

# Configuring DLSw+

---

This chapter describes how to configure DLSw+, our implementation of the data-link switching (DLSw) standard for Systems Network Architecture (SNA) devices. For a complete description of the commands in this chapter, refer to the “DLSw+ Configuration Commands” chapter of the *Router Products Command Reference* publication.

## Cisco’s Implementation of DLSw: DLSw+

DLSw+ is our implementation of DLSw, an SNA-over-IP routing standard that helps to integrate SNA and local-area network (LAN) internetworks by encapsulating nonroutable SNA and NetBIOS protocols within routable IP protocols. It is a means of transporting SNA and NetBIOS traffic over an Internet Protocol (IP) network. DLSw is an alternative to source-route bridging (SRB) and addresses the following limitations of SRB:

- SRB hop-count limits (SRB limit is 7)
- Broadcast traffic (from SRB explorer frames or NetBIOS name queries)
- Unnecessary traffic (acknowledgments)
- Data link control timeouts
- Lack of flow control and prioritization

Because these limitations occur when SRB is extended across a wide-area network (WAN), DLSw is typically used to transport SNA and NetBIOS across a WAN.

## DLSw Standard

The DLSw standard, documented in RFC 1795, defines the switch-to-switch protocol used between DLSw routers and defines a mechanism to terminate data link control connections locally and multiplex the traffic from the data link control connections onto a Transmission Control Protocol (TCP) connection. The standard always calls for the transport protocol to be TCP and always requires that data link control connections be locally terminated (the equivalent of our local acknowledgment option). The standard also requires that the SRB route information field (RIF) be terminated at the DLSw router. The standard describes a means for prioritization and flow control and defines error recovery procedures that assure data link control connections are appropriately disabled if any part of their associated circuits breaks.

The DLSw standard does not specify when to establish TCP connections. The capabilities exchange allows compliance to the standard but at different levels of support. The standard does not specify how to cache learned information about MAC addresses, RIFs, or NetBIOS names. It also does not describe how to keep track of both capable or preferred DLSw partners for either backup or

load-balancing purposes. It does not provide the specifics of media conversion, but leaves the details up to the implementation. It does not define how to map switch congestion to data link control flow control. Finally, the management information base (MIB) is documented under a separate RFC.

### DLSw+ Features and Enhancements

DLSw+ includes the following features:

- Full compliance with the DLSw standard RFC 1795.
- A choice of transport options, including TCP, Fast-Sequenced Transport (FST), and direct encapsulation in High-Level Data Link Control (HDLC) or Frame Relay
- Media conversion between local or remote LANs and Synchronous Data Link Control (SDLC) or Ethernet
- Conversion between LAN/SDLC and Qualified Logical Link Control (QLLC) for PU 2.0 and PU 2.1 devices.
- Scalability enhancements through peer groups
- Scalability enhancements through explorer firewalls and location learning
- Configuration reduction through on-demand peers

DLSw+ includes enhancements in the following areas:

- Modes of operation—The ability to determine the capabilities of the participating router and to operate according to those capabilities
- Scalability—The ability to construct IBM internetworks in a way that reduces the amount of broadcast traffic and therefore enhances their scalability
- Performance—The ability to offer higher-performance transport options when the line speeds and traffic conditions do not require local acknowledgment
- Availability—The ability to rapidly recover from failures by caching multiple peers that can be used to reach a given destination

### Modes of Operation

DLSw+ operates in three modes:

- Backward compatibility mode—remote source-route bridging (RSRB) can be used in parallel with DLSw+ to communicate with older releases of Cisco Internetwork Operating System (Cisco IOS) running RSRB and SDLC-to-LLC2 conversion (SDLLC).
- Standards compliance mode—DLSw+ can automatically detect (through the DLSw+ capabilities exchange) that the participating router is manufactured by another vendor. DLSw+ then operates in DLSw standard mode.
- Enhanced mode—DLSw+ can automatically detect that the participating router is another DLSw+ router. DLSw+ then operates in enhanced mode, providing the additional features of DLSw+ to the SNA and NetBIOS end systems.

---

**Note** DLSw+ does not interoperate with pre-standard implementations such as RFC 1434.

---

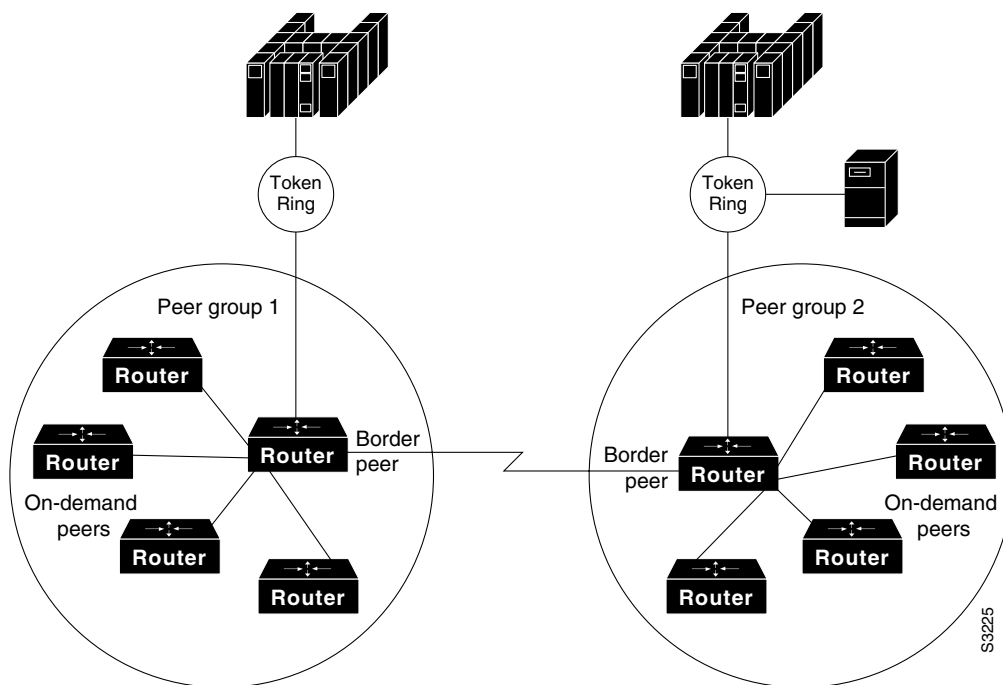
Some enhanced DLSw+ features are also available when a Cisco router is operating in standards compliance mode with another vendor's router. In particular, enhancements that are locally controlled options on a router can be accessed even though the remote router does not have DLSw+. These include location learning (the ability to determine if a destination is on a local LAN before sending "canureach" frames across a WAN), explorer firewalls, and media conversion.

## Improved Scalability

One significant factor that limits the size of Token Ring internetworks is the amount of explorer traffic that traverses the WAN. DLSw+ includes the following features to reduce the number of explorers:

- **Peer groups**—The large Token Ring internetworks that Cisco has helped to build over the last several years have all followed a similar structure. That structure is a hierarchical grouping of routers based upon the usual flow of broadcasts through the network. A cluster of routers in a region or a division of a company are combined into a peer group.
- **Border peers**—Within a peer group, one or more routers are designated as border peers. When a DLSw+ router receives a test frame or NetBIOS name query, it sends a single explorer frame to its border peer. The border peer takes complete responsibility for forwarding the explorer on behalf of the peer group member. This arrangement eliminates duplicate explorers on the access links and minimizes the processing required in access routers.
- **On-demand peers**—On-demand peers greatly reduce the number of peers that must be configured. As Figure 26-1 shows, you can use on-demand peers to establish an end-to-end circuit even though the DLSw+ routers servicing the end systems have no specific configuration information about the peers. This configuration permits casual, any-to-any connection without the burden of configuring the connection in advance. It also allows any-to-any routing in large internetworks where persistent TCP connections would not otherwise be possible.
- **Explorer firewalls**—An explorer firewall permits only a single explorer for a particular destination MAC address to be sent across the WAN. While an explorer is outstanding and awaiting a response from the destination, subsequent explorers for that MAC address are merely stored. Once the explorer response is received at the originating DLSw+, all explorers receive an immediate local response. This eliminates the start-of-day explorer storm that many networks experience.

Figure 26-1 Scalability with DLSw+



## Performance

The transport connection between DLSw+ routers can vary according to the needs of the network and is not necessarily tied to TCP/IP as the DLSw standard is. We support three different transport protocols between DLSw+ routers:

- TCP/IP for transport of SNA and NetBIOS traffic across WANs where bandwidth is limited and termination of data link control sessions is required. This transport option is required when DLSw+ is operating in DLSw+ standards compliance mode.
- FST/IP for transport across WANs with an arbitrary topology with sufficient bandwidth to accommodate SNA and NetBIOS.
- Direct encapsulation for transport across a point-to-point connection where the benefits of an arbitrary topology are not important.

## Enhanced Availability

DLSw+ offers enhanced availability by maintaining a peer table of multiple paths to a given MAC address or NetBIOS name (where a path is either a remote peer or a local port). Each of our routers maintains a preferred path and one or more capable paths to each destination. The preferred peer is either the peer that responds first to an explorer frame or the peer with the least cost. The preferred port is always the port over which the first positive response to an explorer was received. If the preferred peer to a given destination is unavailable, the next available capable peer is promoted to the new preferred peer. No additional broadcasts are required, and recovery through an alternate peer is immediate.

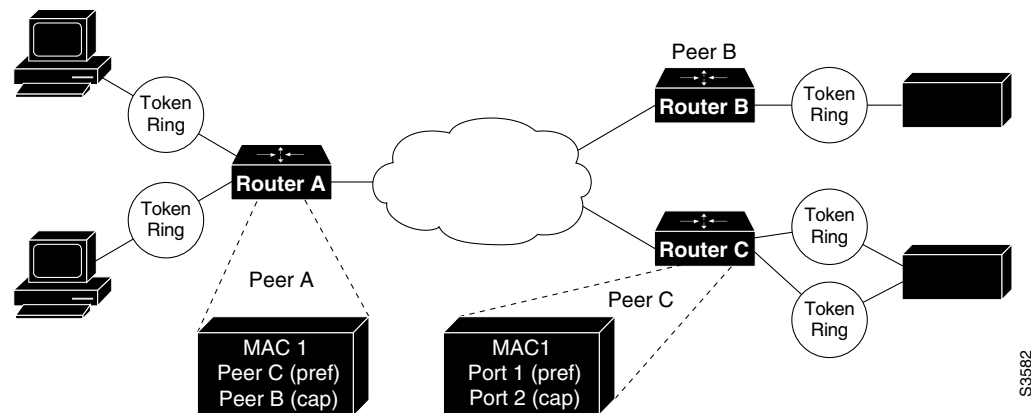
Maintaining multiple paths per destination is especially attractive in SNA networks. A common technique used in the hierarchical SNA environment is assigning the same MAC address to different Token Ring interface couplers (TICs) on the IBM front-end processors (FEPs). DLSw+ ensures that duplicate TIC addresses are found, and if multiple DLSw+ peers can be used to reach the FEPs, they are all cached.

The way that multiple capable peers are handled with DLSw+ can be biased to meet either of the following network needs:

- **Fault tolerance**—To rapidly reconnect if a data-link connection is lost. Whenever a new circuit is established between a pair of end systems and the end-to-end path for the circuit is already known (that is, it is cached), the originating DLSw+ router sends a circuit-establishment message directly to the preferred partner. If the preferred partner is no longer available, a circuit-establishment message is sent to the next capable router in the cache. Maintaining multiple cache entries facilitates a timely reconnection after session outages.
- **Load balancing**—To distribute the network traffic over multiple DLSw+ peers in the network. The routers can be configured to perform load balancing, in which case circuits are established in round-robin fashion using the list of capable routers. When used for load balancing, this technique improves overall SNA performance.

Figure 26-2 shows a peer table of preferred (Pref) and capable (Cap) routes.

**Figure 26-2 Enhanced Availability and Performance**



## DLSw+ Configuration Task List

DLSw+ supports media conversion between local or remote LANs and SDLC or Ethernet. For clarity, the configuration task list below describes configuration in a Token Ring environment. The only differences for SDLC and Ethernet are the specific commands needed to configure those media, plus a media-specific command to associate the interface with DLSw+.

To configure DLSw+, perform tasks in the following sections:

- Define a Source-Bridge Ring Group for DLSw+
- Define a DLSw+ Local Peer for the Router
- Define a DLSw+ Ring List or Port List
- Define a DLSw+ Bridge Group List

- Define DLSw+ Remote Peers
- Enable DLSw+ Over Frame Relay
- Configure Peer-on-Demand Defaults
- Configure Static Resources Exchanged in Capabilities Exchange
- Configure Static Paths
- Configure Duplicate Path Handling
- Enable DLSw+ on the Appropriate Token Ring Interface
- Enable DLSw+ on the Appropriate Ethernet Interface
- Enable DLSw+ on the Appropriate SDLC Interface
- Enable DLSw+ Over QLLC
- Tune the DLSw+ Configuration
- Monitor and Maintain the DLSw+ Network

See the end of this chapter for “DLSw+ Configuration Examples.” Media-specific configuration examples for Ethernet and SDLC are also provided. For details of SDLC commands in the sample SDLC configuration, refer to the “LLC2 and SDLC Commands” chapter of the *Router Products Command Reference* publication.

## Define a Source-Bridge Ring Group for DLSw+

The source-bridge ring can be shared between DLSw+ and SRB/RSRB. In DLSw+, the source-bridge ring group specifies the virtual ring that will appear to be the last ring in the RIF. Because RIFs are terminated at the router, there is no correlation between the ring-group number specified in DLSw+ peers. They can be the same for management simplicity, but they do not have to be. To define a source-bridge ring group for DLSw+, perform the following task in global configuration mode:

Task	Command
Define a ring group.	<b>source-bridge ring-group</b> <i>ring-group</i> <sup>1</sup>

1. This command is documented in the “Source-Route Bridging Commands” chapter of the *Router Products Command Reference* publication.

Refer to “DLSw+ Using TCP Encapsulation and LLC2 Local Acknowledgment—Basic Configuration Example” for a sample configuration file.

## Define a DLSw+ Local Peer for the Router

Defining a DLSw+ local peer for a router enables DLSw+. You specify all local DLSw+ parameters as part of the local peer definition. To define a local peer, perform the following task in global configuration mode:

Task	Command
Define the DLSw+ local peer.	<b>dlsw local-peer</b> [ <b>peer-id</b> <i>ip-address</i> ] [ <b>group</b> <i>group</i> ] [ <b>border</b> ] [ <b>cost</b> <i>cost</i> ] [ <b>if</b> <i>size</i> ] [ <b>keepalive</b> <i>seconds</i> ] [ <b>passive</b> ] [ <b>promiscuous</b> ]

Refer to “DLSw+ Using TCP Encapsulation and LLC2 Local Acknowledgment—Basic Configuration Example” for a sample configuration.

## Define a DLSw+ Ring List or Port List

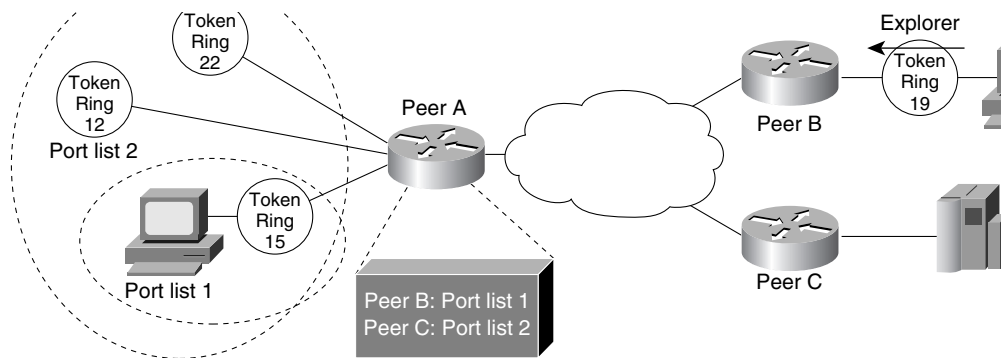
DLSw+ ring lists are used to map traffic on a local interface to remote peers. You can create a ring list of local ring numbers and apply the list to remote peer definitions. Traffic received from a remote peer is only forwarded to the rings specified in the ring list. Traffic received from a local interface is only forwarded to peers if the input ring number appears in the ring list applied to the remote peer definition. The definition of a ring list is optional. If you want all peers and all rings to receive all traffic, you do not have to define a ring list. Simply specify 0 for the list number in the remote peer statement.

To define a ring list, perform the following task in global configuration mode:

Task	Command
Define a ring list.	<b>dlsw ring-list</b> <i>list-number</i> <b>rings</b> <i>ring-number</i>

DLSw+ port lists are used to map traffic on a local interface (either Token Ring or serial) to remote peers. You can create a port list of local ports and apply the list to remote peer definitions. Traffic received from a remote peer is only forwarded to peers if the input port number appears in the port list applied to the remote peer definition. The port list command provides a single command to specify both serial and Token Ring interfaces. Figure 26-3 shows how port lists are used to map traffic.

Figure 26-3 Mapping Traffic Using Port Lists



The definition of a port list is optional. If you want all peers and all interfaces to receive all traffic, you do not have to define a port list. Simply specify 0 for the list number in the remote peer statement.

To define a port list, perform the following task in global configuration mode:

Task	Command
Define a port list.	<b>dlsw port-list</b> <i>list-number</i> [ <b>serial</b>   <b>tokenring</b> ] <i>number</i> [ <b>serial</b>   <b>tokenring</b> ] <i>number</i> ...

**Note** Either the ring list or the port list command can be used to associate rings with a given ring-list. The ring list command is easier to type in if you have a large number of rings to define.

---

## Define a DLSw+ Bridge Group List

DLSw+ bridge group lists are used to map traffic on the local Ethernet bridge group interface to remote peers. You can create a bridge group list and apply the list to remote peer definitions. Traffic received from a remote peer is only forwarded to the bridge group specified in the bridge group list. Traffic received from a local interface is only forwarded to peers if the input bridge group number appears in the bridge group list applied to the remote peer definition. The definition of a bridge group list is optional. Because each remote peer has a single list number associated with it, if you want traffic to go to a bridge group and to either a ring list or port list, you should specify the same list number in each definition.

Task	Command
Define a ring list.	<b>dlsw bgroup-list</b> <i>list-number</i> <b>bgroups</b> <i>number</i>

## Define DLSw+ Remote Peers

You can define direct, FST, or TCP encapsulation remote peers by performing one of the following tasks in global configuration mode:

Task	Command
Define a direct encapsulation in HDLC for remote peer.	<b>dlsw remote-peer</b> <i>list-number</i> <b>interface</b> <i>interface-name</i> [ <i>mac-address</i> ] [ <b>cost</b> <i>cost</i> ] [ <b>lf</b> <i>size</i> ] [ <b>keepalive</b> <i>seconds</i> ] [ <b>lsap-output-list</b> <i>list</i> ] [ <b>host-netbios-out</b> <i>host-list-name</i> ] [ <b>bytes-netbios-out</b> <i>bytes-list-name</i> ]
Define a direct encapsulation in Frame Relay for the remote peer.	<b>dlsw remote-peer</b> <i>list-number</i> <b>frame-relay interface serial</b> <i>number</i> <i>dcci-number</i> [ <b>pass-thru</b> ] [ <b>cost</b> <i>cost</i> ] [ <b>lf</b> <i>size</i> ] [ <b>keepalive</b> <i>seconds</i> ] [ <b>lsap-output-list</b> <i>list</i> ] [ <b>host-netbios-out</b> <i>host-list-name</i> ] [ <b>bytes-netbios-out</b> <i>bytes-list-name</i> ]
Define an FST encapsulation remote peer.	<b>dlsw remote-peer</b> <i>list-number</i> <b>fst</b> <i>ip-address</i> [ <b>cost</b> <i>cost</i> ] [ <b>lf</b> <i>size</i> ] [ <b>keepalive</b> <i>seconds</i> ] [ <b>lsap-output-list</b> <i>list</i> ] [ <b>host-netbios-out</b> <i>host-list-name</i> ] [ <b>bytes-netbios-out</b> <i>bytes-list-name</i> ] [ <b>backup-peer</b> <i>ip-address</i> ]
Define a TCP encapsulation remote peer.	<b>dlsw remote-peer</b> <i>list-number</i> <b>tcp</b> <i>ip-address</i> [ <b>priority</b> ] [ <b>cost</b> <i>cost</i> ] [ <b>lf</b> <i>size</i> ] [ <b>keepalive</b> <i>seconds</i> ] [ <b>tcp-queue-max</b> <i>size</i> ] [ <b>lsap-output-list</b> <i>list</i> ] [ <b>host-netbios-out</b> <i>host-list-name</i> ] [ <b>bytes-netbios-out</b> <i>bytes-list-name</i> ] [ <b>backup-peer</b> <i>ip-address</i> ]

The following is a list of valid port numbers used for TCP connections when the **priority** keyword is used with the **dlsw remote-peer** command:

high	2065
medium	1981
normal	1982
low	1983

Refer to “DLSw+ Using TCP Encapsulation and LLC2 Local Acknowledgment—Basic Configuration Example” for an example DLSw+ configuration for TCP encapsulation.

## Enable DLSw+ Over Frame Relay

You can configure the router for direct encapsulation of DLSw+ in Frame Relay according to RFC 1490. DLSw+ Direct over RFC 1490 supports either passthrough or local acknowledgment (DLC termination). DLSw+ supports transport for both SNA and NetBIOS data. SNA PU 2.0 and PU 2.1 are supported.

The media on either end must be Token Ring.

The solution requires a minimum number of PVCs (since multiple protocols can share a single PVC). This simplifies configuration because multiple PUs can share a PVC without requiring configuration of multiple SAPs.

The passthrough option adds the smallest amount of link overhead and requires minimal processing cycles in the attaching routers when compared to TCP/IP encapsulation.

The local acknowledgment option prevents DLC timeouts during periods of WAN congestion. It also minimizes WAN traffic by keeping data link control (DLC) acknowledgments and keepalives off the WAN.

No controller or FEP upgrades are required to take advantage of this feature (if already Token Ring attached), reducing costs and simplifying migration to Frame Relay.

To enable DLSw+ over Frame Relay with passthrough, perform the following tasks, beginning in global configuration mode:

Task	Command
Specify the serial port.	<b>interface serial</b> <i>number</i> <sup>1</sup>
Enable Frame Relay encapsulation.	<b>encapsulation frame-relay</b> <sup>2</sup>
Define the mapping between DLSw+ and the DLCI.	<b>frame-relay map dlsw</b> <i>dlsi-number</i> <sup>2</sup>

1. This command is documented in the “Interface Commands” chapter of the *Router Products Command Reference* Publication.

2. This command is documented in the “Frame Relay Commands” chapter of the *Router Products Command Reference* publication.

**Note** The DLSw+ remote peer statement should also specify passthrough.

To enable DLSw+ over Frame Relay with local acknowledgment, perform the following tasks, beginning in global configuration mode:

Task	Command
Specify the serial port.	<b>interface serial</b> <i>number</i> <sup>1</sup>
Enable Frame Relay encapsulation.	<b>encapsulation frame-relay</b> <sup>2</sup>
Define the mapping between DLSw+ and the DLCI.	<b>frame-relay map llc2</b> <i>dlsi-number</i> <sup>2</sup>

1. This command is documented in the “Interface Commands” chapter of the *Router Products Command Reference* Publication.
2. This command is documented in the “Frame Relay Commands” chapter of the *Router Products Command Reference* publication.

## Configure Peer-on-Demand Defaults

To configure peer-on-demand defaults, perform one of the following task in global configuration mode:

Task	Command
Configure FST peer-on-demand defaults.	<b>dlsw peer-on-demand-defaults fst</b> [ <b>bytes-netbios-out</b> <i>bytes-list-name</i> ] [ <b>cost</b> <i>cost</i> ] [ <b>host-netbios-out</b> <i>host-list-name</i> ] [ <b>inactivity</b> <i>minutes</i> ] [ <b>keepalive</b> <i>seconds</i> ] [ <b>lf</b> <i>size</i> ] [ <b>lsap-output-list</b> <i>list</i> ] [ <b>port-list</b> <i>port-list-number</i> ]
Configure TCP peer-on-demand defaults.	<b>dlsw peer-on-demand-defaults tcp</b> [ <b>bytes-netbios-out</b> <i>bytes-list-name</i> ] [ <b>cost</b> <i>cost</i> ] [ <b>host-netbios-out</b> <i>host-list-name</i> ] [ <b>inactivity</b> <i>minutes</i> ] [ <b>keepalive</b> <i>seconds</i> ] [ <b>lf</b> <i>size</i> ] [ <b>local-ack</b> ] [ <b>lsap-output-list</b> <i>list</i> ] [ <b>priority</b> ]

## Configure Static Resources Exchanged in Capabilities Exchange

To reduce explorer traffic destined for this peer, the peer can send other peers a list of resources for which it has information (icanreach) or does not have information (icannotreach). This information is exchanged as part of a capabilities exchange. To configure static resources that will be exchanged as part of a capabilities exchange, perform one of the following tasks in global configuration mode:

Task	Command
Configure a resource not locally reachable by the router.	<b>dlsw icannotreach saps</b> <i>sap</i> [ <i>sap...</i> ]
Configure a resource locally reachable by the router.	<b>dlsw icanreach</b> { <b>mac-exclusive</b>   <b>netbios-exclusive</b>   <b>mac-address</b> <i>mac-addr</i> [ <b>mask</b> <i>mask</i> ]   <b>netbios-name</b> <i>name</i> }

## Configure Static Paths

To configure static paths to minimize explorer traffic originating in this peer, perform one of the following tasks in global configuration mode:

Task	Command
Configure the location or path of a static MAC address.	<b>dlsw mac-addr</b> <i>mac-addr</i> { <b>ring-group</b> <i>ring</i>   <b>remote-peer</b> { <b>interface</b> <i>serial number</i>   <b>ip-address</b> <i>ip-address</i> }   <b>group</b> <i>group</i> }
Configure a static NetBIOS name.	<b>dlsw netbios-name</b> <i>netbios-name</i> { <b>ring-group</b> <i>ring</i>   <b>remote-peer</b> { <b>interface</b> <i>serial number</i>   <b>ip-address</b> <i>ip-address</i> }   <b>group</b> <i>group</i> }

## Configure Duplicate Path Handling

To configure duplicate path handling, perform the following task in global configuration mode:

Task	Command
Configure duplicate path handling.	<b>dlsw duplicate-path-bias</b> [load-balance]

## Enable DLSw+ on the Appropriate Token Ring Interface

To enable DLSw+ on a Token Ring interface, perform the following task in interface configuration mode:

Task	Command
Enable DLSw+ on a Token Ring interface.	<b>source-bridge</b> <i>local-ring bridge-number ring-group</i> <sup>1</sup>

1. This command is documented in the “Source-Route Bridging Commands” chapter of the *Router Products Command Reference*.

## Enable DLSw+ on the Appropriate Ethernet Interface

To enable DLSw+ on certain Ethernet interfaces, perform the following task in global configuration mode:

Task	Command
Enable DLSw+ on an Ethernet interface.	<b>dlsw bridge-group</b> <i>group-number</i>

## Enable DLSw+ on the Appropriate SDLC Interface

To enable DLSw+ on an SDLC interface, perform the following task in interface configuration mode:

Task	Command
Enable DLSw+ on an SDLC interface.	<b>sdlc dlsw</b> <i>sdlc-address</i>

## Enable DLSw+ Over QLLC

You can configure DLSw+ for QLLC connectivity, which enables both of the following two scenarios:

- Remote LAN-attached devices (physical units) or SDLC-attached devices can access a front-end processor (FEP) or an AS/400 over an X.25 network.

Our QLLC support allows remote X.25-attached SNA devices to access a FEP without requiring NPSI in the FEP. This may eliminate the requirement for NPSI (if GATE and DATE are not required), thereby eliminating the recurring license cost. In addition, because the QLLC attached devices appear to be Token Ring-attached to the NCP, they require no preconfiguration in the FEP. Remote X.25-attached SNA devices can also connect to an AS/400 over Token Ring using this support.

- Remote X.25-attached SNA devices can access a FEP or an AS/400 over a Token Ring or over SDLC.

For environments just beginning to migrate to LANs, our QLLC support allows deployment of LANs in remote sites while maintaining access to the FEP over existing NPSI links. Remote LAN-attached devices (physical units) or SDLC- attached devices can access a FEP over an X.25 network without requiring X.25 hardware or software in the LAN-attached devices. The Cisco IOS supports direct attachment to the FEP over X.25 without the need for routers at the data center for SNA traffic.

To enable QLLC connectivity for DLSw+, perform the following tasks in interface configuration mode:

Task	Command
Specify an interface as an X.25 device.	<b>encapsulation x.25</b> <sup>1</sup>
Activate X.25 subaddresses.	<b>x25 address subaddress</b> <sup>1</sup>
Associate a virtual MAC address with the X.121 address of the remote X.25 device.	<b>x25 map qllc x121-addr [x25-map-options]</b> <sup>2</sup>
Enable DLSw+ over QLLC.	<b>qllc dslw {subaddress subaddress}   {pvc pvc-low [pvc-high]} [vmac vmacaddr [poolsize]] [partner partner macaddr] [sap ssap dsap] [xid xidstring] [npsi-poll]</b> <sup>3</sup>

1. This command is documented in the “X.25 and LAPB Commands” chapter of the *Router Products Command Reference* publication.
2. This command is documented in the “IBM Network Media Translation Commands” chapter of the *Router Products Command Reference* publication.
3. This command is documented in the “DLSw+ Configuration Commands” chapter of the *Router Products Command Reference* publication.

## Tune the DLSw+ Configuration

To modify an existing configuration parameter, perform one or more of the following tasks in global configuration mode:

Task	Command
Disable and re-enable DLSw+ without altering the configuration.	<b>dslw disable</b>
Configure the depth of DLSw+ explorer queue router.	<b>dslw explorerq-depth queue-max</b>
Configure DLSw+ timers.	<b>dslw timer {icannotreach-block-time   netbios-cache-timeout   netbios-explorer-timeout   netbios-retry-interval   netbios-verify-interval   sna-cache-timeout   sna-explorer-timeout   sna-retry-interval   sna-verify-interval} time</b>

## Monitor and Maintain the DLSw+ Network

To monitor and maintain activity on the DLSw+ network, perform one or more of the following tasks in privileged EXEC mode:

Task	Command
Display capabilities of a direct-encapsulated remote peer.	<b>show dslw capabilities interface type   number</b>
Display capabilities of a TCP/FST remote peer.	<b>show dslw capabilities ip-address ip-address</b>
Display capabilities of the local peer.	<b>show dslw capabilities local</b>
Display DLSw+ circuit information.	<b>show dslw circuits</b>
Display DLSw+ peer information.	<b>show dslw peers</b>
Display DLSw+ reachability information.	<b>show dslw reachability</b>

## DLSw+ Configuration Examples

The following sections provide DLSw+ configuration examples:

- DLSw+ Using TCP Encapsulation and LLC2 Local Acknowledgment—Basic Configuration Example
- DLSw+ Using TCP Encapsulation with Local Acknowledgment—Peer Group Configuration Example 1
- DLSw+ Using TCP Encapsulation with Local Acknowledgment—Peer Group Configuration Example 2
- DLSw+ Translation between Ethernet and Token Ring Configuration Example
- DLSw+ Translation between SDLC and Token Ring Media Example
- DLSw+ over Frame Relay Configuration Example
- DLSw+ over QLLC Configuration Examples

### DLSw+ Using TCP Encapsulation and LLC2 Local Acknowledgment—Basic Configuration Example

This sample configuration requires the following tasks, which are described in earlier sections of this document:

- Define a Source-Bridge Ring Group for DLSw+
- Define a DLSw+ Local Peer for the Router
- Define DLSw+ Remote Peers
- Enable DLSw+ on the Appropriate LAN Interface

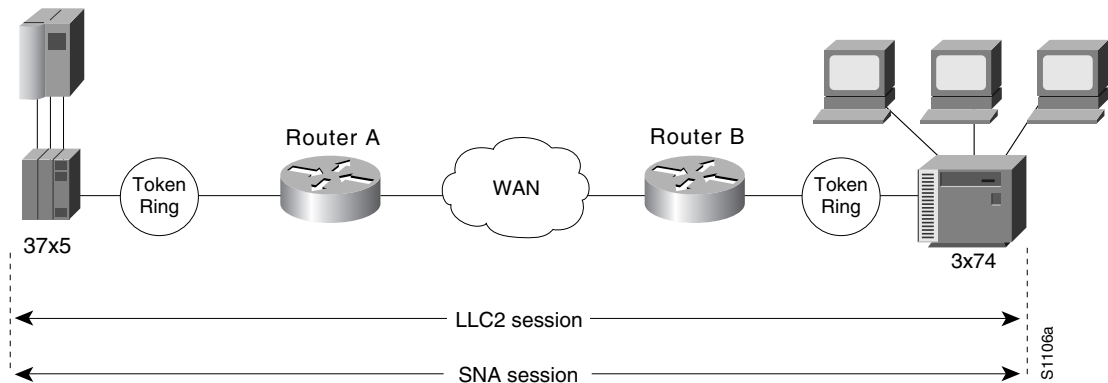
Encapsulate the source-route bridged traffic inside IP datagrams passed over a TCP connection between two routers/bridges with local acknowledgment enabled when you have LANs separated by wide geographic distances, and you want to avoid multiple retransmissions or loss of user sessions that can occur with time delays.

Logical Link Control–Type 2 (LLC2) is an ISO standard data link level protocol used in Token Ring networks. LLC2 was designed to ensure reliable transmission of data across LAN media with minimal or predictable time delays. With the advent of DLSw+ and WAN backbones, LANs are now separated by wide, geographic distances spanning countries and continents. As a result, these LANs have time delays that are longer than LLC2 allows for bidirectional communication between hosts. The local acknowledgment capability in routers and bridges supporting remote source-route bridging addresses the problem of unpredictable time delays, multiple retransmissions, and loss of user sessions.

In a typical LLC2 session, when one host sends a frame to another host, the sending host expects the receiving host to respond positively or negatively in a predefined period of time commonly called the *T1 time*. If the sending host does not receive an acknowledgment of the frame it sent within the T1 time, it retries a few times (normally 8 to 10). If there is still no response, the sending host drops the session.

Figure 26-4 illustrates an LLC2 session. A 37x5 on a LAN segment can communicate with a 3x74 on a different LAN segment separated via a wide-area backbone network. Frames are transported between Router A and Router B by means of DLSw+. However, the LLC2 session between the 37x5 and the 3x74 is still end-to-end; that is, every frame generated by the 37x5 traverses the backbone network to the 3x74, and the 3x74, on receipt of the frame, acknowledges it.

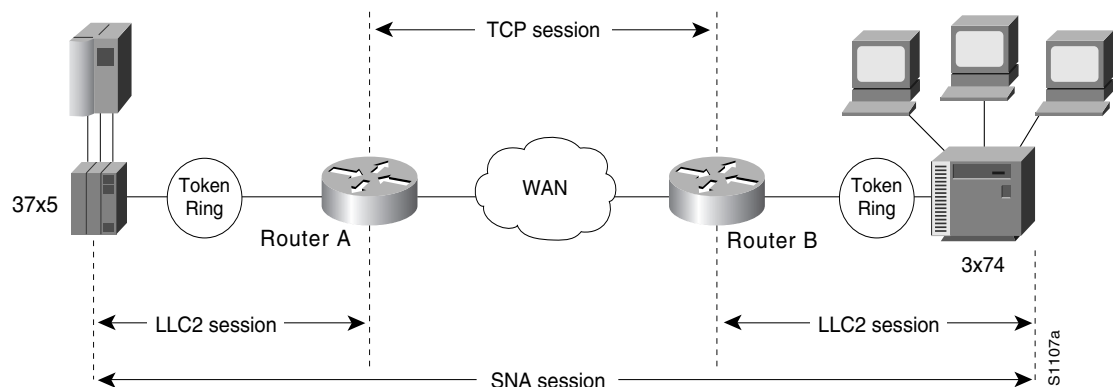
**Figure 26-4 LLC2 Session without Local Acknowledgment**



On backbone networks consisting of slow serial links, the T1 timer on end hosts could expire before the frames have a chance to reach the remote hosts, causing the end host to retransmit. This results in duplicate frames reaching the remote host at the same time as the first frame also reached the remote host, albeit slowly. These frame duplications break the LLC2 protocol, resulting in the loss of sessions between the two IBM machines.

One way to solve this time delay problem is to increase the timeout value on the end nodes to account for the maximum transit time between the two end machines. However, in networks consisting of hundreds or even thousands of nodes, every machine would need to be reconfigured with new values. With local acknowledgment for LLC2 turned on, the LLC2 session between the two end nodes would not be end-to-end, but instead, terminate at two local routers. Figure 26-5 shows the LLC2 session with the 37x5 ending at Router A and the LLC2 session with the 3x74 ending at Router B. Both Router A and Router B execute the full LLC2 protocol as part of local acknowledgment for LLC2.

**Figure 26-5 LLC2 Session with Local Acknowledgment**



With local acknowledgment for LLC2 enabled in both routers, Router A acknowledges frames received from the 37x5. The 37x5 still recognizes the acknowledgments it receives as belonging to the 3x74. Router A looks like the 3x74 to the 37x5. Similarly, Router B acknowledges frames received from the 3x74. The 3x74 recognizes the acknowledgments it receives as coming from the 37x5. Router B looks like the 3x74 to 37x5. Because the frames no longer have to travel the WAN backbone networks to be acknowledged, but instead are locally acknowledged by routers, the end machines do not time out, resulting in no loss of sessions.

The advantages of enabling local acknowledgment for LLC2 include the following:

- Local acknowledgment for LLC2 solves the T1 timer problem without having to change any configuration on the end nodes. The end nodes are unaware that the sessions are being locally acknowledged. In networks consisting of hundreds or even thousands of machines, this is a definite advantage. All the frames acknowledged by the router appear to the end hosts to be coming from the remote IBM machine. In fact, by looking at a trace from a protocol analyzer, you cannot determine whether a frame was acknowledged by the local router or by a remote IBM machine. The MAC addresses generated by the routers are identical to those generated by the remote IBM machine.
- All the supervisory (RR, RNR, REJ) frames that are locally acknowledged go no farther than the router. Without local acknowledgment for LLC2, *every* frame traverses the backbone. With local acknowledgment, only data (I-frames) traverses the backbone, resulting in less traffic on the backbone network. For installations in which customers pay for the amount of traffic passing through the backbone, this could be a definite cost-saving measure. A simple protocol exists between the two *peers* to bring up or down a TCP session.

### Notes on Using LLC2 Local Acknowledgment

LLC2 local acknowledgment is enabled only with TCP remote peers (as opposed to LAN or direct serial interface remote peers).

If the LLC2 session between the local host and the router terminates in either router, the other will be informed to terminate its connection to its local host.

If the TCP queue length of the connection between the two routers reaches the highwater mark, the routers sends Receiver-Not-Ready (RNR) messages to the local hosts until the queue limit is reduced to below this limit.

The configuration of the LLC2 parameters for the local Token Ring interfaces can affect overall performance. Refer to the chapter “Configuring LLC2 and SDLC Parameters” in this manual for more details about fine-tuning your network through the LLC2 parameters.

The routers at each end of the LLC2 session execute the full LLC2 protocol, which could result in some overhead. The decision to use local acknowledgment for LLC2 should be based on the speed of the backbone network in relation to the Token Ring speed. For LAN segments separated by slow-speed serial links (for example, 56 kbps), the T1 timer problem could occur more frequently. In such cases, it might be wise to turn on local acknowledgment for LLC2. For LAN segments separated by a T1, backbone delays will be minimal; in such cases, FST or direct should be used. Speed mismatch between the LAN segments and the backbone network is one criterion to help you decide to use local acknowledgment for LLC2.

There are some situations (such as the receiving host failing between the time the sending host sends data and the time the receiving host receives it), in which the sending host would determine, *at the LLC2 layer*, that data was received when it actually was not. This error occurs because the router acknowledges that it received data from the sending host before it determines that the receiving host can actually receive the data. But because both NetBIOS and SNA have error recovery in situations where an end device goes down, these higher-level protocols will resend any missing or lost data. Because these transaction request/confirmation protocols exist above LLC2, they are not affected by tight timers, as is LLC2. They also are transparent to local acknowledgment.

If you are using NetBIOS applications, note that there are two NetBIOS timers—one at the link level and one at the next higher level. Local acknowledgment for LLC2 is designed to solve link timeouts only. If you are experiencing NetBIOS session timeouts, you have two options:

- Experiment with increasing your NetBIOS timers and decreasing your maximum NetBIOS frame size.
- Avoid using NetBIOS applications on slow serial lines.

Figure 26-6 illustrates a DLSw+ configuration with local acknowledgment.

**Figure 26-6 DLSw+ with Local Acknowledgment —Simple Configuration**



#### Configuration for Router A

```
source-bridge ring-group 10
!
dlsw local-peer peer-id 10.2.25.1
dlsw remote-peer 0 tcp 10.2.5.2
int loopback 0
ip address 10.2.25.1 255.255.255.0
.
.
.
interface TokenRing 0
no ip address
ring-speed 16
source-bridge active 25 1 10
```

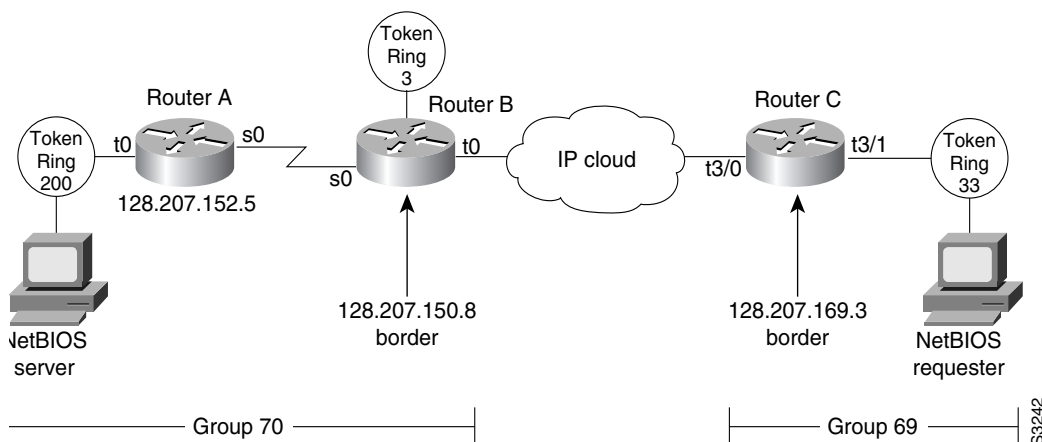
#### Configuration for Router B

```
source-bridge ring-group 12
dlsw local-peer peer-id 10.2.5.2
dlsw remote-peer 0 tcp 10.2.25.1
int loopback 0
ip address 10.2.5.2 255.255.255.0
.
.
.
interface TokenRing 0
no ip address
ring-speed 16
source-bridge active 5 1 12
```

## DLSw+ Using TCP Encapsulation with Local Acknowledgment—Peer Group Configuration Example 1

Figure 26-7 illustrates DLSw+ configured using border peers, showing circuits to each other. Router A is configured to operate in promiscuous mode, and border peers Routers B and C forward broadcasts. This configuration reduces processing requirements in Router A (the access router) and still support any-to-any networks.

**Figure 26-7 DLSw with Peer Groups Specified (Example 1)**



The following are configuration files for the routers in Figure 6.

### Configuration for Router A

```
hostname RouterA
!
source-bridge ring group 31
dlsw local-peer peer-id 128.207.152.5 group 70 promiscuous
dlsw remote peer 0 tcp 128.207.150.8
!
interface Serial0
ip unnumbered TokenRing
clockrate 56000
!
interface TokenRing 0
ip address 128.207.152.5 255.255.255.0
ring-speed 16
source-bridge 200 13 31
source-bridge spanning
!
.
.
.
router igrp 777
network 128.207.0.0
```

### Configuration for Router B

```
hostname RouterB
!
.
.
```

```
.
source-bridge ring-group 31
dlsw local-peer peer-id 128.207.150.8 group 70 border promiscuous
dlsw remote-peer 0 tcp 128.207.169.3
dlsw remote-peer 0 tcp 128.207.152.5
!
.
.
.
interface serial0
ip unnumbered tokenring 0
bandwidth 56
!
.
.
.
interface tokenring 0
ip address 128.207.150.8 255.255.255.0
ring-speed 16
source-bridge 3 14 31
source-bridge spanning
!
router igrp 777
network 128.207.0.0
```

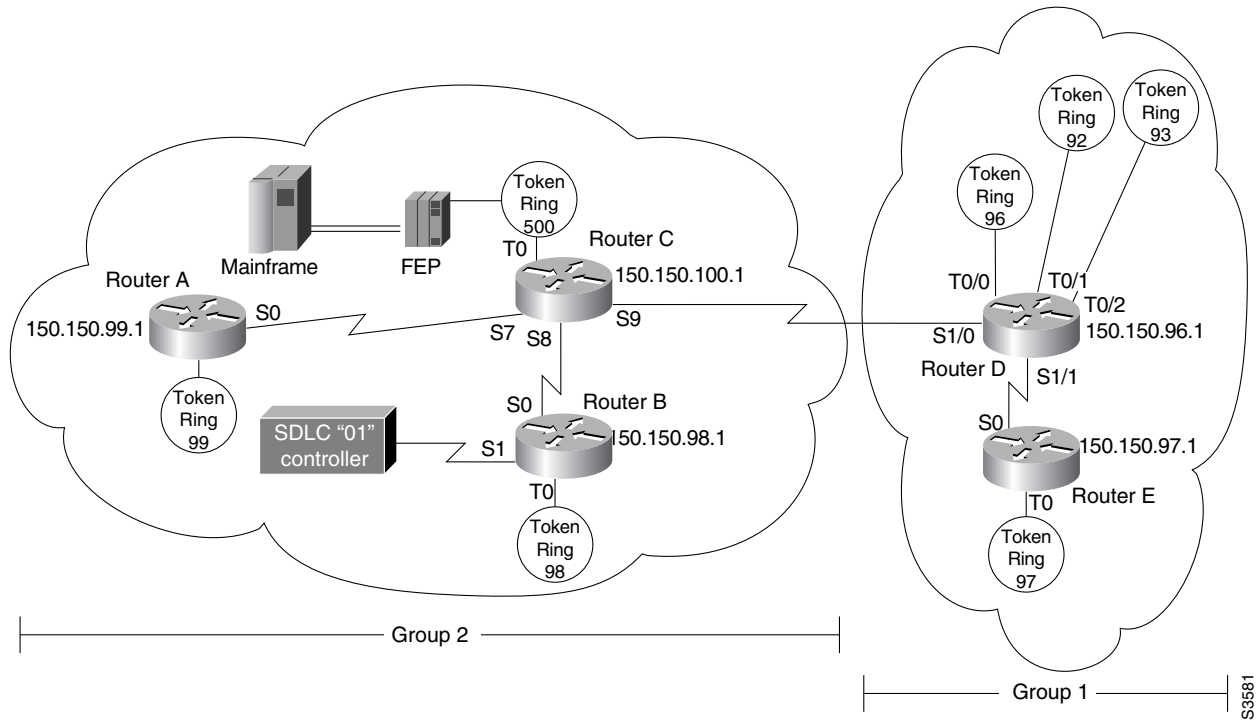
### Configuration for Router C

```
hostname RouterC
!
.
.
.
source-bridge ring-group 69
dlsw local-peer peer-id 128.207.169.3 group 69 border promiscuous
dlsw remote-peer 0 tcp 128.207.150.8
!
.
.
.
interface tokenring 3/0
description fixed to flashnet
ip address 128.207.2.152 255.255.255.0
ring-speed 16
multiring all
!
interface tokenring 3/1
ip address 128.207.169.3 255.255.255.0
ring-speed 16
source-bridge 33 2 69
source-bridge spanning
!
.
.
.
router igrp 777
network 128.207.0.0
```

## DLSw+ Using TCP Encapsulation with Local Acknowledgment—Peer Group Configuration Example 2

Figure 26-8 illustrates a peer group configuration that allows any-to-any connection except for Router B.

**Figure 26-8 DLSw with Peer Groups Specified (Example 2)**



The following are configuration files for the routers in Figure 26-8:

### Configuration for Router A

```
hostname Router A
!
.
.
.
source-bridge ring-group 2000
dlsw local-peer peer-id 150.150.99.1
dlsw remote-peer 0 tcp 150.150.100.1
!
interface loopback 0
 ip address 150.150.99.1 255.255.255.192
!
interface serial 0
 ip address 150.150.9.1 255.255.255.192
!
.
.
.
interface tokenring 0
```

```

no ip address
ring-speed 16
source-bridge 99 1 2000
source-bridge spanning
!
.
.
.
router eigrp 202
network 150.150.0.0

```

### Configuration for Router B

```

hostname RouterB
!
.
.
.
source-bridge ring-group 2000
dlsw local-peer peer-id 150.150.98.1 group 2
dlsw remote-peer 0 tcp 150.150.100.1
!
interface loopback 0
ip address 150.150.98.1 255.255.255.192
!
.
.
.
interface serial 1
no ip address
encapsulation sdhc
no keepalive
priority-group 1
clockrate 9600
sdhc role primary
sdhc vmac 4000.8888.0100
sdhc address 01
sdhc xid 01 05d20006
sdhc partner 4000.1020.1000 01
sdhc dlsw 1
!
interface tokenring 0
no ip address
ring-speed 16
multiring all
source-bridge 98 1 2000
source-bridge spanning
!
.
.
.
router eigrp 202
network 150.150.0.0

```

### Configuration for Router C

```

hostname RouterC
!
.
.
.
source-bridge ring-group 2000
dlsw local-peer peer-id 150.150.100.1 group 2 border promiscuous

```

```
dlsw remote-peer 0 tcp 150.150.96.1
dlsw remote-peer 0 tcp 150.150.98.1
dlsw remote-peer 0 tcp 150.150.99.1
!
interface loopback 0
 ip address 150.150.100.1 255.255.255.192
!
.
.
.
interface serial 7
 ip address 150.150.9.2 255.255.255.192
 clockrate 56000
!
interface serial 8
 ip address 150.150.10.2 255.255.255.192
!
interface serial 9
 ip address 150.150.8.2 255.255.255.192
!
interface tokenring 0
 no ip address
 ring-speed 16
 multiring all
 source-bridge 500 1 2000
!
router eigrp 202
 network 150.150.0.0
```

### Configuration for Router D

```
hostname RouterD
!
.
.
.
.
source-bridge ring-group 2000
dlsw local-peer peer-id 150.150.96.1 group 1 border
dlsw remote-peer 0 tcp 150.150.97.1
dlsw remote-peer 0 tcp 150.150.100.1
!
interface loopback 0
 ip address 150.150.96.1 255.255.255.192
!
.
.
.
interface serial 1/0
 ip address 150.150.8.1 255.255.255.192
 clockrate 56000
!
interface serial 1/1
 ip address 150.150.16.1 255.255.255.192
!
.
.
.
interface tokenring g0/0
 ip address 150.150.2.1 255.255.255.192
 ring-speed 16
 source-bridge 96 1 2000
 source-bridge spanning
!
interface tokenring 0/1
```

```
ip address 150.150.13.1 255.255.255.192
no ip address
ring-speed 16
source-bridge 92 1 2000
source-bridge spanning
!
.
.
.
router eigrp 202
network 150.150.0.0
```

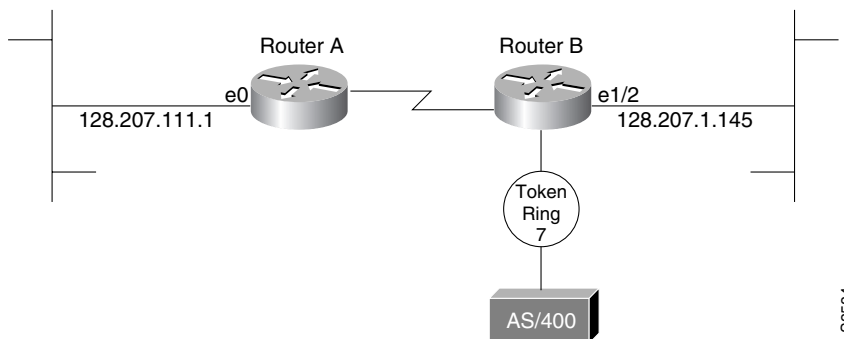
### Configuration for Router E

```
hostname RouterE
!
.
.
.
source-bridge ring-group 2000
dlsw local-peer peer-id 150.150.97.1 group 1 promiscuous
dlsw remote-peer 0 tcp 150.150.96.1
!
interface loopback 0
ip address 150.150.97.1 255.255.255.192
!
interface serial 0
mtu 1400
ip address 150.150.16.2 255.255.255.192
!
.
.
.
interface tokenring 0
no ip address
no ip route-cache
ring-speed 16
source-bridge 97 1 2000
source-bridge spanning
!
.
.
.
router eigrp 202
network 150.150.0.0
```

## DLSw+ Translation between Ethernet and Token Ring Configuration Example

DLSw+ also supports Ethernet media. Except for configuring for a specific media, in this case Ethernet, the configuration is similar to other DLSw+ configuration (see Figure 26-9).

**Figure 26-9 DLSw+ Translation between Ethernet and Token Ring**



The following are the configuration files for the routers in Figure 26-9.

### Configuration for Router A

```
hostname RouterA
!
.
.
.
source-bridge ring-group 31
dlsw local-peer peer-id 128.207.111.1
dlsw remote-peer 0 tcp 128.207.1.145 lf 1500
dlsw bridge-group 5
!
interface Ethernet 0
 ip address 128.207.111.1 255.255.255.0
 bridge-group 5
!
.
.
.
bridge 5 protocol ieee
!
.
.
```

### Configuration for Router B

```
hostname RouterB
!
.
.
.
source-bridge ring-group 500
dlsw local-peer peer-id 128.207.1.145
dlsw remote-peer 0 tcp 128.207.111.1 lf 1500
 dlsw bridge-group 5
.
.
.
```

```

interface ethernet 1/2
 ip address 128.207.1.145 255.255.255.0
 bridge-group 5
.
.
.
interface tokenring 2/0
 no ip address
 ring-speed 16
 multiring all
 source-bridge 7 1 500
 source-bridge spanning
!
.
.
.
router igrp 777
 network 128.207.0.0

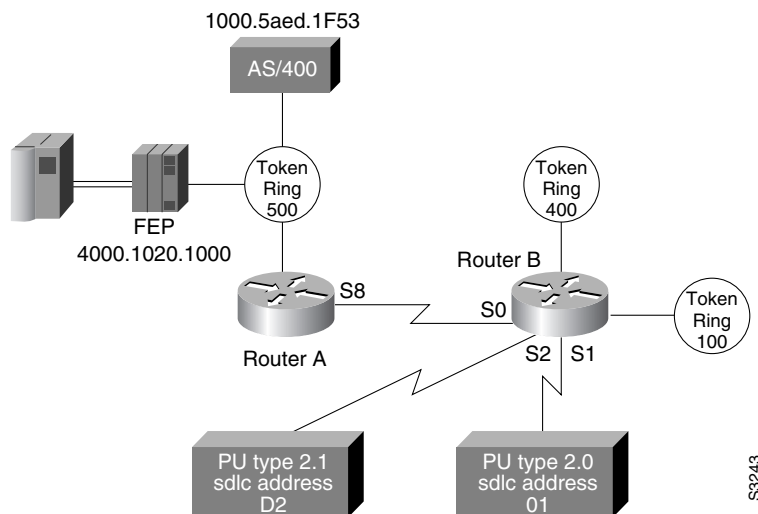
```

## DLSw+ Translation between SDLC and Token Ring Media Example

DLSw+ provides media conversion between local or remote LANs and SDLC. For additional information about configuring SDLC parameters, refer to the chapter “Configuring LLC2 and SDLC Parameters.”

Figure 26-10 illustrates DLSw+ with SDLC encapsulation. For this example, 4000.1020.1000 is the MAC address of the FEP host (PU4). 1000.5aed.1f53 is the MAC address of the AS/400 host, which is defined as Node Type 2.1. Router B serves as the primary station for the remote secondary stations 01. Router B can serve as either primary station or secondary station to remote station D2.

**Figure 26-10 DLSw+ Translation between SDLC and Token Ring Media**



The following is the configuration file for Router A:

### Configuration for Router A

```
hostname RouterA
!
.
.
.
source-bridge ring-group 2000
dlsw local-peer peer-ed 150.150.10.2
dlsw remote-peer 0 tcp 150.150.10.1
!
.
.
.
interface serial 8
 ip address 150.150.10.2 255.255.255.192
 clockrate 56000
!
.
.
.
interface tokenring 0
 no ip address
 ring-speed 16
 source-bridge 500 1 2000
 source-bridge spanning
!
.
.
.
router eigrp 202
 network 150.150.0.0
```

### Configuration for Router B

```
hostname RouterB
!
.
.
.
source-bridge ring-group 2000
dlsw local-peer peer-id 150.150.10.1
dlsw remote-peer 0 tcp 150.150.10.2
!
.
.
.
interface serial 0
 ip address 150.150.10.1 255.255.255.192
!
interface serial 1
 description PU2 with SDLC station role set to secondary
 no ip address
 encapsulation sdlc
 no keepalive
 clockrate 9600
 sdhc role primary
 sdhc vmac 4000.9999.0100
 sdhc address 01
 sdhc xid 01 05d20006
 sdhc partner 4000.1020.1000 01
```

```

sdhc dlsw 1
!
interface serial 2
  description Node Type 2.1 with SDLC station role set to negotiable or primary
  encapsulation sdhc
  sdhc role none
  sdhc vmac 1234.3174.0000
  sdhc address d2
  sdhc partner 1000.5aed.1f53 d2
  sdhc dlsw d2
!
interface tokenring 0
  no ip address
  early-token-release
  ring-speed 16
  multiring all
  source-bridge 100 1 2000
  source-bridge spanning
!
interface tokenring 1
  no ip address
  ring-speed 16
  multiring all
  source-bridge 400 1 2000
  source-bridge spanning
!
router eigrp 202
  network 150.150.0.0

```

## DLSw+ over Frame Relay Configuration Example

Frame Relay support extends the DLSw+ capabilities to include Frame Relay in direct mode. Frame Relay support includes permanent virtual circuit capability and provides a newly supported DLC. DLSw+ runs over Frame Relay without LACK. It supports the Token Ring-to-Token Ring connections similar to FST and other direct DLCs. Figure 26-11 illustrates a DLSw+ configuration over Frame Relay.

**Figure 26-11 DLSw+ Over Frame Relay**

The following configuration examples are based on Figure 26-11. The Token Rings in the illustration are Ring 2.

### Configuration for Router A

```

source-bridge ring-group 100
dlsw local-peer peer-id 1.1.1.1
dlsw remote-peer 0 frame-relay interface 0 30

```

```
!  
interface tokenring 0  
  ring-speed 16  
  source-bridge active 1 1 100  
!  
interface serial 0  
  mtu 3000  
  no ip address  
  encapsulation frame-relay  
  frame-relay lmi-type ansi  
  frame-relay map llc2 30
```

### Configuration for Router B

```
source-bridge ring-group 100  
dlsw local-peer peer-id 1.1.1.2  
dlsw remote-peer 0 frame-relay interface 0 30  
!  
interface tokenring 0  
  ring-speed 16  
  source-bridge active 2 1 100  
!  
interface serial 0  
  mtu 3000  
  no ip address  
  encapsulation frame-relay  
  frame-relay lmi-type ansi  
  frame-relay map llc2 30
```

## DLSw+ over QLLC Configuration Examples

The following three examples describe QLLC support for DLSw+.

### Example 1

In this configuration, DLSw+ is used to allow remote devices to connect to a DLSw+ network over an X.25 public packet-switched network.

In this example, all QLLC traffic is addressed to destination address 4000.1161.1234, which is the MAC address of the FEP.

The remote X.25-attached 3174 is given a virtual MAC address of 1000.0000.0001. This virtual MAC address is mapped to the X.121 address of the 3174 (31104150101) in the X.25 attached router.

```
interface serial 0  
  encapsulation x25  
  x25 address 3110212011  
  x25 map qllc 1000.0000.0001 31104150101  
  qllc dlsw partner 4000.1611.1234
```

### Example 2

In this configuration, a single 3174 needs to communicate with both an AS/400 and a FEP. The FEP is associated with subaddress 150101 and the AS/400 is associated with subaddress 151102.

If an X.25 call comes in for 33204150101, the call is mapped to the FEP and forwarded to mac address 4000.1161.1234. The 3174 appears to the FEP as a Token Ring-attached resource with MAC address 1000.0000.0001. The 3174 uses a source SAP of 04 when communicating with the FEP, and a source SAP of 08 when communicating with the AS/400.

```
interface serial 0
encapsulation x25
x25 address 31102
x25 map qllc 1000.0000.0001 33204
qllc dlsw subaddress 150101 partner 4000.1161.1234
qllc dlsw subaddress 150102 partner 4000.2034.5678 sap 04 08
```

### Example 3

In this example, two different X.25 resources want to communicate over X.25 to the same FEP.

In the router attached to the X.25 network, every X.25 connection request for X.121 address 31102150101 is directed to DLSw+. The first SVC to be established will be mapped to virtual MAC address 1000.0000.0001. The second SVC to be established will be mapped to virtual MAC address 1000.0000.0002.

```
interface serial 0
encapsulation x25
x25 address 31102
x25 map qllc 33204
x25 map qllc 35765
qllc dlsw subaddress 150101 vmacaddr 1000.0000.0001 2 partner 4000.1611,1234
```

