernet0/0 sna
DLSw config>
```

### 2.2.25 PROMISCUOUS

Allows you to define the local node behavior when the remote nodes send connection requests that

have not been declared through the **TCP-NEIGHBOR** command.

*Syntax:*

```
DLSw config>[no] promiscuous
```

#### 2.2.25.1 PROMISCUOUS

Allows connections from any node or remote neighbor to be accepted, even when they haven't been configured. This command is usually used in the central or concentrated nodes and enables network expansion without the central node having to be reconfigured every time a new remote node is added. All the nodes that are able to connect with the local node in this way are considered PASSIVE connections. This means that, when connection is lost, no attempt is made to reconnect to them.

*Example:*

```
DLSw config>promiscuous
DLSw config>
```

#### 2.2.25.2 NO PROMISCUOUS

Allows the local node to reject any connection attempt from remote nodes that have not been configured through the **TCP-NEIGHBOR** command. This is the default mode.

*Example:*

```
DLSw config>no promiscuous
DLSw config>
```

### 2.2.26 QLLC-STATION

Allows you to eliminate (**NO QLLC-STATION** ) or create and modify (**QLLC-STATION** ) QLLC stations. A QLLC station is defined by its virtual MAC address. This deals with a fictitious address, as the QLLC stations do not have MAC addresses, and serves to identify the station (Physical Unit) in the DLSw Domain. The MAC address is in Token Ring format (non-canonical format).

*Syntax:*

```
DLSw config>[no] qllc-station <local-mac-virtual> ?
  address           Qllc address
  disabled          Disable this qllc station
  local-nua         Local X.25 nua
  local-sap         Virtual local sap
  no                Negate a command or set its defaults
    disabled          Enable this qllc station
  remote-alt-nua    Alternative remote X.25 nua
  remote-mac        Remote mac address
  remote-nua        Remote X.25 nua
  remote-sap        Remote sap
```

#### 2.2.26.1 NO QLLC-STATION <local-mac-virtual>

Eliminates the specified SDLC station from the list of stations that the DLSw can connect to.

*Syntax:*

```
DLSw config>no qllc-station <local-mac-virtual>
```

*Example:*

```
DLSw config>no qllc-station 40:00:12:FF:00:01
DLSw config>
```

#### 2.2.26.2 QLLC-STATION <local-mac-virtual> ADDRESS <qllc-addr>

Allows you to specify the address to use in QLLC messages. This is a hexadecimal value between 00 and FE. If 00 is programmed, the session will use FF and learn the address from the remote QLLC station. The default value is FF.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> address <qllc-addr>
```

*Example:*

```
DLSw config>qllc-station 40:00:12:34:00:01 address C1
DLSw config>
```

#### 2.2.26.3 QLLC-STATION <local-mac-virtual> DISABLED

Prevents DLSw connections to the specified QLLC station.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> disabled
```

*Example:*

```
DLSw config>qllc-station 40:00:12:FF:00:01 disabled
DLSw config>
```

#### 2.2.26.4 QLLC-STATION <local-mac-virtual> NO DISABLED

Readmits DLSw connections to the specified QLLC station. This is the default value.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> no disabled
```

*Example:*

```
DLSw config>qllc-station 40:00:12:FF:00:01 no disabled
DLSw config>
```

#### 2.2.26.5 QLLC-STATION <local-mac-virtual> LOCAL-NUA <x25-nua>

Through this command, you can configure the X.25 network number that identifies the local QLLC station. This number discriminates the possible connections in incoming calls. In outgoing calls, this is sent in call packets. No sending is done if there are any wildcards ('X'). The parameter is configured with wildcards by default.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> local-nua <x25-nua>
```

*Example:*

```
DLSw config>qllc-station 40:00:12:FF:00:01 local-nua 213022456
DLSw config>
```

#### 2.2.26.6 QLLC-STATION <local-mac-virtual> LOCAL-SAP <sap-virtual>

Allows you to define the SAP associated to the QLLC station. This serves to identify the station (Physical Unit) in the DLSw Domain. The SAP is for LLC use only. The default value is 4.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> local-sap <sap-virtual>
```

*Example:*

```
DLSw config>qllc-station 40:00:12:34:00:01 local-sap 8
DLSw config>
```

#### 2.2.26.7 QLLC-STATION <local-mac-virtual> REMOTE-ALT-NUA <x25-nua>

Through this command, you can configure the X.25 network number that will be used to execute outgoing calls when the main number (**REMOTE-NUA**) fails to connect. In cases where the **REMOTE-NUA** is configured with wildcards, this parameter is not taken into account. If this parameter is configured with wildcards ('X'), the alternative call option is left inactive. The parameter is configured with wildcards by default.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> remote-alt-nua <x25-nua>
```

*Example:*

```
DLSw config>qllc-station 40:00:12:FF:00:01 remote-alt-nua 213022499
DLSw config>
```

#### 2.2.26.8 QLLC-STATION <local-mac-virtual> REMOTE-MAC <mac-addr>

Allows you to define the MAC address associated to the remote station. This deals with the MAC address of the remote station to which the local QLLC station is connecting to. The MAC address is in Token Ring format (non-canonical format). This holds true even if the end remote station is in Ethernet. Leaving this address full of “0” means that outgoing calls are allowed from all stations that wish to connect to the source address programmed in this station. Incoming X.25 calls are not admitted in this station. The default value is 00:00:00:00:00:00.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> remote-mac <mac-addr>
```

*Example:*

```
DLSw config>qllc-station 40:00:12:34:00:01 remote-mac 40:00:37:45:00:01
DLSw config>
```

#### 2.2.26.9 QLLC-STATION <local-mac-virtual> REMOTE-NUA <x25-nua>

Through this command, you can configure the X.25 network number that identifies the remote QLLC station across the X.25 network. This is the number used in outgoing calls to connect to the station through the X.25 network. This number also discriminates the possible connections in incoming calls. If there are wildcards, then outgoing calls are prohibited. The parameter is configured with wildcards by default.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> remote-nua <x25-nua>
```

*Example:*

```
DLSw config>qllc-station 40:00:12:FF:00:01 remote-nua 213022433
DLSw config>
```

#### 2.2.26.10 QLLC-STATION <local-mac-virtual> REMOTE-SAP <sap>

Defines the Service Access Point (SAP) that is going to be used when automatically attempting a connection when the station requests one. If this SAP is 0, then the link station is in passive mode and does not send a CANUREACH. The default value is 0.

*Syntax:*

```
DLSw config>qllc-station <local-mac-virtual> remote-sap <sap>
```

*Example:*

```
DLSw config>qllc-station 40:00:12:34:00:01 remote-sap 4
DLSw config>
```

### 2.2.27 REMOTE-STATION

Allows you to define the links through which remote stations are accessed. As a result, you can establish a priority when executing station exploration, optimizing and reducing the traffic sent by the transport links. In order to avoid long lists, you can define a mask to so define a single group of stations via a single entry.

By using this command, you establish the exploration priority to locate a remote station. In cases where the MAC address coincides with one on the list, the exploration messages are sent only through the specified links. In cases where there is no response, exploration messages are sent through the remaining links (meaning exploration traffic can be greatly reduced).

Both the MAC address and the mask are in Token Ring format (non-canonic format). This is applied even through the final remote station is located in Ethernet. The mask is optional, default is ff:ff:ff:ff:ff:ff. Each mask bit set to 1 indicates that this MAC address bit must be taken into account. The stored MAC address is calculated by executing the AND between the introduced MAC address and the mask. Please see the **ICANREACH-STATION** command.

*Syntax:*

```
DLSw config> [no] remote-station <ip-addr> mac-address <mac> [<mask>]
```

#### 2.2.27.1 REMOTE-STATION <ip-addr> MAC-ADDRESS <mac> [<mask>]

Defines the transport link wanted to establish connection with the entered remote station or stations. Various links can be defined for the same address or group of MAC addresses.

*Example:*

```
DLSw config>remote-station 128.185.14.1 mac-address 40:00:00:00:00:01
DLSw config>remote-station 210.137.36.4 mac-address 40:00:00:00:00:01
DLSw config>remote-station 1.1.1.1 mac-address 50:00:00:00:00:00 F0:00:00:00:00:00
DLSw config>remote-station 2.2.2.2 mac-address 00:05:64:00:00:00 FF:FF:FF:00:00:00
DLSw config>
```

#### 2.2.27.2 NO REMOTE-STATION <lip-addr> MAC-ADDRESS <mac> [<mask>]

Eliminates the entered address or group of MAC addresses from the priority list.

*Example:*

```
DLSw config>no remote-station 128.185.14.1 mac-address 40:00:00:00:00:01
DLSw config>
```

### 2.2.28 SDLC-SESSION-MEMORY

Allows you to configure the amount of memory assigned to each SDLC or QLLC connection established in order to cope with congestion situations. This value is expressed in bytes. Default is 4096.

*Syntax:*

```
DLSw config>sdlc-session-memory <size>
```

*Example:*

```
DLSw config>sdlc-session-memory 16384
DLSw config>
```

### 2.2.29 SDLC-STATION

Allows you to eliminate (**NO SDLC-STATION**) or create and modify (**SDLC-STATION**) SDLC stations. An SDLC station is defined through two parameters. <intf> is the interface (name or number) where the SDLC station is connected. <sdlc-addr> is the SDLC address expressed by a two digit hexadecimal number whose permitted range goes from 01 to FE.

The local and remote 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, such as Token Ring, then the SAPs must correspond to those in use on the remote LAN. However, if the local devices are to communicate with remote SNA devices that are attached by an SDLC data link, then the MAC addresses and SAPs are arbitrary, providing legal values. In this case, the MAC addresses and SAPs must logically map to the inverse source and destination addresses at the remote router.

In SDLC-to-SDLC configurations, the remote 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 where each router is 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. However, since the secondary router cannot itself activate the data link to the adjacent SDLC primary station, the connection is guaranteed to fail.

*Syntax:*

```
DLSw config>[no] sdlc-station <intf> <sdlc-addr> ?
  disabled      Disable this sdlc station
  idblk         ID-block
  idnum         ID-number
  local-mac     Virtual local mac address
  local-sap     Virtual local sap
  no            Negate a command or set its defaults
    disabled      Enable this sdlc station
  remote-mac    Remote mac address
  remote-sap    Remote sap
```

#### 2.2.29.1 NO SDLC-STATION <intf> <sdlc-addr>

Eliminates the SDLC station specified from the list of stations the DLSw can connect to.

*Syntax:*

```
DLSw config>no sdlc-station <intf> <sdlc-addr>
```

*Example:*

```
DLSw config>no sdlc-station serial0/1 C1
DLSw config>
```

### 2.2.29.2 SDLC-STATION <intf> <sdlc-addr> DISABLED

Prevents DLSw connections to the specified SDLC station.

*Syntax:*

```
DLSw config>sdlc-station <intf> <sdlc-addr> disabled
```

*Example:*

```
DLSw config>sdlc-station serial0/1 C1 disabled
DLSw config>
```

### 2.2.29.3 SDLC-STATION <intf> <sdlc-addr> NO DISABLED

Re-admits DLSw connections to the specified SDLC station. This is the default value.

*Syntax:*

```
DLSw config>sdlc-station <intf> <sdlc-addr> no disabled
```

*Example:*

```
DLSw config>sdlc-station serial0/1 C1 no disabled
DLSw config>
```

### 2.2.29.4 SDLC-STATION <intf> <sdlc-addr> IDBLK <idblk>

The device can manage the XID exchange with the remote station if the local SDLC station is not capable of doing it. In order to do this, the station must be configured as SECONDARY in the SDLC link.

This command allows you to define the ID-Block that the device is going to use for XID management whenever the SDLC station does not support this function. The IDBLK is a three digit hexadecimal number that identifies the device (Physical Unit) to which it is connected. The Idblk is normally used for Physical Units in switched lines (as opposed to dedicated lines). Therefore, this value must match the parameter of the VTAM Switched Major Node that corresponds to each Physical Unit. The default value is 000.

This option is used together with the IDNUM option.

*Syntax:*

```
DLSw config>sdlc-station <intf> <sdlc-addr> idblk <idblk>
```

*Example:*

```
DLSw config>sdlc-station serial0/1 C1 idblk 017
DLSw config>
```

### 2.2.29.5 SDLC-STATION <intf> <sdlc-addr> IDNUM <idnum>

The device can manage the XID exchange with the remote station if the local SDLC station is not capable of doing it. In order to do this, the station must be configured as SECONDARY in the SDLC link.

This command allows you to define the ID-Number the device is going to use for XID management whenever the SDLC station does not support this function. The IDNUM is a five digit hexadecimal number that identifies the specific type of device (2.0) to which this is connected. The Idnum is normally used for Physical Units in switched lines (as opposed to dedicated lines). Therefore, this value must match the parameter of the VTAM Switched Major Node that corresponds to said Physical Unit. The default value is 00000.

This option is used together with the IDBLK option.

*Syntax:*

```
DLSw config>sdlc-station <intf> <sdlc-addr> idnum <idblk>
```

*Example:*

```
DLSw config>sdlc-station serial0/1 C1 idnum 54545
DLSw config>
```

### 2.2.29.6 SDLC-STATION <intf> <sdlc-addr> LOCAL-MAC <virtual-mac-addr>

This command allows you to define the MAC address associated to the SDLC station. This deals with a fictitious address, as the SDLC stations do not have MAC addresses and serves to identify the station (Physical Unit) in the DLSw Domain. The MAC address is in Token Ring format (non-canonical format). Although the device assigns a default address, it's preferable to explicitly define this.

*Syntax:*

```
DLSw config>sdlc-station <intf> <sdlc-addr> local-mac <virtual-mac-addr>
```

*Example:*

```
DLSw config>sdlc-station serial0/1 C1 local-mac 40:00:12:34:00:01
DLSw config>
```

### 2.2.29.7 SDLC-STATION <intf> <sdlc-addr> LOCAL-SAP <sap-virtual>

This command allows you to define the SAP associated to the SDLC station. This helps identify the station (Physical Unit) in the DLSW Domain. It can be explicitly assigned through the configuration or automatically assigned by the software. The SAP is for LLC use only. The default value is 4.

*Syntax:*

```
DLSw config>sdlc-station <intf> <sdlc-addr> local-sap <sap-virtual>
```

*Example:*

```
DLSw config>sdlc-station serial0/1 C1 local-sap 8
DLSw config>
```

### 2.2.29.8 SDLC-STATION <intf> <sdlc-addr> REMOTE-MAC <mac-addr>

Allows you to define the MAC address associated to the remote station. This command deals with the MAC address of the remote station to which the local SDLC station is connecting to. The MAC address is in Token Ring format (non-canonical format). This holds true even if the end remote station is in Ethernet. The default value is 00:00:00:00:00:00. However, this is not valid and you need to explicitly configure it.

*Syntax:*

```
DLSw config>sdlc-station <intf> <sdlc-addr> remote-mac <mac-addr>
```

*Example:*

```
DLSw config>sdlc-station serial0/1 C1 remote-mac 40:00:37:45:00:01
DLSw config>
```

### 2.2.29.9 SDLC-STATION <intf> <sdlc-addr> REMOTE-SAP <sap>

Defines the Service Access Point (SAP) that is going to be used when automatically attempting a connection when the link station starts 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 remote MAC Address. The default value is 0.

*Syntax:*

```
DLSw config>sdlc-station <intf> <sdlc-addr> remote-sap <sap>
```

*Example:*

```
DLSw config>sdlc-station serial0/1 C1 remote-sap 4
DLSw config>
```

## 2.2.30 SDLC-TEST-TIMER

Indicates how long you have to wait for an SDLC test response before giving up. This value is expressed in seconds. The default value is 15 seconds.

*Syntax:*

```
DLSw config>sdlc-test-timer <time>
```

*Example:*

```
DLSw config>sdlc-test-timer 10
DLSw config>
```

## 2.2.31 SEND-LLC-DISC

Allows the router to activate or deactivate DISC frame sending to terminate an LLC connection. As a default, DISC frames are sent to close LLC connections.

*Syntax:*

```
DLSw config>[no] send-llc-disc
```

### 2.2.31.1 SEND-LLC-DISC

Activates the DISC frame sending to terminate LLC connections.

*Example:*

```
DLSw config>send-llc-disc
DLSw config>
```

### 2.2.31.2 NO SEND-LLC-DISC

Deactivates DISC frame sending to terminate LLC connections.

*Example:*

```
DLSw config>no send-llc-disc
DLSw config>
```

## 2.2.32 SNA-PRIORITY

Allows you to specify circuit priorities when managing SNA traffic. The default value is MEDIUM.

*Syntax:*

```
DLSw config>sna-priority ?
  critical
  high
  low
  medium
```

### 2.2.32.1 SNA-PRIORITY CRITICAL

Specifies the SNA circuit priority as critical or the highest.

*Example:*

```
DLSw config>sna-priority critical
DLSw config>
```

### 2.2.32.2 SNA-PRIORITY HIGH

Specifies the SNA circuit priority as high.

*Example:*

```
DLSw config>sna-priority high
DLSw config>
```

### 2.2.32.3 SNA-PRIORITY MEDIUM

Specifies the SNA circuit priority as medium.

*Example:*

```
DLSw config>sna-priority medium
DLSw config>
```

#### 2.2.32.4 SNA-PRIORITY LOW

Specifies the SNA circuit priority as low.

*Example:*

```
DLSw config>sna-priority low
DLSw config>
```

### 2.2.33 TCP-NEIGHBOR

Allows you to define or eliminate DLSw neighbors that are going to connect the device through TCP. This connection can be carried out in two ways: through manual configuration of the IP neighbors addresses (this command) or with DLSw groups (see the GROUP command). You must specify the IP address of the neighbor device. In cases where you introduce the internal IP address of the device, a link is established for CONVERSION-LOCAL, and all the options are deactivated with the exception of priority. If you enter the word “promiscuous” instead of the IP address, the configured parameters will be those used by the connections established in promiscuous mode for non-configured nodes. In this case, you can’t configure the connection mode and the mode established by default is not inherited, forcing the connection to be PASSIVE.

*Syntax:*

```
DLSw config>[no] tcp-neighbor <ip-addr> | promiscuous ?
  default       Create a new tcp neighbour
  connection    Define connection mode
    default       Use default tcp connection mode
    always        Connect transport connections always
    on-demand     Connect transport connections when needed
    passive       Only accept incoming transport connections
  inactivity    Inactivity time to disconnect from neighbor
  keepalive     dls keepalive
  low-priority  Go to low priority parameters
    max-connections  Maximum number of simultaneous connections to loose priority
    min-connections  Minimum number of simultaneous connections to recover lost
                     priority
    retries          Failed circuit connections before to go to low priority
    timeout          Time to wait before recover configured priority
    retries          Failed circuit connections before to go to low priority
    timeout          Time to wait before recover configured priority
  max-sgsize    Maximum segment size
  no            Negate a command or set its defaults
    keepalive     Dls keepalive
  priority      Neighbour priority
  rx-bfsize     Reception buffer size
  tx-bfsize     Transmission buffer size
```

#### 2.2.33.1 TCP-NEIGHBOR <ip-addr> DEFAULT

Defines a DLSw neighbor the device will connect to. This will initialize with the default values. You must specify the IP address of the other device or enter “promiscuous”.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> default
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 default
DLSw config>tcp-neighbor promiscuous default
DLSw config>
```

#### 2.2.33.2 NO TCP-NEIGHBOR <ip-addr>

Eliminates a given DLSw neighbor that was previously configured through the **TCP-NEIGHBOR** command. In cases where “promiscuous” is used, the values used in this mode will be used by default in the connections established.

*Syntax:*

```
DLSw config>no tcp-neighbor <ip-addr>
```

*Example:*

```
DLSw config>no tcp-neighbor 128.185.14.1
DLSw config>no tcp-neighbor promiscuous
DLSw config>
```

#### 2.2.33.3 TCP-NEIGHBOR <ip-addr> CONNECTION DEFAULT

Configures the specific connection mode for a remote node as “default”. This is the mode configured by default. This means that the mode that has been generally defined for all the connections is inherited. Please see the **CONNECTION** command.

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 connection default
DLSw config>
```

#### 2.2.33.4 TCP-NEIGHBOR <ip-addr> CONNECTION ALWAYS

Configures the specific connection mode for a remote node as “always”. Please see the **CONNECTION** command.

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 connection always
DLSw config>
```

#### 2.2.33.5 TCP-NEIGHBOR <ip-addr> CONNECTION ON-DEMAND

Configures the specific connection mode for a remote node as “on-demand”. Please see the **CONNECTION** command.

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 connection on-demand
DLSw config>
```

#### 2.2.33.6 TCP-NEIGHBOR <ip-addr> CONNECTION PASSIVE

Configures the specific connection mode for a remote node as “passive”. Please see the **CONNECTION** command.

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 connection passive
DLSw config>
```

#### 2.2.33.7 TCP-NEIGHBOR <ip-addr> KEEPALIVE

Forces the sending of keepalive SSP messages (IAMOKAY) to periodically check that the TCP link established with the DLSw neighbor is still active. This is deactivated by default.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> keepalive
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 keepalive
DLSw config>tcp-neighbor promiscuous keepalive
DLSw config>
```

#### 2.2.33.8 TCP-NEIGHBOR <ip-addr> NO KEEPALIVE

Deactivates the sending of keepalive SSP messages (IAMOKAY) for the TCP link established with the DLSw neighbor.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> no keepalive
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 no keepalive
DLSw config>tcp-neighbor promiscuous no keepalive
DLSw config>
```

#### 2.2.33.9 TCP-NEIGHBOR <ip-addr> MAX-SGSIZE <max-size>

Configures the maximum TCP segment length to send through the link established with the neighbor. These values range between 64 and 16.384 bytes. The default value is 1.024.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> max-sgsize <max-size>
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 max-sgsize 576
DLSw config>tcp-neighbor promiscuous max-sgsize 576
DLSw config>
```

#### 2.2.33.10 TCP-NEIGHBOR <ip-addr> PRIORITY HIGH

Configures the priority of a TCP link established with the neighbor. In this case, this is configured as High. DLSw uses this parameter to determine which DLSw neighbor to choose when several can reach the destination station.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> priority high
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 priority high
DLSw config>tcp-neighbor promiscuous priority high
DLSw config>
```

#### 2.2.33.11 TCP-NEIGHBOR <ip-addr> PRIORITY MEDIUM

Configures the priority of a TCP link established with the neighbor. In this case, this is configured as Medium. DLSw uses this parameter to determine which DLSw neighbor to choose when several can reach the destination station. The default value is Medium.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> priority medium
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 priority medium
DLSw config>tcp-neighbor promiscuous priority medium
DLSw config>
```

#### 2.2.33.12 TCP-NEIGHBOR <ip-addr> PRIORITY LOW

Configures the priority of a TCP link established with the neighbor. In this case, this is configured as Low. DLSw uses this parameter to determine which DLSw neighbor to choose when several can reach the destination station.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> priority low
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 priority low
DLSw config>tcp-neighbor promiscuous priority low
DLSw config>
```

#### 2.2.33.13 TCP-NEIGHBOR <ip-addr> RX-BFSIZE <rx-size>

Configures the size of the reception buffer for the link established with the neighbor. These values range between 1.024 and 32.768. The default value is 5.120.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> rx-size <rx-size>
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 rx-bfsize 8192
DLSw config>tcp-neighbor promiscuous rx-bfsize 8192
DLSw config>
```

#### 2.2.33.14 TCP-NEIGHBOR <ip-addr> TX-BFSIZE <tx-size>

Configures the size of the transmission buffer for the link established with the neighbor. These values range between 1.024 and 32.768. The default value is 5.120.

*Syntax:*

```
DLSw config>tcp-neighbor <ip-addr> tx-size <tx-size>
```

*Example:*

```
DLSw config>tcp-neighbor 128.185.14.1 tx-bfsize 8192
DLSw config>tcp-neighbor promiscuous tx-bfsize 8192
DLSw config>
```

### 2.2.34 EXIT

Returns to the Config> prompt.

*Syntax:*

```
DLSw config>exit
```

*Example:*

```
DLSw config>exit
Config>
```

# Chapter 3 Monitoring the DLSw Protocol

## 3.1 About DLSw Monitoring Commands

DLSw monitoring commands are available at the DLSw+ prompt.

Monitoring activities consist of:

(1) Monitoring the protocols and network interfaces currently in use by the router.

(2) Displaying Event Logging System (ELS) messages relating to router activities and performance.

## 3.2 Accessing the DLSw Monitoring Environment

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

*Example:*

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

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

*Example:*

```
+protocol dls

Data Link Switching Console

DLSw+
```

## 3.3 Monitoring Commands

Enter DLSw monitoring commands at the DLSw+ prompt.

| Command | Function |
|---|---|
| *? (HELP)* | Lists the monitoring commands and any parameters associated with them. |
| *BAN* | Displays the BAN prompt (Boundary Access Node). |
| *DELETE* | Deactivates DLSw sessions between stations. |
| *LIST* | Displays information for SDLC, QLLC link stations, SAPs, TCP connections, and DLSw groups. This command also offers detailed information on the aptitudes and statistics of TCP connections. |
| *NETBIOS* | Displays the NetBIOS prompt. |
| *EXIT* | Exits the DLSw configuration process and returns to the + prompt. |

### 3.3.1 ? (HELP)

Lists the commands available at the current prompt level. You can also enter **?** after a specific command name to list its options.

*Syntax:*

```
DLSw+?
  ban         BAN console
  delete      Delete section
  list        Show protocol state
  netbios     NetBIOS console
  exit
```

### 3.3.2 BAN

Displays the Boundary Access Node console prompt.

*Syntax:*

```
DLSw+ban
```

*Example:*

```
DLSw+ban
Boundary Access Node Console
BAN+
```

### 3.3.3 DELETE

Deletes a DLSw connection between two stations.

*Syntax:*

```
DLSw+delete?
  dlsw    Shutdown DLSw sessions
```

#### 3.3.3.1 DELETE DLSW <id-session>

Disconnects the dlsw session established between two stations. You need to enter the identifier number that appears on the list of stations.

*Example:*

```
DLSw+delete dlsw 1
DLSw+
```

### 3.3.4 LIST

Displays DLSw information on local and remote LLC stations, SDLC, QLLC, SAPs, TCP neighbors, groups and priorities.

*Syntax:*

```
DLSw+LIST ?
  dlsw                  Show DLSw section
  groups                Show groups
  icanreach-stations    Show icanreach section
    mac                   Show Icanreach MAC Address List
    netbios               Show Icanreach NetBIOS Name List
  llc2                  Show LLC section
  priority              Show priority section
  qllc-stations         Show QLLC section
  remote-stations       Show remote stations section
  sdlc-stations         Show SDLC section
  tcp-neighbors         Show TCP section
```

#### 3.3.4.1 LIST DLSW

Displays related information on DLSW.

*Syntax:*

```
DLSw+list dlsw ?
  cache          Show MAC<->IP cache contents
    all            All entries
    range          Select a range of entries
  global         Show global parameters
  memory         Show memory state
  sessions       Show DLSw sessions
    all            All sessions
    ban            Only BAN sessions
    destination    Only sessions by destination
```

```
    detail          Detailed session
    ip              Select sessions by neighbor
    netbios         Only NetBIOS sessions
    range           Select a range of sessions
    source          Only sessions by origin
    state           Only sessions by state
```

#### 3.3.4.1.1 LIST DLSW CACHE ALL

Lists all the entries in the DLSw MAC address cache. This cache contains a database with the most recent conversions of IP neighbors to MAC addresses. This provides the MAC address, the lifetime (in seconds) in 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+
```

#### 3.3.4.1.2 LIST DLSW CACHE RANGE <first><last>

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

*Example:*

```
DLSw+list dlsw cache range 2 2
MAC Address           Secs to live   IP Adress(es)    Largest Frame
10:00:5A:F1:81:A4     1170           128.185.236.84   2052
DLSw+
```

#### 3.3.4.1.3 LIST DLSW GLOBAL

Displays global information on DLS parameters.

*Example:*

```
DLSw+list dlsw global
DLSw is                              ENABLED
LLC2 send Disconnect is              ENABLED
Default TCP cnx mode is              ALWAYS
Promiscuous mode is                  DISABLED
MAC Exclusivity mode is              DISABLED
NetBIOS Exclusivity mode is          DISABLED

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 as follows:

| | |
|---|---|
| *DLSw is* | Status of the DLSw protocol, enabled or disabled. |
| *LLC2 send Disconnect is* | Status preventing the router from terminating an LLC2 connection upon the loss of the TCP connection. Values are enabled or disabled. |

| | |
|---|---|
| *Default TCP cnx mode is* | Indicates the default behavior mode for the local node in order to connect to remote nodes. The modes are always, on-demand and passive. |
| *Promiscuous mode is* | Indicates if the promiscuous mode is activated or not. This mode allows the local node to accept connections from remote nodes not configured in the TCP neighbors list. |
| *MAC Exclusivity mode is* | Indicates if the MAC address lists announced in the CAPEX phase are Exclusive. |
| *NetBIOS Exclusivity mode is* | Indicates if the NetBIOS name lists announced in the CAPEX phase are Exclusive. |
| *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* | Maximum number of DLSw sessions that the router will support. |
| *DLSw global memory allotment* | Maximum amount of memory DLSw may use. |
| *LLC per-session memory allotment* | Maximum amount of memory each LLC session may use. |
| *SDLC per-session memory allotment* | Maximum amount of memory each SDLC/QLLC session may use. |
| *NetBIOS UI-frame memory allotment* | Number of bytes the router allocates as a buffer for NetBIOS UI frames. |
| *Database age timer* | Maximum time active database entries can be held. |
| *Max wait timer for ICANREACH* | Time waited for a response to a CANUREACH before giving up. |
| *Wait timer for LLC test response* | Maximum time (in seconds) the router waits for an LLC TEST response before re-transmitting an LLC TEST frame. |
| *Wait timer for SDLC test response* | Maximum 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 broadcasts. |
| *Neighbor priority wait timer* | Time DLSw waits for another ICANREACH response before selecting a neighbor. |

#### 3.3.4.1.4 LIST DLSW MEMORY

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 session assignments, control messages and TCP reception buffers.

**Note**

You need to use the DLS-GLOBAL-MEMORY configuration 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+
```

#### 3.3.4.1.5 LIST DLSW SESSIONS ALL

Displays current information on all established DLSw connections, including source, destination, state, flags, destination IP address and ID (identifier).

*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 as follows:

| | | |
|---|---|---|
| *Local* | | The session's source MAC address. **Warning**: for space reasons, the notation is TKR. However, the separators cannot be viewed. |
| *Remote* | | The session's destination MAC address. **Warning**: for space reasons, the notation is TKR. However, the separators cannot be viewed. |
| *State* | | Current state of the session: |
| | *DISCONNECTED* | The initial state with no circuit or connection established. |
| | *RSLV_PEND* | The target DLSw is waiting for an SSP_STARTED indication following an SSP_START request. |
| | *CIRC_PEND* | The target DLSw is waiting for 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 waiting for the restart of the data link and an SSP_RESTARTED response to an SSP_RESTART message. |
| | *CONN_PEND* | The source DLSw is waiting for an SSP_CONTACTED response to an SSP_CONTACT message. |
| | *CONT_PEND* | The target DLSw is waiting for an SSP_CONTACTED confirmation to an SSP_CONTACT message. |
| | *CONNECT_STATE* | The source DLSw is waiting for an SSP_CONTACTED response to an SSP_CONTACT message. |
| | *DISC_PEND* | The DLSw that originated the disconnect is waiting for an SSP_HALTED response to an SSP_HALT message. |
| | *HALT_PENDING* | The remote DLSw is waiting for an SSP_HALTED indication following an SSP_HALT request. |
| | *HALT_RSTRT* | The remote DLSw is waiting for an SSP_HALTED indication following an SSP_HALT request. |
| | *RESTART_PEND* | The remote DLSw is waiting for an SSP_HALTED indication following an SSP_HALT request. |
| | *RESET_PEND* | The remote DLSw is waiting for an SSP_HALTED indication following an SSP_HALT request. |
| *Flags* | | Flags can be as follows. |
| | A- CONTACT MSG PENDING | |
| | B- SAP RESOLVE PENDING | |
| | C- EXIT BUSY EXPECTED | |
| | D- TCP BUSY | |
| | E- DELETE PENDING | |
| | F- CIRCUIT INACTIVE | |
| *Rem IP Addr* | | IP address of the remote DLSw peer. |
| *Id* | | Number used to identify the session. Use this number in any command that requires the session ID. |

#### 3.3.4.1.6 LIST DLSW SESSIONS BAN <ban-port>

Displays current information on all the established connections through bridge ports defined as BAN. The bridge port number defined as BAN is entered as a parameter. If you enter a 0, then all BAN ports defined are listed.

*Example:*

```
DLSw+list dlsw sessions ban 2
No active sessions
DLSw+
```

#### 3.3.4.1.7 LIST DLSW SESSIONS DEST <mac-addr>

Displays DLS session information by destination MAC address.

*Example:*

```
DLSw+list dlsw sessions dest 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+
```

#### 3.3.4.1.8 LIST DLSW SESSIONS DETAIL <identifier>

Displays detailed information on DLS session selected by its identifier.

*Example:*

```
DLSw+list dlsw sessions detail 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 as follows:

| | |
|---|---|
| *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* | 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. |

#### 3.3.4.1.9 LIST DLSW SESSIONS IP <ip-addr>

Displays information on the sessions established with the IP link.

*Example:*

```
DLSw+list dlsw sessions ip 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+
```

#### 3.3.4.1.10 LIST DLSW SESSIONS NETBIOS

Lists information about the current active circuits that support NetBIOS.

*Example:*

```
DLSw+list dlsw sessions netbios
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/F0  500000000003/F0   CONNECTED           128.185.236.51  2
DLSw+
```

#### 3.3.4.1.11 LIST DLSW SESSIONS RANGE <first><last>

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 1 1
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
-----------      -------------     ---------  -----    -----------    --
400000000003/04  500000000003/04   CONNECTED           128.185.236.51  2
DLSw+
```

#### 3.3.4.1.12 LIST DLSW SESSIONS SOURCE <mac-addr>

Displays all the DLSw session information by local MAC Address.

*Example:*

```
DLSw+list dlsw sessions source 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-STATIONS CONFIGURATION ALL or LIST QLLC-STATIONS CONFIGURATION to obtain it.

#### 3.3.4.1.13 LIST DLSW SESSIONS STATE <status>

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

*Syntax:*

```
DLSw+list dlsw sessions state ?
  disconnected
  resolve-pending
  circuit-pending
  circuit-established
  circuit-restart
  connect-pending
  contact-pending
  connected
  disconnect-pending
  halt-pending
  restart-pending
  wait-noack
  circuit-start
  halt-pending-noack
```

*Example:*

```
DLSw+list dlsw sessions state connected
Local  (TKR)     Remote  (TKR)     State      Flags    Rem IP Addr    Id
```

```
------------     --------------    ---------  -----    -----------    --
400000000003/04  500000000003/04   CONNECTED           128.185.236.51  2
DLSw+
```

### 3.3.4.2 LIST GROUPS

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

*Syntax:*

```
DLSw+list groups
```

*Example:*

```
DLSw+list groups
Group  Role      Xmit Bufsize   Rcv Bufsize   Max Segsize   Keepalive   Priority
Inact. Time      Max cnx.       Min cnx.      Retries       Timeout
1      CLIENT    5120           5120          1024          DISABLED    MEDIUM
        0           0              0             0               0
DLSw+
```

The meaning of each field is as follows:

| | |
|---|---|
| *Group* | Group number. |
| *Role* | Type of group. |
| *Xmit Bufsize* | Size of the TCP transmit buffer within the 1.024 - 32.768 range. The transmission buffer size must at least double the maximum segment size. Default value is 5.120. |
| *Rcv Bufsize* | Size of the TCP receive buffer within the 1.024 - 32.768 range. The reception buffer size must at least double the maximum segment size. Default is 5.120. |
| *Max Segsize* | Maximum size of the TCP segment, within the 64 - 16.384 range. Default is 1.024. |
| *Keepalive* | The status of the keepalive functionality, enabled or disabled. |
| *Priority* | Displays the priority of the DLSw group as HIGH, MEDIUM or LOW. |
| *Inact. Time* | Displays the time during which the link should not have circuits established in order to deactivate it. Default is 0 which deactivates this functionality. |
| *Max cnx.* | Displays the maximum number of connections which if surpassed penalizes the link by dropping its priority to LOW. Default is 0 which deactivates this functionality. |
| *Min cnx.* | Displays the minimum number of connections which if reached or is below this value, the link then recovers its priority. Default is 0. |
| *Retries* | Displays the maximum number of unsuccessful connection attempts, which if surpassed penalizes the link by dropping its value to LOW. Default is 0 which deactivates this functionality. |
| *Timeout* | Displays the time that the link must remain with LOW priority due to an excess of unsuccessful connection attempts before recovering its priority. Default is 0 which prevents priority recovery if the link is lost for this reason. |

### 3.3.4.3 LIST ICANREACH-STATIONS MAC

Displays information on the list of stations announced to the remote nodes, previously configured through the **ICANREACH-STATION MAC** command.

*Example:*

```
DLSw config>list icanreach-stations mac

MAC Address List Exclusivity mode: ENABLED

  MAC Address          Mask
---------------------------------------
40:37:45:ff:01:00    ff:ff:ff:ff:ff:fc
40:00:00:00:00:00    ff:ff:ff:ff:ff:ff
50:00:00:00:00:00    f0:00:00:00:00:00

DLSw config>
```

#### 3.3.4.4 LIST ICANREACH-STATIONS NETBIOS

Displays information on the list of stations announced to the remote nodes, previously configured through the **ICANREACH-STATION NETBIOS** command.

*Example:*

```
DLSw config>list icanreach-stations netbios

NetBIOS Name List Exclusivity mode: DISABLED

  I/G  NetBIOS Name
-------------------------------------------------------
   I    "STATION-1"
   I    "<0102>MSBROWSE<0201>"
   I    "STATION-R??"
   I    "STATION-S*"
   G    "GROUP-1"
   I    "<0102>__MSBROWSE__<02><01>"

DLSw config>
```

#### 3.3.4.5 LIST LLC2

Displays LLC2-related information. The options (OPEN Saps, SAP PARAMETERS, and SESSIONS) for LLC2 are described in the following sections.

*Syntax:*

```
DLSw+list llc2 ?
  open-saps         Show open saps
  sap-parameters    Show sap parameters
  sessions          Show LLC sessions
    all               All sessions
    ban               Only BAN sessions
    netbios           Only NetBIOS sessions
    range             Select a range of sessions
```

##### 3.3.4.5.1 LIST LLC2 OPEN-SAPS

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

*Example:*

```
DLSw+list llc2 open-saps
Interface   SAP
ethernet0/0     0
ethernet0/0     4
DLSw+
```

##### 3.3.4.5.2 LIST LLC2 SAP-PARAMETERS

Displays configuration information on SAP parameters. The command only displays configurations that have changed. If you did not use the LLC-SAP command, no output is generated.

*Example:*

```
DLSw+list llc2 sap-parameters
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 as follows:

| | |
|---|---|
| *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. |
| *wt* | 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. |

#### 3.3.4.5.3 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's 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 in the circuit. 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. |

#### 3.3.4.5.4 LIST LLC2 SESSIONS BAN <ban-port>

Displays current information on the LL2 connections established through bridge ports defined as BAN. The bridge port number defined as BAN is entered as a parameter. If you enter 0, then all the defined BAN ports are listed.

*Example:*

```
DLSw+list llc2 sessions ban 0
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+
```

#### 3.3.4.5.5 LIST LLC2 SESSIONS NETBIOS

Displays current information on established LL2 connections that support NetBIOS.

*Example:*

```
DLSw+list llc2 sessions netbios
     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+
```

#### 3.3.4.5.6 LIST LLC2 SESSIONS RANGE <first><last>

Displays current information for the selected range of LLC2 sessions.

*Example:*

```
DLSw+list llc2 sessions range 1 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+
```

#### 3.3.4.6 LIST PRIORITY

Displays information on the different priorities for transport protocols.

*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+
```

#### 3.3.4.7 LIST SDLC-STATIONS

Displays information on SDLC stations defined in DLSw.

*Syntax:*

```
DLSw+list sdlc-stations ?
  configuration    Show SDLC configuration
    <interface>      Interface name
    all              All interfaces
  sessions         Show SDLC sessions
```

##### 3.3.4.7.1 LIST SDLC-STATIONS CONFIGURATION <interface>

Displays the parameters configured for the PUs connected by the selected SDLC interface.

*Example:*

```
DLSw+list sdlc configuration serial0/1
Net        Addr  Status   Idblk   Idnum  Local SAP/MAC         Remote SAP/MAC
serial0/1  C1    Enabled  000     00000  04/40:18:99:7E:05:C1  04/40:1A:AB:92:00:C1
DLSw+
```

##### 3.3.4.7.2 LIST SDLC-STATIONS CONFIGURATION ALL

Displays the parameters configured for the Physical Unit (PC) connected by all the SDLC interfaces.

*Example:*

```
DLSw+list sdlc-stations configuration all
Net        Addr  Status   Idblk   Idnum  Local SAP/MAC         Remote SAP/MAC
serial0/1  C1    Enabled  000     00000  04/40:18:99:7E:05:C1  04/40:1A:AB:92:00:C1
DLSw+
```

##### 3.3.4.7.3 LIST SDLC-STATIONS SESSIONS

Displays information on all the DLS sessions over SDLC interfaces in the router.

*Example:*

```
DLSw+list sdlc sessions
Net        Addr  Local SAP/MAC          Remote SAP/MAC        OutQ   State
serial0/1  C1    04/40:00:00:00:00:01   04/40:00:00:00:00:02  0      Contacted
DLSw+
```

#### 3.3.4.8 LIST QLLC-STATIONS

Displays information on the QLLC stations defined in DLSw.

*Syntax:*

```
DLSw+list qllc ?
  configuration    Show QLLC configuration
  sessions         Show QLLC sessions
```

#### 3.3.4.8.1 LIST QLLC-STATIONS CONFIGURATION

Displays the parameters configured for the PUs connected by QLLC.

*Example:*

```
DLSw+list qllc-stations 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 as follows:

| | |
|---|---|
| *Remote NUA* | X.25 network number identifying the remote QLLC station. This number discriminates the incoming calls. If there are any wildcards ('X'), outgoing calls are not permitted from this station. |
| *Local NUA* | X.25 network number identifying the local QLLC station. This number discriminates the incoming calls. In outgoing calls this is used as NUA calling. If there are 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 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 establish connection with the QLLC station. |
| *QLLC Address* | Address to use in QLLC messages. Hexadecimal value between 00 and FE. If 00 is programmed, the session will use FF and learn the address from the remote QLLC station. |
| *Status* | Indicates the QLLC station's status (Active or Inactive) when it comes to carrying out connections. |

#### 3.3.4.8.2 LIST QLLC-STATIONS SESSIONS

Displays information on all QLLC DLSw sessions in the router.

*Example:*

```
DLSw+list qllc-stations 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 as follows

| | |
|---|---|
| *Remote NUA* | X.25 network number identifying the remote QLLC station. This number discriminates incoming calls. If there are any wildcards ('X'), outgoing calls are not permitted from this station. |
| *Local NUA* | X.25 network number identifying the local QLLC station. This number discriminates the incoming calls. In outgoing calls, this is used as NUA calling. If there are 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 establish a connection with the QLLC station. |
| *QLLC Address* | Address to use in the QLLC messages. Hexadecimal value between 00 and FE. If 00 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.

#### 3.3.4.9 LIST REMOTE-STATIONS <ip-addr>

Displays the configuration-defined remote stations, whose traffic must be prioritized by a TCP link.

*Syntax:*

```
DLSw+list remote-stations <ip-addr>
```

*Example:*

```
DLSw+list remote-stations 128.152.14.3

Remote stations defined for: 128.152.14.3

  MAC Address           Mask
--------------------------------------
40:37:45:ff:01:04    ff:ff:ff:ff:ff:ff

DLSw+
```

#### 3.3.4.10 LIST TCP-NEIGHBORS

Displays information on TCP connections in the DLSw router.

*Syntax:*

```
DLSw+list tcp-neighbors ?
  capabilities     Connection capabilities
  configuration    Configuration
  promiscuous      Default promiscuous parameters
  sessions         All connections
  statistics       Detailed connection
```

##### 3.3.4.10.1 LIST TCP-NEIGHBORS CAPABILITIES <ip-addr>

Displays the information received from an associated router on its exchange message capabilities.

*Example:*

```
DLSw+list tcp-neighbors capabilities 128.152.14.3
Vendor ID                   000564
Vendor product version:     10.7.21
Initial pacing window:      12
Preferred TCP connections:  1
Supported SAPs:             00 04 08 0c f0
MAC List Exclusivity:       Yes
NetBIOS List Exclusivity:   Yes
MAC Address List:           (value - mask)
                            40:00:00:00:00:00 - ff:ff:ff:ff:ff:ff
                            40:37:45:ff:01:00 - ff:ff:ff:ff:ff:fc
```

```
NetBIOS Name List:          (I/G   - Name)
                            I - "<0102>MSBROWSE<0201>"
                            I - "FAST??"
                            I - "SLOW*"
                            I - "<3E>HELLO"
                            I - "<0102>__MSBROWSE__<02><01>"
                            G - "GROUP1"
DLSw+
```

#### 3.3.4.10.2 LIST TCP-NEIGHBORS CONFIGURATION

Displays information on all TCP sessions configured.

*Example:*

```
DLSw+list tcp-neighbors configuration
Neighbor      Xmit Buf    Rcv Buf    Max Seg    Kalive   Conn Mode  Priority
Inact. Time      Max cnx.       Min cnx.      Retries       Timeout
--------      ---------   --------   --------   -------  ---------  --------
128.185.122.234   5120       5120       1024    DISABLED DEFAULT     MEDIUM
        0           0              0             0                0
DLSw+
```

#### 3.3.4.10.3 LIST TCP-NEIGHBORS PROMISCUOUS

Displays the configuration information incoming TCP connections will use by default (in promiscuous mode).

*Example:*

```
DLSw+list tcp-neighbors promiscuous
Neighbor      Xmit Buf    Rcv Buf    Max Seg    Kalive   Conn Mode  Priority
Inact. Time      Max cnx.       Min cnx.      Retries       Timeout
--------      ---------   --------   --------   -------  ---------  --------
PROMISCUOUS       5120       5120       1024    DISABLED DEFAULT     MEDIUM
        0           0              0             0                0
DLSw+
```

#### 3.3.4.10.4 LIST TCP-NEIGHBORS SESSIONS

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

Some asterisks may appear in the following fields:

- *Active Sess:* Link priority has dropped to LOW due to an excess of simultaneously open circuits.
- *Sess Creates:* Link priority has dropped to LOW due to an excess of unsuccessful circuit connection attempts.

*Example:*

```
DLSw+list tcp-neighbors sessions
    Group    IP Address      Conn State   Version  Active Sess  Sess Creates
   ------- --------------- -------------- -------- -----------  ------------
1          128.185.122.234 ESTABLISHED    AIW V1R0         2 *           4 *
DLSw+
```

#### 3.3.4.10.5 LIST TCP-NEIGHBORS STATISTICS <ip-addr>

Displays the usage statistics of TCP sessions.

*Example:*

```
DLSw+list tcp-neighbors statistics 128.185.122.234
                                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+
```

### 3.3.5 NETBIOS

Displays the NetBIOS monitoring prompt.

*Syntax:*

```
DLSw+netbios
```

*Example:*

```
DLSw+netbios
NetBIOS Support User Console
NetBIOS+
```

### 3.3.6 EXIT

Returns to the + prompt.

*Syntax:*

```
DLSw+exit
```

*Example:*

```
DLSw+exit
+
```

# Chapter 4 Using Boundary Access Node

## 4.1 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 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 of 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. As a result, capital equipment costs are significantly reduced since another router, a Token Ring, and a TIC-3745 interface card attached to the remote SNA device are no longer needed.

BAN achieves this by enabling IBM type 2.0 and 2.1 end nodes attached to a router to directly connect, via Frame Relay, with the front end processor (FEP) affixed to an IBM mainframe.

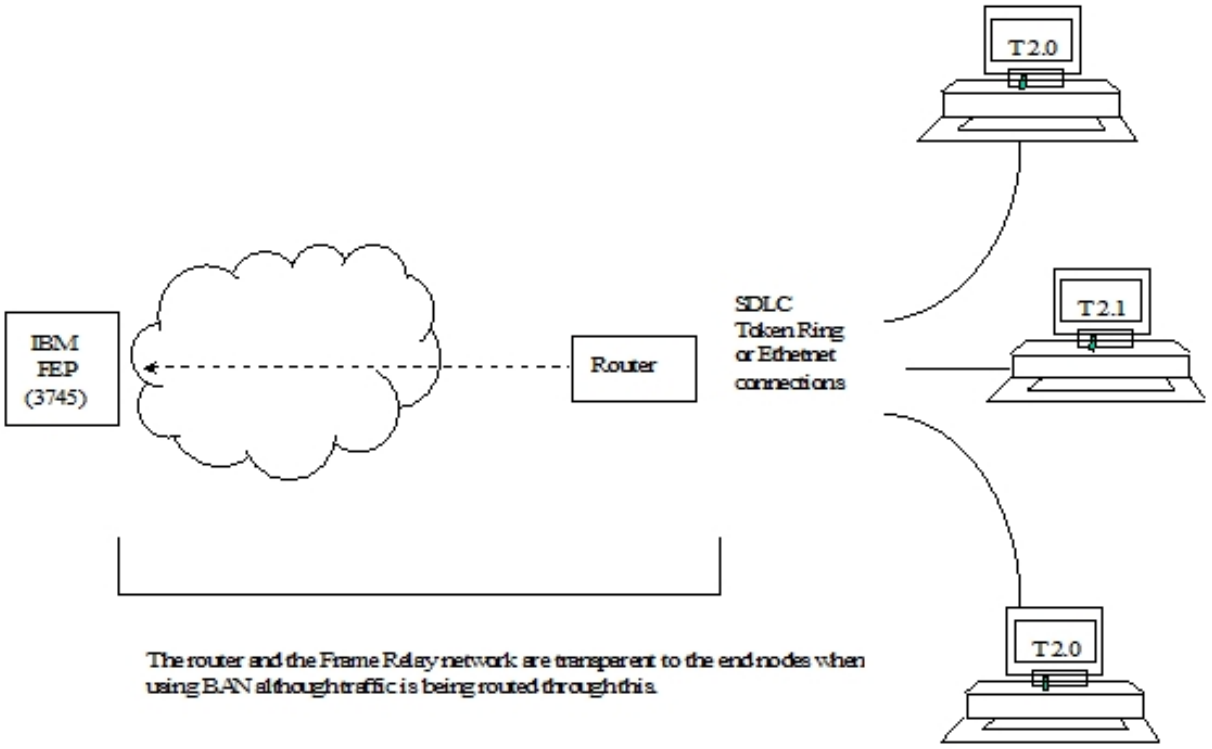


*Fig. 5: Direct Connection of End Nodes to IBM FEP Using BAN.*

### 4.1.1 How BAN Works

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

With BAN, only one DLCI is generally 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.

### 4.1.2 Bridged and DLSw-terminated BAN

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

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

The figure shows 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 whatever frames it receives to bridged Token Ring format (RFC 1490) frames, and bridges directly to the NCP.

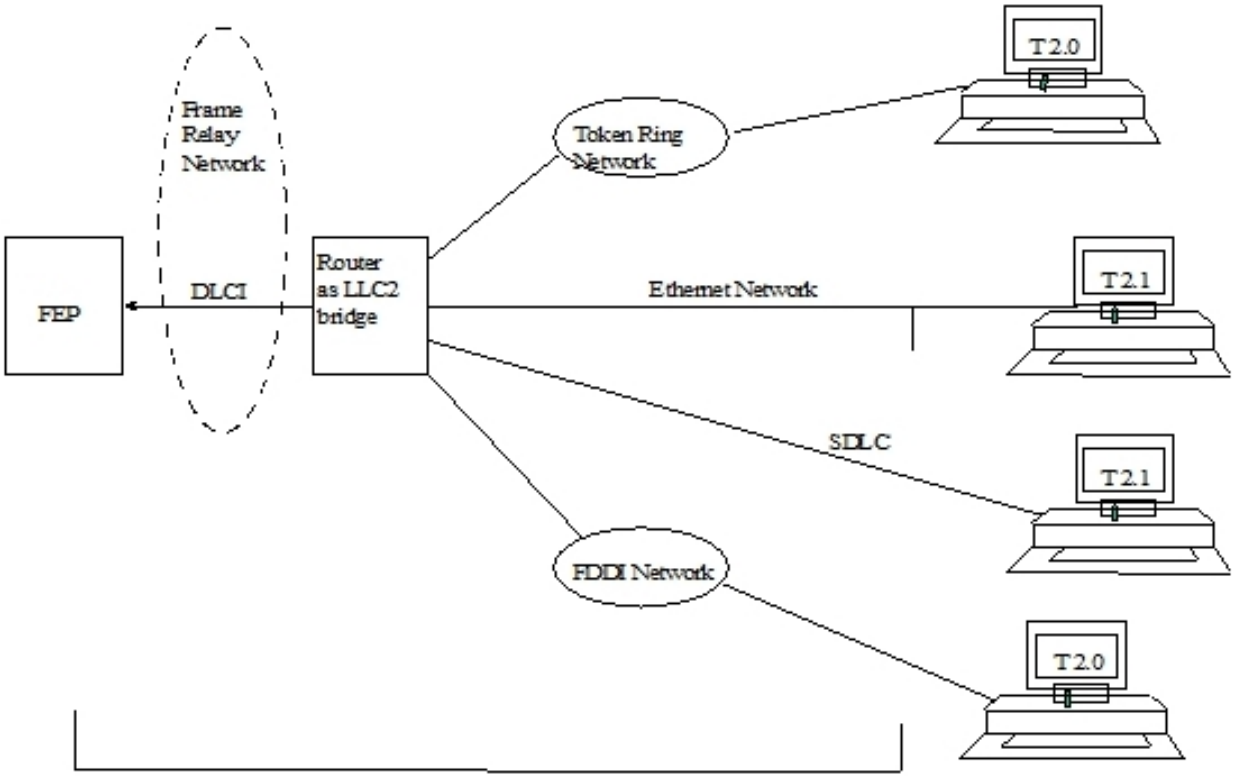


*Fig. 6: Bridged LLC2 connection with BAN.*

BAN Type 1.

In this case, the router acts as a bridge between the FEP and end stations. DLSw does not terminate the 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.

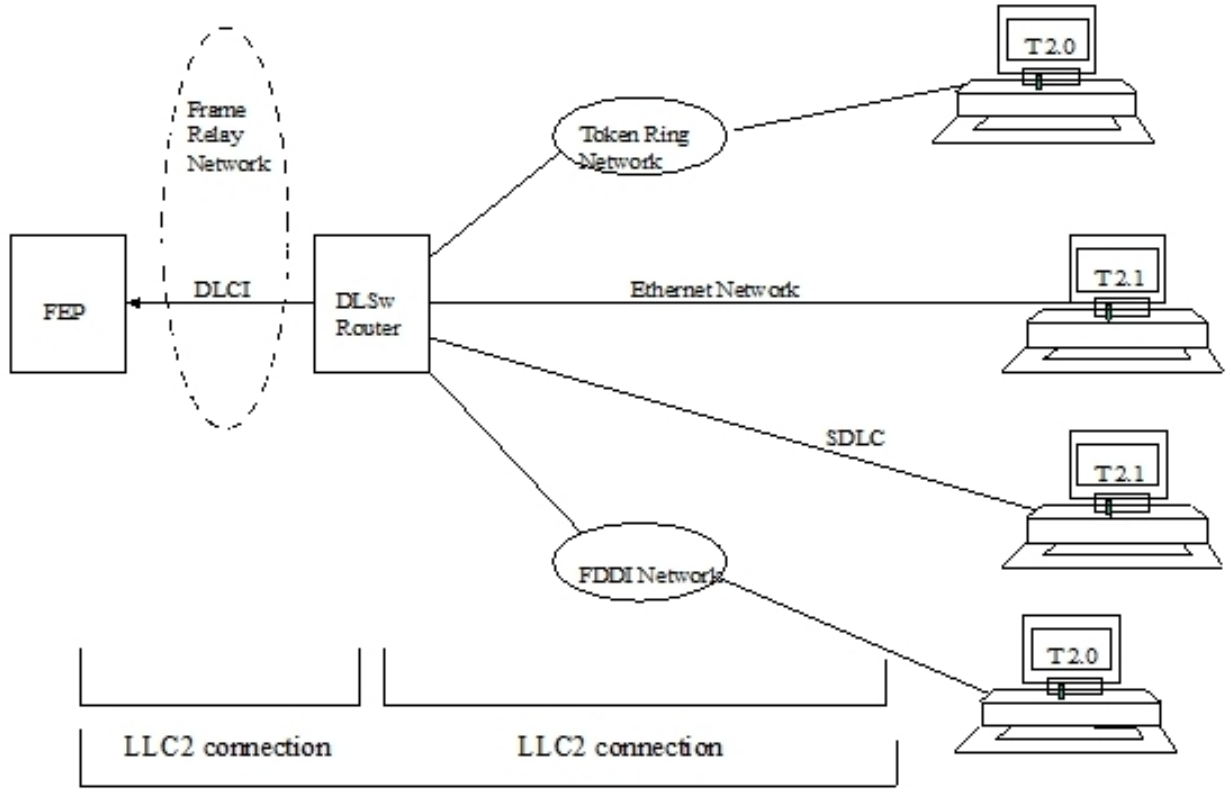


*Fig. 7: Virtual BAN DLSw LLC2 connection.*

BAN type 2.

### 4.1.3 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 the 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.

## 4.2 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.

### 4.2.1 Configuring Frame Relay

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

```
Config>network serial0/0

-- Frame Relay user configuration --
serial0/0 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.

```
serial0/0 FR Config>pvc 16 name 20-ncp10
serial0/0 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 or fewer characters. 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 router with the IBM FEP when using BAN. The next step is to configure 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.

### 4.2.2 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
-- ASRT Bridge user configuration --
ASRT config>bridge
ASRT config>port ethernet0/0 1
ASRT config>
```

At the ASRT config> prompt, add a port. The router prompts you for the interface name or 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>port serial0/0 5 20-ncp10
ASRT config>
```

The next step is to enable source routing and to define the source routing segment number for the FR port.

```
ASRT config>source-routing 2 456
ASRT config>
```

Once done, disable transparent bridging on the bridge port as shown:

```
ASRT config>no transparent 2
ASRT  config>
```

### 4.2.3 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 to handle BAN traffic.

```
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>ban-port 5 dlci-mac 40:00:00:00:00:01
BAN config>
```

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 Boundary Node Identifier MAC address has not been entered, since the default address (4F:FF:00:00:00:00) is going to be used. The type of BAN to be used will be bridged (type 1) and in normal or direct mode.

**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 in the FEP.

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

### 4.2.4 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 ehternet0/0 sna
DLSw config>
```

Entering the OPEN-SAP command for interface ethernet0/0 opens the SAP on the LAN interface. You issue the same command to open the SAPs on the FR interface.

```
DLSw config>open-sap serial0/0 sna
DLSw config>
```

## 4.3 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.

### 4.3.1 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.

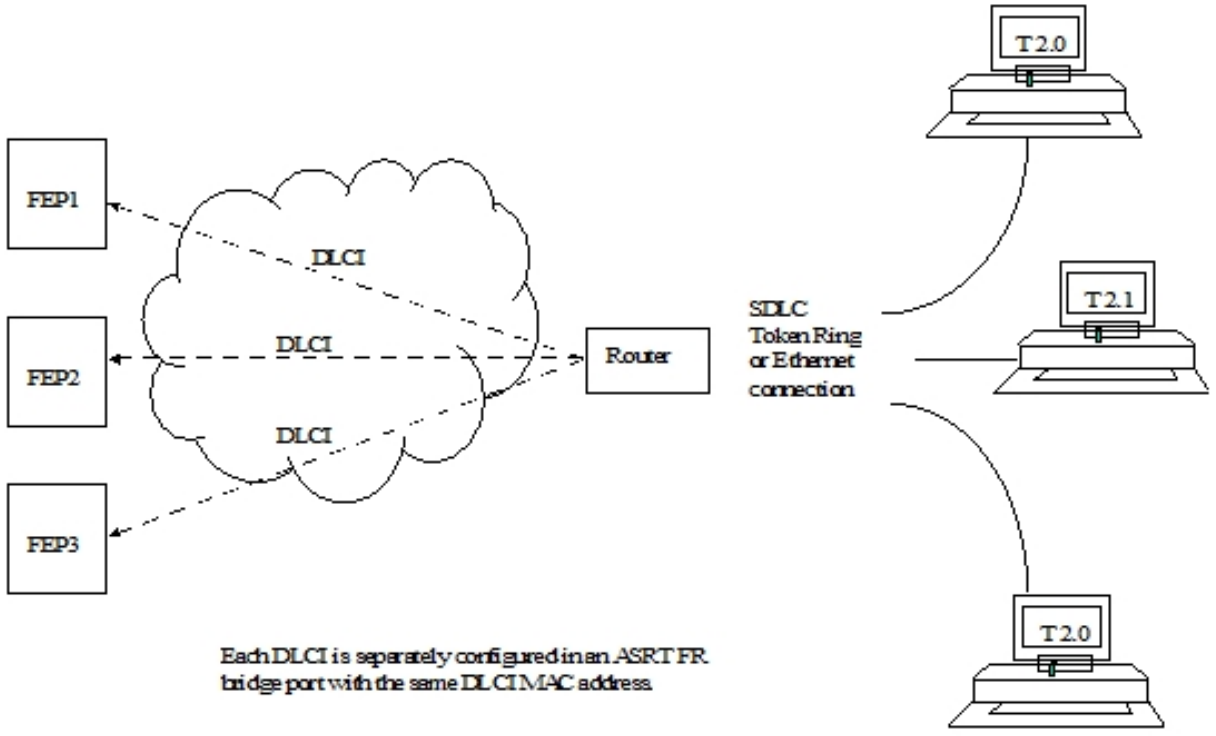


*Fig. 8: BAN Configuration with Multiple DLCIs.*

### 4.3.2 Setting up multiple DLCIs

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

When setting up multiple connections, keep in mind that each Frame Relay DLCI corresponds to 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.

## 4.4 Checking the BAN configuration

When you restart the router, the BAN bridge appears as an 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 demonstrated by this example, 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 (detailing, moreover, if the mode is normal or inverse).

To check that BAN has initialized properly on startup, you can use the router's monitoring environment (at P 3):

```
+protocol asrt
ASRT>virtual-bridge 0
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:

(1) **Init Fail** indicates that a configuration problem exists.

(2) **Down** indicates that the DLCI FR is not running.

(3) **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.

# Chapter 5 Boundary Access Node Configuration

## 5.1 BAN Configuration

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

To access the configuration environment, enter PROCESS 4 (or P 4). This takes you to the Config> prompt:

*Example:*

```
*PROCESS 4
Config>
```

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

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

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

*Example:*

```
Config>protocol dls
-- DLSw protocol user configuration --
DLSw config>ban
-- Boundary Access Node user Configuration --
BAN config>
```

## 5.2 Configuration commands

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

| Command | Function |
|---|---|
| *? (HELP)* | Lists all configuration commands or associated parameters. |
| *BAN-PORT* | Aggregates or modifies a BAN port. |
| *LIST* | Displays the current BAN configuration and tells you if the port has initialized properly or not. |
| *NO* | Eliminates a BAN port. |
| *EXIT* | Exits the BAN configuration process and returns to the DLSw config> or ASRT config> prompts. |

### 5.2.1 ?(HELP)

Lists the commands available at the current prompt level. You can also enter ? after a specific command name to list its options.

*Syntax:*

```
BAN config>?
  ban-port    Configure BAN port
  list        List configuration
  no          Negate a command or set its defaults
    ban-port    Delete BAN port
  exit
```

### 5.2.2 BAN-PORT <port number>

Creates and modifies BAN ports. As with any parameter, you must specify the port number assigned in the bridge. You can specify various options simultaneously in the same command.

*Syntax:*

```
BAN config> BAN config>[no] ban-port <port number> ?
  dlci-mac      Dlci mac address
  bni-mac       Boundary node identifier
  no            Negate a command or set its defaults
    terminated    Bridged traffic
    inverse       Normal traffic
  terminated    Dlsw terminated traffic
  inverse       Inverse traffic
```

#### 5.2.2.1 BAN-PORT <port number> DLCI-MAC <mac-addr>

Allows you to specify the MAC address to configure the outgoing traffic filter for the bridge port. All outgoing traffic through this port whose destination is not the destination defined by the DLCI-MAC parameter will be filtered and dropped. The default value is 00:00:00:00:00:00

*Syntax:*

```
BAN config>ban-port <port number> dlci-mac <mac-addr>
```

*Example:*

```
BAN config>ban-port 2 dlci-mac 40:37:45:00:00:01
BAN config>
```

In this example, bridge port number 2 has been defined as the BAN port that will permit outgoing traffic where the destination address is 40:37:45:00:00:01

#### 5.2.2.2 BAN-PORT <port number> BNI-MAC <mac-addr>

Allows you to specify the MAC address configured in the FEP or Boundary Node Identifier. The device will translate the traffic destination address (DLCI-MAC) to the address defined in this parameter. The default value is the one configured by default in the FEPs: 4F:FF:00:00:00:00.

*Syntax:*

```
BAN config>ban-port <port number> bni-mac <mac-addr>
```

*Example:*

```
BAN config>ban-port 2 bni-mac 4F:FF:FF:FF:FF:FF
BAN config>
```

In this example, the FEP has modified the default BNI and the destination address (DLCI-MAC) for traffic leaving bridge port number 2 with address 4F:FF:FF:FF:FF:FF must be translated.

#### 5.2.2.3 BAN-PORT <port number> TERMINATED

Allows you to define the port so that it will only transmit traffic whose session has been terminated by DLSw (BAN Type 2), and does not permit bridged traffic (BAN Type 1).

*Syntax:*

```
BAN config>ban-port <port number> terminated
```

*Example:*

```
BAN config>ban-port 2 terminated
BAN config>
```

#### 5.2.2.4 BAN-PORT <port number> NO TERMINATED

Allows you to define the port so that it transmits both traffic whose session has been terminated by DLSw (BAN Type 2) and bridged traffic (BAN Type 1). By default, this port is defined as not terminated (BAN Type 1).

*Syntax:*

```
BAN config>ban-port <port number> no terminated
```

*Example:*

```
BAN config>ban-port 2 no terminated
```

```
BAN config>
```

#### 5.2.2.5 BAN-PORT <port number> INVERSED

Allows the device to behave as an FEP (see note). This operating mode only works with a port defined as **NO TERMINATED**. This mode must only be used in special situations. In cases where this behavior is needed, instead of using this command, it's better to configure the bridge normally without BAN and apply a MAC filter in the Frame Relay port.

*Syntax:*

```
BAN config>ban-port <port number> inversed
```

*Example:*

```
BAN config>ban-port 2 inversed
BAN config>
```

**Note**

You should not use a router to replace an FEP. In cases where this is necessary, only use it to connect a few units.

#### 5.2.2.6 BAN-PORT <port number> NO INVERSED

Allows the device to behave as an access device (see note). This is the default behavior.

*Syntax:*

```
BAN config>ban-port <port number> no inversed
```

*Example:*

```
BAN config>ban-port 2 no inversed
BAN config>
```

**Note**

You should not use a router to replace an FEP. In cases where this is necessary, only use it to connect a few units.

#### 5.2.2.7 NO BAN-PORT <port number>

Suppresses or eliminates a BAN port. You need to specify the port number assigned in the bridge as a parameter.

*Syntax:*

```
BAN config>no ban-port <port number>
```

*Example:*

```
BAN config>no ban-port 2
BAN config>
```

### 5.2.3 LIST

Displays information on the current BAN configuration or helps check 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>
```

### 5.2.4 EXIT

Exits the configuration module and returns to the DLSw config> or ASRT config> prompt.

*Syntax:*

```
BAN config>exit
```

*Example:*

```
BAN config>exit
DLSw config>
```

# Chapter 6 Boundary Access Node Monitoring

## 6.1 BAN Monitoring

To access the monitoring environment, enter PROCESS 3 (or P 3). This takes you to the + prompt:

*Example:*

```
*PROCESS 3
+
```

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
Boundary Access Node Console
BAN+
```

## 6.2 Monitoring Commands

Monitoring commands are entered at the BAN+ prompt.

| Command | Function |
|---|---|
| *? (HELP)* | Lists all monitoring commands or associated parameters. |
| *LIST* | Displays the current BAN configuration and tells you if the port has initialized properly or not. |
| *EXIT* | Exits the BAN configuration process and returns to the DLSw+ or ASRT+ prompt. |

### 6.2.1 ?(HELP)

Lists the commands available at the current prompt level. You can also enter ? after a specific command name to list its options.

*Syntax:*

```
BAN+?
  list    List BAN ports
  exit
```

### 6.2.2 LIST

Displays information on the current BAN configuration or helps check if the DLCI is functioning properly. When the BAN monitoring module is active, the LIST command provides general information on BAN monitoring. This command also details if all BAN ports have 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+
```

### 6.2.3 EXIT

Exits the monitoring module and returns to the DLSw+ or ASRT+ prompt.

*Syntax:*

```
BAN+exit
```

*Example:*

```
BAN+exit
DLSw+
```