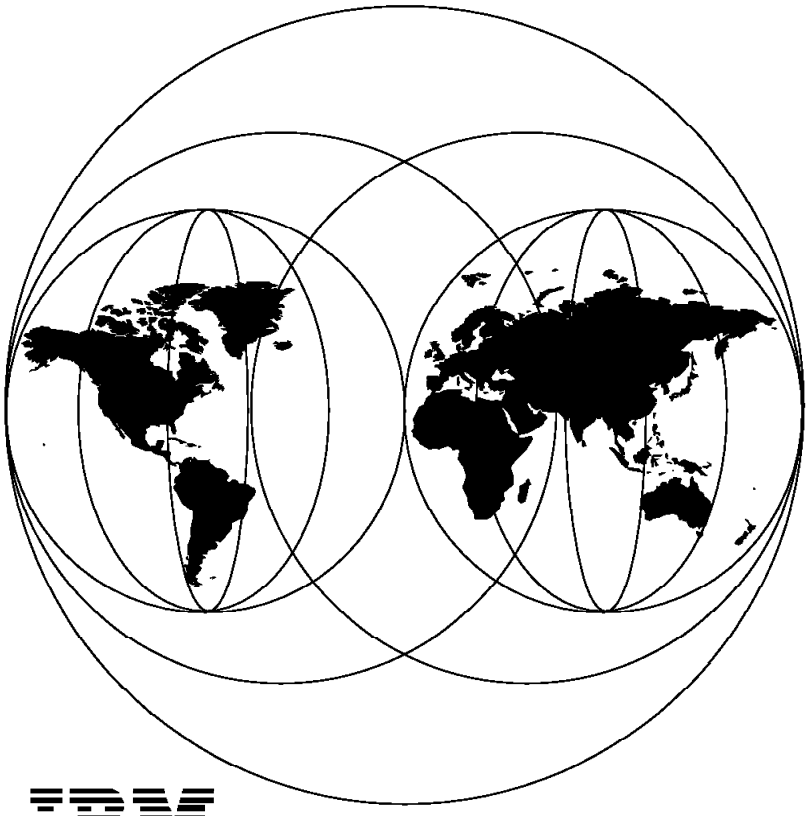
SG24-4956-00

IBM 2210 Nways Multiprotocol Router
IBM 2216 Nways Multiaccess Connector
Description and Configuration Scenarios - Volume II

September 1997



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

SG24-4956-00

IBM 2210 Nways Multiprotocol Router
IBM 2216 Nways Multiaccess Connector
Description and Configuration Scenarios - Volume II

September 1997

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix A, “Special Notices” on page 427.

First Edition (September 1997)

This edition applies to Version 1 Release 1 of the Multiprotocol Routing Services, 5785-B86, for use with the IBM 2210 Nways Multiprotocol Router and Version 1 Release 1 of the Multiprotocol Access Services, 5765-B87, for use with the IBM 2216 Nways Multiaccess Connector.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

Contents

Preface

This redbook describes the SNA and ATM functions of the IBM 2210 Nways Multiprotocol Router and its operating software, the Multiprotocol Routing Services (MRS) and of the IBM 2216 Nways Multiaccess Connector and its operating software, the Multiprotocol Access Services (MAS). It provides a technical overview of functions implemented by the IBM 2210 and 2216 in the SNA environment like APPN, HPR, DLUR and DLSw and in the ATM environment like LAN Emulation and Classical IP. The redbook also contains practical scenario description and implementation showing details on the topology and the commands entered in the console of the 2210 and 2216.

This redbook will help the reader to understand and design the IBM 2210 and the IBM 2216 in the SNA and ATM environments. The many practical scenario implementations will help the reader to configure and customize the IBM 2210 and the IBM 2216 in a real network.

Some knowledge of networking architectures and protocols is assumed.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the Systems Management and Networking ITSO Center, Raleigh.

Juan R. Rodriguez is a Networking Specialist at the Systems Management and Networking ITSO Center, Raleigh. He received his M.S. degree in Computer Science from Iowa State University, writes extensively and teaches IBM classes worldwide on areas such as Networking and Data Security. Before joining the ITSO two years ago, he worked at the IBM laboratory in Research Triangle Park (North Carolina, USA) as a designer and developer of networking products.

Tim Kearby is an Advisory ITSO Specialist for Networking at the Systems Management and Networking ITSO Center, Raleigh. He writes redbooks and teaches workshops on local and wide area networking. Tim has held various positions in his IBM career including assignments in product development, systems engineering, and consulting. He holds a Bachelors of Science degree in Electrical Engineering from Purdue University.

Ricardo Haragutchi is a Senior ITSO Specialist for Networking, Internet and Multimedia at the Systems Management and Networking ITSO Center, Raleigh. He holds a Bachelors of Science degree in Electrical Engineering from Escola Politecnica in Sao Paulo University. He writes extensively and teaches IBM classes worldwide on such areas as routing, remote access, and Internet environment. Before joining the ITSO two years ago, Ricardo worked in the Field Systems Center (FSC) in IBM Brazil as a Senior System Engineer.

John Parker is an IT Specialist in the UK. He has over 25 years of experience in the networking field, and has worked in a technical marketing role for IBM for 29 years. He holds a masters degree in Mechanical Sciences from Cambridge University in the UK. His areas of expertise include most areas of networking, but with a focus on large host-based networks, particularly those using SNA and APPN, and their management and automation.

Andrew Shadbolt is a Systems Engineer in Australia. He has one year of experience in the field. He holds a degree in Electronic Engineering from the University of Tasmania. He has been working in the routing and ATM fields and has written extensively on the ATM support provided on the 2210 and 2216.

Romulo Matriano is a Networking Specialist in the Philippines. He has over four years of experience in the networking field. He holds a degree in Electrical Engineering from the University of the Philippines. His areas of expertise include router, hubs, APPN, and ATM.

Helena Qiu is an Associate I/T specialist in China. She has one year of experience in the networking field. She holds a degree in Computer Science from Zhongshan University in China. Her areas of expertise include routers, hubs and LAN servers. She has written on new adapters, MRS configuration program, SDLC and DLSw.

Thanks to the following people for the invaluable advice and guidance provided in the production of the this edition:

Volkert Kreuk
Harry J. R. Dutton
Carla Sadtler
Barry Nusbaum
John Parker
Mick Lugton
Martin Murhammer
Aroldo Yuji Yai
Gail Wojton
Paul Brown
Shawn Walsh
David Boone
Systems Management and Networking ITSO Center, Raleigh

Acee Lindem
Adel Fahmy
Don Page
Ellen Cybrynski
Ellen Niemitalo
Eric Walls
Frank Pita
Gerry Graham
Hank Schuwarzell
John Baxter
Jon Houghton
Julia Holloway
Julio Vazquez
Karen Heron
Mark Townsley
Peter Gayek
Pramod Patel
Rich Reid
Sallie Everette
Steve Klein
Steve Worley

Terri Davis
IBM Research Triangle Park (2210)

Bill McCauley
Bruce Gillooly
Don Boston
Doug Flint
Gwen Adams
Imre Szabo
Isaac Allen
Janet Andersen
Jason Cornpropst
Jerry Sents
Jim Ayres
Keith Karlsson
Kevin McClain
Paul Shoytush
Pete Andrews
Rainer Jenke
Randy Worzella
Rosemary Cook
Skip Wilder
Szabo Imre
Timothy Smith
Wayne Taylor
Wes Moorehead
IBM Research Triangle Park (2216)

Alfredo Esteban (IBM Spain)
Andrea Paravan (IBM Germany)
Andreas Schmengler (IBM EMEA)
Andres Calzada (IBM Spain)
Anton Eksteen (IBM South Africa)
Babis Liaropoulos (IBM Greece)
Christoph Spielmann (IBM Switzerland)
Claudia Takami (IBM Brazil)
David Hull (IBM US)
David Murray (IBM EMEA)
Frank Petretti (IBM US)
Jean-Paul Verhoustraeten (IBM Belgium)
Joe Consorti (IBM US)
Kacir Samra (IBM Brazil)
Lynda Linney (IBM UK)
Marc Fleuette (IBM US)
Maurizio Ferrando (IBM Italy)
Michael Martin (IBM EMEA)
Mike Prendergast (IBM EMEA)
Mohammad Shabani (IBM UK)
Noboru Umenai (IBM Japan)
Paul Werner (IBM US)
Takeharu Ogura (IBM Japan)
Thierry Chapellier (IBM France)
Wolfgang Singer (IBM Austria)

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in “ITSO Redbook Evaluation” on page 437 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

  For Internet users `http://www.redbooks.ibm.com`
  For IBM Intranet users `http://w3.itso.ibm.com`

- Send us a note at the following address:

  `redbook@vnet.ibm.com`

Part 1. APPN

Chapter 1. 2210 and 2216 SNA Support

This chapter provides a brief summary of the different techniques that the IBM 2210 and IBM 2216 offer for handling SNA traffic, both subarea and APPN. It also briefly summarizes some of the potential benefits of using the APPN routing function rather than the alternative approaches.

The APPN and Data Link Switching (DLSw) capabilities are described in some detail in this redbook, whereas the other techniques are covered in either of the companion volumes *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios Volume I* and *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume I*.

1.1 Methods of Providing SNA Connectivity

There are two general approaches that the router takes to providing SNA connectivity:

- Connection passthrough

  With this approach, one or more routers provide the transport for an SNA connection, either subarea or APPN, without looking at or processing in any way the contents of the SNA headers: the transmission header (TH) and request header (RH). All processing takes place at the logical link level, and the most that the router does is replace the link header of one type for one appropriate to the next hop. In essence, an SNA connection at one side of the router network reappears as an SNA connection at the other side of the router network.

- APPN routing

  The APPN function takes a different approach, and from this stems some of its additional benefits. SNA connections end in the APPN function in a router, such that there is no end-to-end transport of the connection across the router network. The APPN function also interprets and acts on the SNA headers, and from this decides on which APPN connection to forward the message and any other APPN processing that is required before doing so.

1.2 SNA Connection Passthrough

Various techniques are available to transport SNA connections across a network that includes any mix of IBM 2210s and IBM 2216s.

1.2.1 Bridging

The router implements bridging for both Ethernet and token-ring LANs, including both types over ATM, using Forum-Compliant LAN Emulation (FC LANE). The bridging provided is:

- Transparent Bridging (TB) - Ethernet-to-Ethernet
- Source Route Bridging (SRB) - token-ring to token-ring
- Source Route Transparent (SRT) - token-ring to Ethernet
- Source Route Translational Bridging (SRTB) - token-ring to Ethernet

To transport the bridged frames across WAN links, various protocols may be used:

- Point-to-Point Protocol (PPP)
- Frame relay
- IP bridging tunnel

In each case, the SNA connection appears as a bridged LAN to the connecting nodes, and the router network is otherwise transparent. No configuration of the connecting SNA nodes is required in the router network.

1.2.2 Frame Relay Boundary Access Node

Frame-relay boundary access node (BAN) is a variety of bridging that allows a *direct* frame relay connection of a single router to an SNA node. To that node, the SNA nodes attached via the router appear as though they are nodes that are directly LAN-attached, though they may actually be SDLC or X.25 QLLC-attached to the router (exploiting a function of data link switching) rather than LAN-attached. BAN uses the SNA *bridged* format of the RFC 1490 header, and the 802.5 header is transferred across the frame-relay connection.

BAN allows remote routers to connect directly to a central SNA node (for example, an NCP or a 3746 NN) without requiring separate routers at the central site.

1.2.3 Frame Relay Boundary Network Node

Frame-relay boundary network node (BNN) uses a different RFC 1490 header format from BAN. This is referred to as the SNA *routed* format. A DLCI and SAP value must be configured on the router for each attached SNA node. Specification of different SAP values allows multiple SNA nodes to share a single DLCI.

In comparison with BAN, BNN has benefits in terms of reduced frame overhead across the frame-relay link (no 802.5 header), but requires configuration effort at the router. There are also limits to the number of SNA stations that may be connected through a single DLCI because of a limited range of possible SAP values.

1.2.4 Data Link Switching (DLSw)

The primary function provided by DLSw is the reliable transport of SNA (and NetBIOS) traffic using TCP/IP between routers with DLSw endpoints. Between these endpoints, any connectivity that supports IP may be used. In the basic configuration, when connecting LANs, the router network just appears as a bridged LAN to the connecting SNA nodes.

DLSw provides isolation of the local and remote LAN topologies, reducing or eliminating the hop count limits for token-ring SRB. It can also provide local LLC termination, protecting SNA users from the potential impact of attempting to use LAN-oriented LLC values across slower, more congestion-prone WAN connections. Another connection-oriented benefit is the provision of flow control on the connections to individual attaching SNA nodes when WAN connections become congested.

DLSw enables the benefits of IP routing to be extended to SNA users, providing availability benefits by transparently using any alternate routes if intermediate

links or nodes within the router network fail. It also allows intermediate IP routing nodes that do not have any SNA support to be used.

Another useful function that DLSw provides is local LLC termination and conversion. LLC termination is discussed earlier. LLC conversion is provided for:

- SDLC
- X.25 QLLC

The specific LLCs used on these types of link are converted to an 802.2 LLC appearance, and can then be transported by DLSw to a remote DLSw node as though such SNA nodes are LAN-attached.

So there are two basic functions provided by DLSw:

- Remote DLSw-to-DLSw transport
- Local LLC conversion

These may be used individually or in combination.

1.2.5 ESCON LSA

2216 Only

ESCON is not supported by the 2210. ESCON on the 2216 requires MAS V1 R1.1.

Link Services Architecture (LSA) provides SNA-attachment to VTAM using the same external communications adapter (XCA) support as the IBM 3172 with the Interconnect Control Program (ICP).

Two basic capabilities are provided:

- Local LAN interfaces (real or emulated over ATM using FC LAN Emulation) to channel
- Remote DLSw-to-DLSw attachment, providing host channel attachment from any interface supported by a remote DLSw:
  - LAN (real and emulated over ATM)
  - SDLC, X.25 QLLC (LLC conversion)
  - WAN bridging (frame relay or PPP)
  - ESCON LSA

In all cases, the host sees the attached SNA stations as though they are LAN-attached.

1.2.6 SDLC Relay

SDLC relay provides a connection from an SDLC link on one side of the router network to an SDLC link on the other side of the SNA network. The SDLC frames are transported between the routers using IP encapsulation, but *all* SDLC frames (both control and data) are transferred across the router network.

1.3 Benefits of Using APPN on the 2210/2216

From a user session perspective, APPN on the router:

- Terminates LLC connections
- Routes messages at the session level according to information in the SNA headers
- Queues messages according to session priority
- Segments and reassembles messages according to the sizes supported on individual connections (not required for ANR routing)
- Handles hop-by-hop flow control (not required for ANR routing)
- Allows non-disruptive session reroute (HPR only)

The benefits of using APPN on the router rather than the connection passthrough techniques derive from these points, plus the general advantages of using APPN on the attaching SNA nodes, particularly on mainframe hosts. These advantages include:

- Extending use of session priority into the network:
  - In host-based subarea networks, SNA session priority was previously used only up to the most remote NCP.
  - With APPN, session priority is used outbound *at least* as far as the remote router.
- Moving the session routing point into the network:
  - With the connection passthrough techniques, sessions are tied to the connection, and any session routing has to be done by the SNA node at the other end of the connection (such as the boundary NCP or VTAM, in a mainframe-based network).
  - Now, session routing can be pushed out to the furthest router that has alternate connectivity (or even to the end user workstation itself, if it implements APPN and has alternate connectivity). This provides the ability to:
    - Use a more direct route to secondary server nodes.
    - Use any alternate connectivity automatically if there is a loss of a connection or failure of an intermediate node. This requires session re-initiation unless HPR is used.
    - Spread sessions across multiple connections of equal desirability, where alternate connectivity is provided. It may already be in place, perhaps for availability reasons.
    - Remove the dependence on a single “network ownership” VTAM by providing alternate connections via another “owner” VTAM.

    DLUR allows these benefits to be provided for dependent LU sessions as well as for independent LU sessions.
- Dynamic configuration and single definition:
  - Changes to the network topology are recognized immediately and new session paths exploit the current connectivity.
  - Resources are defined where they exist, and their location is discovered when required. This removes the need to define attached nodes and the location of any independent LUs to which they provide a path.
  - DLUR converts all dependent LU/PU definitions into switched ones, even if on leased connections (such as SDLC leased lines), making definition change within VTAM much easier.
- Nondisruptive session reroute:

  - HPR enables connection and intermediate node failures to be bypassed without disrupting user sessions, provided alternate connectivity is available or the single connection can be re-established promptly (including through an alternate gateway).
  - If the end node also supports HPR and has alternate connectivity, it is possible to connect through another remote router, providing continuing session availability even when a local router fails.

- Connection concentration

  A central node only handles a single connection to the nearest APPN router; the connections for the downstream stations are handled by other APPN nodes, such as a remote router.

- Reducing resource requirements in intermediate nodes

  The resources required in intermediate nodes (such as a router, an NCP, or a 3746 NNP), are significantly reduced by using ANR routing (part of HPR) to eliminate the per session storage requirement in such nodes, and to significantly reduce the per message processing load.

- Better network management:
  - With the various connection passthrough approaches, the whole of the router network is invisible to SNA management because it is just part of what appears to be a single connection.
  - With APPN, each hop and node on the session path is visible from a management viewpoint. Therefore, it is useful when:
    - Assisting problem determination.
    - Allowing better usage tracking and analysis.
  - Improved congestion control and avoidance, particularly with HPR.
  - Better control of where traffic is routed.
  - More automatic tuning.

Chapter 2. APPN and the 2210/2216

This chapter provides an overview of the APPN architecture, including the components that make up an APPN network, and some of the more common optional functions that an APPN node may implement. It also describes the specific APPN functions implemented on the 2210 and 2216.

Unless indicated otherwise, all functions apply equally to both the 2210 and the 2216 implementations. The APPN support is essentially the same, with the main differences between the two implementations being a result of physical differences:

- The 2216 has more physical interfaces than the 2210.
- The 2210 has BRI and PRI ISDN; the 2216 PRI ISDN.
- The 2210 has 25 Mbps ATM; the 2216 155 Mbps.
- The 2216 has ESCON; the 2210 does not.
- The 2210 has fixed numbering of physical interfaces; they are variable on the 2216.
- The 2216 has a hard disk; the 2210 does not.
- The 2216 has more memory than the 2210.

Also, because of differences in availability dates, there may be minor APPN software changes or enhancements in MAS that have not yet been added to MRS.

2.1 APPN Overview

Advanced peer-to-peer networking (APPN) extends the SNA architecture by enabling indirectly connected Type 2.1 (T2.1) nodes to communicate without requiring the services of an SNA host computer. In a way, this dramatically reduces the amount of predefinition required.

2.1.1 Peer-to-Peer Communications

T2.1 nodes can activate connections with other T2.1 nodes and establish LU-LU sessions with these nodes. The relationship between a pair of T2.1 nodes is referred to as a *peer relationship* because either side can initiate communication.

Prior to APPN, a T2.1 node could communicate directly with another T2.1 node, but required the services of a centralized SNA host to locate its partner and any associated resources in a network where all the nodes were not fully intermeshed. All routes between the two nodes had to be predefined, as was the location of partner LUs.

APPN enhanced the T2.1 node function by:

- Requiring network resources to be defined only at the node where they are located
- Distributing information about these resources throughout the network as needed

- Dynamically generating routes between nodes using current information about the network's topology and the desired class of service

2.1.2 APPN Node Types

The APPN architecture allows four types of nodes in a network:

- APPN network nodes
- APPN end nodes
- Low-entry networking (LEN) nodes
- PU 2.0 nodes supported by DLUR

The router can be configured as an APPN network node that supports connections with all four node types. The router cannot function as an end node for APPN.

2.1.2.1 APPN Network Node

An APPN network node provides directory and routing services for all resources (LUs) in its domain. A network node's domain consists of:

- Local resources owned by the node
- A control point (CP), which manages the node's resources
- Resources owned by APPN end nodes and LEN nodes that use the services of the network node

APPN network nodes also:

- Exchange information about the topology of the network. This information is exchanged each time network nodes establish a connection or when there is a change in the topology of the network (such as when a network node is deactivated, brought online, or when a link is congested or fails). When a network node receives a topology update, it broadcasts this information to other active network nodes with which it has CP-CP sessions.
- Act as intermediate nodes, receiving session data from one adjacent node and passing that data on to the next adjacent node along the route.

As a network node, the router can act as a server to attached APPN end nodes and LEN nodes and provide functions that include:

Directory services

The network node, communicating with other network nodes, can locate a resource in the network on behalf of an APPN end node. The network node also maintains a local directory containing the location of resources in adjacent LEN nodes and (usually) in adjacent APPN end nodes that use the services of the network node. This directory also contains dynamically built entries indicating the last known location of remote LUs as their location is discovered during session initiations with LUs served by the network node.

Topology and routing services

At the request of an adjacent APPN end node or LEN node, the network node dynamically determines the most appropriate route from an origin logical unit (LU) to a destination LU in the network. The network node also maintains information on other network nodes and the routes to those nodes. The route selected is based on the current topology of the

network as well as the class-of-service requested and connection (link) characteristics.

Management services
The network node can pass *alert* conditions to a designated focal point to allow centralized problem management. The network node is responsible for processing alert conditions for all the resources in its domain. 2.2.4, “APPN Management” on page 22 describes this process.

2.1.2.2 APPN End Nodes

An APPN end node provides limited directory, routing, and management services for logical units (LUs) associated with the node. An APPN end node selects a network node to be its network node server. If the network node agrees to act as the APPN end node’s server, the end node can register its local resources with the network node. This enables the network node server to intercept and pass along search requests for resources located on the APPN end node rather than sending search requests to all of its attached APPN end nodes.

The APPN end node and its network node server communicate by establishing CP-CP sessions. An APPN end node may be connected to a number of network nodes, but only one of these nodes acts as the APPN end node’s server at any one time.

When the APPN end node wants to initiate a session with a remote partner, it sends a LOCATE request to the network node server. The network node server, in turn, uses its search facilities to locate the requested resource and calculate a route from the APPN end node to the resource. It then returns the route information to the end node, and the end node sends the BIND to start the session along that route.

2.1.2.3 LEN Nodes

A LEN node is a T2.1 node without APPN extensions. A LEN node can establish peer connections with other LEN nodes, APPN end nodes, and APPN network nodes, as long as all of the required destination LUs are defined in the LEN node. A LEN node can also serve as a gateway between an APPN network and an SNA subarea network.

Because a LEN node cannot establish CP-CP sessions with an APPN network node server, it cannot register its resources with the server, or request that the server search for a resource and dynamically calculate a route to that resource. A LEN node may indirectly use the directory and routing services of a network node by predefining remote LUs (owned by non-adjacent nodes) as being located on an APPN network node, although the actual location may be anywhere in the network. When the LEN node needs to initiate a session with the remote LU, it sends a session activation request (BIND) for the LU to the network node. In this case, the network node acts as the LEN node’s network node server, locating the requested resource, calculating a route, and forwarding the BIND to its correct destination.

When configuring the router network node, you can specify the names of LUs that are associated with an attached LEN node. These LU names reside in the router network node’s local directory. If the router network node receives a request to search for one of these LEN node resources, it will be able to find the LU in its local directory and return a positive response to the node originating the search. To reduce the number of LU names you need to specify for an

attached LEN node, network nodes usually support the use of generic LU names. A generic name includes a wildcard character to represent a portion of a target LU name.

2.1.2.4 PU 2.0 Nodes

A PU 2.0 node is a T2.0 node containing dependent LUs. PU 2.0 nodes are supported by the dependent LU requester (DLUR) function which is implemented by an APPN end node or network node. PU 2.0 nodes require the services of a system services control point (SSCP), which is made available through the DLUR-enabled APPN node.

Note that APPN nodes can contain dependent LUs supported by an internal DLUR function. Alternatively, APPN nodes that do not contain the DLUR function, but do contain dependent LUs, require DLUR support in an adjacent network node to allow those LUs to communicate across an APPN network. In such a case, the APPN node will also have a PU 2.0-like appearance to the DLUR support in the adjacent APPN network node.

2.2 What APPN Functions Does the Router Implement?

The router implements the APPN Release 2 base architecture functions for a network node, as defined in the *SNA APPN Architecture Reference*, and a number of important additional option sets.

2.2.1 Base APPN Functions

The base APPN network node functions implemented by the router are summarized in Table 1. Notes on specific functions follow the table. The additional APPN functions that the router implements are summarized in 2.2.2, “APPN Optional Functions” on page 15.

For a description of the APPN management services supported by the router, see 2.2.4, “APPN Management” on page 22.

APPN uses LU 6.2 protocols to provide peer connectivity between CP-CP session partners. The router network node implements the LU 6.2 protocols required for CP-CP sessions and those used in sessions between a network node CP and its network management focal point. The router implementation of APPN does not provide an application program interface to support user-written LU 6.2 programs.

Note that the router does not contain any dependent LUs.

Table 1 (Page 1 of 2). Implementation of APPN Network Node Functions on the IBM 2210 and IBM 2216

APPN Function	Yes	No	Notes
Session services and supporting functions			
Multiple CP-CP sessions	X		
Mode name to class of service (COS) mapping	X		1
Limited resource link stations	X		2
BIND segmentation and reassembly	X		3
Session-level security	X		4
Intermediate session routing			
Intermediate session routing	X		
Routing of dependent LU sessions	X		
Fixed and adaptive session-level pacing	X		

Table 1 (Page 2 of 2). Implementation of APPN Network Node Functions on the IBM 2210 and IBM 2216

APPN Function	Yes	No	Notes
RU segmentation and reassembly	X		5
Directory services			
Broadcast searches	X		
Directed searches	X		
Directory caching	X		
Safe storage of directory services cache		X	6
Central directory server		X	7
Central directory client	X		7
Registration of APPN EN LUs with network node server	X		
Definition of LEN node LUs on network node server	X		
Use of wild cards to define attached LEN node resources	X		
Accept multiple “resource found” conditions	X		
Network node server for DLUR EN - option set 1116	X		
Topology and routing services			
Topology exchange	X		
Periodic topology broadcasts	X		8
Topology database maintenance	X		9
Enhanced garbage collection		X	10
Topology awareness of CP-CP sessions	X		
Randomized route computation	X		11
Cached routing trees	X		12
Safe storage of topology database	X	X	13
Connectivity			
Connection network definition	X		14
Multiple transmission groups	X		
Parallel transmission groups	X		
Management services			
Multiple domain support (MDS)	X		
Explicit focal point	X		
Implicit focal point		X	
Held alerts	X		
SSCP-PU sessions with focal points		X	
SNA/MS problem diagnosis data in alerts	X		

Notes:

1. New mode names can be defined on the router using the command line interface. These new mode names can be mapped to existing class of service (COS) definition names or to new COS definitions, which may be defined using the configuration program.
2. Limited resource link stations are supported for:
   - Connection network links
   - X.25 SVC links
   - PPP links running over ISDN or V.25 bis
   - Frame relay links running over ISDN
3. When the router activates a TG to an adjacent node, it negotiates with this node the maximum message size that can be sent across the TG. If a BIND message is larger than the negotiated message size, the router segments the BIND. Segmentation only occurs if the adjacent node is capable of reassembling the BIND. The router supports BIND reassembly.
4. A session-level security feature can be enabled for connections between the router network node and an adjacent node. Both partners in the connection

require a matching hexadecimal key that enables each node to verify its partner before the connection is established.

5. When routing session data to an adjacent node, the router segments a request/response unit (RU) if the message unit exceeds the maximum message size that can be sent across the transmission group. If the router receives a segmented RU, it is reassembled before onward routing.
6. After successfully locating a resource in the APPN network, the router stores or *caches* this information in its local directory database for future use. However, the router does not save these cached directory entries to a permanent storage medium, such as a disk, to provide for cache recovery if the node fails.
7. The router cannot be used as a central directory server for an APPN network. However, if there is a central directory server in the APPN topology subnetwork, then the router will use it to obtain directory information about the location of a resource rather than do a broadcast search.
8. To prevent other network nodes from discarding information about the router from their topology databases, the router creates a topology database update (TDU) about itself and its locally owned transmission groups every five days and broadcasts this TDU to adjacent network nodes.
9. An interval timer is associated with every resource entry in the router's network topology database. If the router does not receive any information about a resource within 15 days, it discards the entry for that resource from the database.
10. This is an enhancement to the original topology database maintenance protocols that is implemented by some products.
11. If there is more than one least-weighted route from an origin LU to a destination LU for a given class of service, the router randomly selects one of these routes for the session. This practice helps distribute the flow of traffic in the network.
12. The router maintains a copy of the network topology database. The database identifies the available routes to other network nodes for a particular class of service. When the router needs to calculate a route to a network node or to an end node adjacent to that network node, it uses information in the topology database to generate a routing tree for that network node. The routing tree identifies the optimal routes to the network node for the class of service required.

    When the router generates a new routing tree, it stores this tree in a cache. Then, before the router selects a route, it checks this cache first to see if a route has been computed. Use of the cache reduces the number of route calculations required. When the router receives topology information that invalidates a routing tree, it discards the tree. The router then recalculates the tree as needed and caches the new tree.
13. Optionally, the router stores the topology database on a permanent storage medium (disk), and uses this saved information to enable faster network recovery during router APPN restart, mainly by reducing the volume of topology data interchanged with adjacent network nodes.

2216 Only

Safe storage of topology is supported only by the 2216. The 2210 does not support the prerequisite option set 1201 (permanent storage medium).

By default, this optional capability is disabled. If enabled, the topology information is saved to disk once a day during garbage collection.

14. The router can be defined as a member of a connection network on Ethernet and token-ring ports, or over emulated LANs of either type using FC LANE over ATM.

2.2.2 APPN Optional Functions

In addition to the base APPN architecture functions, the router also implements the following option sets and additional functions:

1002 Adjacent link station name

1007 Parallel TGs

1012 LU name = CP name

1067 Dependent LU requester

1071 Generalized ODAI usage

1101 Preloaded directory cache

1107 Central resource registration (of LUs)

1116 Network node server support for DLUS-Served LU registration

1200 Tree caching and TG caching

1201 Permanent storage medium

2216 Only

The 2210 does not implement this option set.

1400 High-Performance Routing base (ANR)

1401 Rapid Transport Protocol (RTP)

1402 Control Flows over RTP

2.2.2.1 High-Performance Routing

HPR is an enhancement to the APPN architecture that provides better performance over high-speed, low error-rate links using existing hardware. HPR replaces the normal APPN intermediate session routing (ISR) with a Network Connection Layer (NCL) containing a new type of source routing function called automatic network routing (ANR). The complete HPR route is contained in the ANR packet allowing intermediate routing nodes to route the packets with less processing overhead and storage.

HPR also eliminates the error recovery, flow control (session-level pacing), and segmenting and reassembly procedures for each link between nodes. The responsibility for these functions is moved to the endpoints of an HPR connection. A transport layer using a new error recovery procedure, called Rapid Transport Protocol (RTP), is used by the endpoints of the HPR connection. HPR intermediate nodes have no session or RTP connection awareness. This new transport layer features:

- Selective retransmission error recovery procedure.
- Segmentation and reassembly.
- Adaptive Rate-Based (ARB) flow and congestion control mechanism that meters data onto a route in order to allow efficient utilization of network resources while minimizing congestion. ARB uses a preventative rather than reactive approach to flow and congestion control.
- Nondisruptive Path Switch (NDPS) function that automatically reroutes traffic around node or link failures without disrupting enduser sessions.
- Reaction to the receipt of the frame-relay Forward Explicit Congestion Notification (FECN) bit, allowing RTP′s adaptive rate-based flow and congestion control algorithm to adjust the data sending rate. This algorithm prevents traffic bursts and congestion, maintaining a high level of throughput.

The router implements both ANR routing and Rapid Transport Protocol; therefore, the router can function both as an intermediate routing HPR node and as an HPR connection endpoint node.

Interoperability: HPR uses APPN network control functions including class of service (COS)-based least-weight route calculation and transmission priority. HPR interoperates seamlessly with APPN ISR:

- The network automatically adapts to the presence of HPR-capable nodes and HPR-enabled links.
- An APPN network can have any mix of ISR and HPR links, although the greatest benefit of HPR is realized when the network has three or more HPR-enabled nodes with two or more HPR-capable links back-to-back. This allows the middle HPR node to be an HPR intermediate node and use only ANR routing, allowing session data to be routed through the middle node using only the NCL.
- A given session route can be made up of a combination of ISR and HPR links.
- HPR uses the same TG and node characteristics for least-weight route calculation as APPN ISR. No special consideration is given to HPR-capable nodes or links other than their potentially improved characteristics (such as higher effective capacity if a higher speed link).

Traffic Types: APPN ISR uses the QLLC protocol for X.25 direct data link control; the IEEE 802.2 LLC Type 2 protocol for token-ring, Ethernet, PPP, and frame relay; and SDLC protocol for the SDLC data link control. APPN HPR, which is supported on token-ring, Ethernet, PPP and frame relay, does not use LLC Type 2 protocol, but does use some functions of an APPN link station for XID and inactivity timeout purposes. Therefore, a single APPN link station is used for both ISR and HPR. Different mechanisms are used to distinguish between ISR and HPR traffic, depending upon the DLC type:

- For token-ring and Ethernet LAN ports:

  Each protocol that uses a port must have a unique SAP address, with the exception of DLSw (which may use the same SAP address as other protocols because DLSw frames will not be destined for the local MAC address, but rather a DLSw/MAC address). A unique SAP address identifies HPR traffic (local HPR SAP address parameter). If ISR traffic is destined for a link station, then a different SAP address (local SAP address parameter) must be

used. The ISR traffic uses LLC Type 2 LAN frames. The HPR traffic is handled in a similar fashion to LLC Type 1 LAN frames and must have a different SAP address.

The default SAP address for HPR traffic is X′C8′. If X′C8′ has already been used by another protocol on a port, the default must be overridden.

Note: There is only one APPN link station even though APPN ISR and HPR traffic use different SAP addresses.

- For frame relay ports:

  APPN ISR traffic and APPN HPR traffic transferred over a frame-relay data link connection support both the RFC 1490 bridged frame format and the RFC 1490 routed frame format.

  – RFC 1490 routed frame format

    APPN ISR traffic will be transferred over a frame-relay data link connection using the connection-oriented multiprotocol encapsulation method defined in RFC 1490 using:
    - NLPID = X′08′ (Q.933 encoding)
    - L2PID = X′4C80′ (layer 2 protocol identifier indicating 802.2 LLC)
    - L3PID = X′7083′ (layer 3 protocol identifier indicating SNA-APPN/FID2)

    APPN HPR traffic transferred over a frame-relay data link connection does not use IEEE 802.2 LLC. It uses a different multiprotocol encapsulation as defined in RFC 1490 using:
    - NLPID = X′08′ (Q.933 encoding)
    - L2PID = X′5081′ (layer 2 protocol identifier for no layer 2 protocol)
    - L3PID = X′7085′ (layer 3 protocol identifier indicating SNA-APPN/HPR)

    APPN HPR does not use a SAP for traffic transferred using the RFC 1490 routed frame format because there is no layer 2 protocol.

  – RFC 1490 bridged format

    APPN HPR uses a different SAP for traffic transferred using the RFC 1490 bridged frame format.

- For PPP ports:

  – APPN ISR traffic uses 802.2 LLC over the PPP connection.

  – Since there is no layer 2 protocol used in HPR′s RFC 1490 encapsulation, no SAP is used for HPR traffic.

Refer to Table 2 on page 20 for a list of DLCs that support HPR.

Note: HPR is not supported over SDLC, X.25, DLSw, or ESCON LSA ports.

2.2.2.2 Dependent LU Requester

The dependent LU requester (DLUR) option extends the support of T2.0 or T2.1 devices containing dependent LUs to APPN networks. The DLUR function on an APPN network node or an APPN end node works in conjunction with a dependent LU server (DLUS) in a mixed APPN/subarea network. The DLUS function may reside in some other part of the mixed network than the DLUR, but there must be an APPN route between the DLUR and the DLUS.

The dependent LU flows (SSCP-PU and SSCP-LU) are encapsulated over an LU 6.2 (CP-SVR) pipe established between the DLUR APPN node and the DLUS

SSCP. The CP-SVR pipe is made up of a pair of LU 6.2 sessions using a special CPSVRMGR mode between the DLUR and the DLUS. This pipe brings the SSCP function (in the DLUS) to the DLUR APPN node where it can be made available to attached T2.0/T2.1 nodes containing dependent LUs.

The dependent LU will appear to be within the domain of the serving SSCP. Session initiation flows will be emulated from the DLUS, but the session BIND and data paths will be calculated directly between the dependent LU and its session partner using APPN protocols. This path may or may not traverse the serving DLUS node, but must pass through the DLUR node.

See Table 2 on page 20 for the types of port that are supported by DLUR for the attachment of downstream PUs (DSPUs).

Functions Supported: The APPN DLUR option includes the following functions:

- Support for SDLC-attached downstream T2.0 nodes containing dependent LUs that do not support XID exchange.
- Support for downstream T2.0 nodes containing dependent LUs that respond with XID type 0 and XID type 1.
- Support for downstream T2.1 nodes containing dependent LUs that respond with XID type 3.
- Support for dependent LUs that is equivalent to the support provided by the subarea environment for:
  - Activating PUs and their LUs
  - Locating and being located by other LUs in an APPN or subarea network
  - Determining the characteristics of an LU
  - Allowing terminal operators to log on to applications both in APPN and subarea networks
  - Supporting SSCP giveback and takeover
  - Continuing LU-LU sessions, if the supporting DLUS (SSCP) fails
  - Supporting session initiation requests from a secondary LU, a primary LU, or a third party, including queuing requests and the RELREQ option

Restrictions: The DLUR option, as implemented on the router network node, has the following functional restrictions:

- Only secondary LUs (SLUs) can be supported by the DLUR function. An LU supported by DLUR cannot function as a primary LU (PLU).
- Because only SLUs are supported, connections to the Network Routing Facility (NRF) and Network Terminal Option (NTO) products are not supported.
- Extended recovery facility (XRF) and XRF/CRYPTO are not supported.
- There must be an APPN route between the DLUR and the DLUS because the CPSVRMGR control sessions cannot pass through a subarea network. (However, a subarea part of a mixed subarea/APPN network can be traversed if VR-TG is used to give that subarea route an APPN capability.) If a APPN border node is used (either within the same network ID or between network IDs), the DLUS can reside in a different topology subnetwork from the DLUR.

Note that most of these restrictions are general DLUR restrictions and are not specific to the router implementation.

2.2.2.3 APPN Connection Network

When nodes are attached to a shared-access transport facility (SATF), any-to-any connectivity is possible. This any-to-any connectivity allows direct connections between any two nodes, eliminating the necessity to route through intermediate network nodes and data traversing the SATF multiple times. To achieve this direct connectivity, however, TGs must be defined on each node to all the other possible partners.

Defining connections between all possible pairs of nodes attached to the SATF results in a large number of definitions (increasing in the order of the square of the number of nodes involved), and also a large number of topology database updates (TDUs) flowing in the APPN network if the interconnected nodes are network nodes. To alleviate these problems, APPN allows nodes to become members of a connection network to represent their attachment to an SATF. Session traffic between two end nodes that have been defined as members of a connection network can be routed directly, without passing through a network node. To become a member of a connection network, an APPN node′s port must be attached to a connection network by defining a connection network interface. When the port is defined, a connection network TG is created by the APPN component to identify the direct connection from the port to the SATF (that is, the connection network). This TG is not a conventional TG as in the case of defined link stations, but rather represents the connection to the connection network in the topology database.

Note: TGs for end nodes are not contained in the network topology database, but are contained in the node′s local topology database. TDUs do not flow through the network when a connection is established through a connection network or when an end node is made a member of a connection network.

Because the connectivity is represented by a TG from a given node to a connection network, normal topology and routing services (TRS) can be used by a network node server to calculate the direct path between any two nodes attached to the SATF (with TGs to the same connection network). DLC signaling information is returned from the destination node during the normal locate process to enable the origin node to establish a dynamic connection directly to the destination node.

Therefore, to achieve direct connectivity on an SATF, instead of each node on the SATF being defined (or connected) to each other, each node is connected to a connection network. The connection network is often visualized as a virtual node on the SATF to which all other nodes are attached. This model is frequently used and, in fact, the term virtual routing node (VRN) is often interchanged with the term connection network.

When a connection network is defined, it is named. This name then becomes the CP name of the VRN and must follow the usual rules for CP names.

Restrictions of the APPN connection networks are:

- Connection networks defined on the router network node are only supported on token-ring and Ethernet LAN ports, including those using FC LANE over ATM.
- The same connection network (VRN) can be defined on only one LAN. However, the same VRN can be defined on multiple ports (with the same characteristics) to the same LAN.

- The same connection network can be defined on a maximum of five ports to the same LAN on the router network node.
- There is only one connection network TG from a given port to a given connection network's VRN.
- The same connection network TG characteristics apply for each port on which a given connection network is defined on this router network node. The TG characteristics could be different on a different node.
- Because the VRN is not a real node, CP-CP sessions cannot be established with or through a VRN. However, the same LAN port can be used for CP-CP sessions using a direct connection to an adjacent node.
- When a connection network is defined on the router network node, a fully qualified name is specified for the connection network name parameter. Only connection networks with the same network ID as the router network node may be defined. The network ID of the VRN is then the same as the network ID of the router network node.

2.2.3 Interfaces Used by APPN

The router APPN function can connect to other APPN, LEN, or PU type 2 nodes using most of the available interface types. This connection layer involves the use of a data link control (DLC) function appropriate to the physical interface and, where appropriate, the particular link layer protocol desired.

2.2.3.1 Supported DLCs

Table 2 shows the ports supported by the router for APPN. An appropriate DLC is provided for each type.

Table 2 (Page 1 of 2). Port Types Supported for APPN Routing

Port Type	Standard	HPR	ISR	DLUR 1
Ethernet	Version 2	Yes	Yes	Yes
Ethernet	IEEE 802.3	Yes	Yes	Yes
Token-Ring	802.5	Yes	Yes	Yes
ATM LANE - Ethernet	Forum-compliant	Yes	Yes	Yes
ATM LANE - Token-Ring	Forum-compliant	Yes	Yes	Yes
Native ATM 2		(Yes)	(No)	(No)
Serial PPP		Yes	Yes	No
PPP over ISDN		Yes	Yes	No
PPP using V.25bis		Yes	Yes	No
Serial FR (BAN - bridged) 3		Yes	Yes	Yes
Serial FR (BNN - routed) 3		Yes	Yes	Yes
FR over ISDN		Yes	Yes	Yes
Serial LAN bridging		NA	NA	NA
SDLC		No	Yes	Yes
X.25 (QLLC) 4	CCITT X.25	(No)	(Yes)	(Yes)
DLSw (remote only) 5		No	Yes	Yes
ESCON LCS 6		No	No	No
ESCON LSA 6		No	Yes	No

Table 2 (Page 2 of 2). Port Types Supported for APPN Routing

Port Type	Standard	HPR	ISR	DLUR 1
ESCON MPC+ 6		Yes	No	No

Notes:

1. This column refers to the port providing the connection to the downstream PU (DSPU).
2. IBM has stated that it intends to make this support available for both the 2210 and 2216 in future levels of MRS and MAS. Note that the support is for HPR only.
3. Use bridged format (BAN) when you have two routers connected by frame relay and one of them does not have APPN capability. Otherwise, use routed format for improved performance.
4. At initial availability, neither MRS V1R1.0 nor MAS V1.R1.0 provided X.25 QLLC support for APPN. However, IBM has stated that it intends to make this support available for both the 2210 and 2216.
5. Since APPN can run over DLSw, you can route any APPN ISR traffic across any port supported by DLSw, including X.25 and Classical IP over ATM, among others.
6. The 2210 does not provide ESCON support.

2216 Only

ESCON support on the 2216 requires MAS V1R1.1 or higher. Note that MPC+ is HPR only, and LSA is ISR only.

LCS is for TCP/IP only.

Parallel TG Restrictions: APPN connections are referred to as transmission groups (TGs), though in the case of the router, a TG may only involve the use of a single connection. In APPN, it is quite permissible to have multiple TGs between the same two APPN nodes, though each TG will be known by a different TG number. Such TGs are known as parallel TGs.

There are a number of restrictions that the router implementation imposes on parallel TGs:

- Parallel TGs are not supported between two router network nodes using the same port on each router. However:
  - Parallel TGs are supported between two router network nodes using different ports on one or both routers.
  - Parallel TGs are supported between a router network node and another non-router remote node over the same port using different remote SAP addresses, provided that the remote node has a mechanism to define or accept different local SAP addresses for APPN on the same port.

2.2.4 APPN Management

You can manage the router network node as an APPN entry point, which forwards APPN-related alerts to an APPN focal point, or as an SNMP-managed node. The router supports MIBs for APPN, HPR, DLUR and SNANAU.

2.2.4.1 Sending APPN-Related Alerts to an SNA Management Focal Point

The router network node can serve as an APPN entry point for alerts related to APPN. As an entry point, the router is responsible for forwarding APPN and LU 6.2 generic alerts about itself and the resources in its domain to a *focal point* for centralized processing. A focal point is an entry point that provides centralized management and control for other entry points for one or more network management categories.

Note: If the focal point node is not available to receive an alert from the router network node, the alert is “held” (stored) by CPMS. APPN on the router can hold up to ten alerts.

Entry points, such as the router, that communicate with a focal point make up that focal point’s *sphere of control*. If a focal point explicitly defines the entry points in its sphere of control and initiates communication with those entry points, it is an *explicit focal point*. If a focal point is designated by its entry points, which initiate communication with the focal point, the focal point is an *implicit focal point*. The focal point for the router is an explicit focal point.

If the session between the router entry point and its primary focal point fails, the router can initiate a session with a designated backup focal point, provided it has been informed by the primary focal point of the backup focal points it is to use. Before initiating a session with a backup focal point, the router entry point makes an attempt to re-establish communication with its primary focal point. If that attempt fails, the router switches to the backup focal point. The primary focal point is then responsible for re-establishing the focal point to entry point relationship with the router.

The router entry point communicates with the focal point through an LU 6.2 session. Multiple domain support (MDS) is the mechanism that controls the transport of management services requests and data between these nodes. The router network node does *not* support SSCP-PU sessions with focal points.

Management processes within the router’s control point are handled by its control point management services (CPMS) component. The CPMS component within the router network node collects unsolicited problem management data from resources within the router’s domain and forwards this data to the appropriate focal point.

Supported Message Units: The router network node uses the following message units for sending and receiving management services data, including alert messages from domain ENs:

Message unit	Description
CP-MSU	Control point management services unit. This message unit is generated by CPMS and contains alert information forwarded by the router entry point. CPMS passes CP-MSU message units to MDS.

MDS-MU Multiple domain support message unit. This message unit is generated by MDS. It encapsulates the CP-MSU for transport between nodes.

2.2.4.2 Managing the Network Node Functions from an SNMP Manager

The router network node can function as an SNMP-managed node. An operator or application at an SNMP network management station can query objects in the APPN MIBs (using the SNMP get and get_next commands) to retrieve APPN status information and node statistics. A subset of APPN MIB objects can be modified using the SNMP set command.

As an SNMP-managed node, the router can send unsolicited status and error information, in the form of traps, to an SNMP manager.

MIBs Provided by APPN: The MIB support provided by APPN in MRS V1R1.0 and MAS V1R1.0 is:

- Support of Get, Get_Next, Set, and Trap
- APPN MIB
- APPN HPR MIB
- APPN DLUR MIB
- RPC 1666 - SNA NAU MIB

The MIB support provided by APPN in MAS V1R1.1 is:

- Support of Get, Get_Next, Set, and Trap
- IETF Standard APPC MIB - RFC 2051
- IETF Standard APPN MIB
- IETF Standard APPN HPR MIB
- IETF Standard APPN DLUR MIB
- RPC 1666 - SNA NAU MIB
- Portions of the previously available private APPN MIB
  - DLC Trace, Memory, and Accounting
- Portions of the previously available private APPN HPR MIB
  - HPR NCL and Route Test

Note that MIB information is also available for the underlying interfaces and protocols that APPN uses. APPN is just a logical protocol that sits above and uses the interfaces.

Router and Bridge Manager (RABM): The Router and Bridge Manager components of the IBM Nways Campus Manager and IBM Nways Enterprise Manager products provide SNMP-based graphical management of APPN nodes. Both the 2210 and 2216 APPN functions can be managed from RABM.

Via an interactive graphical user interface, RABM displays the APPN topology, along with the status of each APPN router and other APPN nodes. A non-IP discovery technique is used to dynamically find APPN nodes. Color-coded icons show the status for APPN network nodes and end nodes, transmission groups, and the APPN function. A rich set of functions are provided to display information about and control the APPN network.

2.2.4.3 Providing Topology Information to the SNA Topology Manager

The SNA Topology Manager (SNATM) components of TME 10 NetView for OS/390 and NetView for MVS/ESA V3R1 provide object-oriented management and control of SNA subarea and APPN networks. SNATM uses CMIP protocols over SNA transport to communicate with agents, which provide it with topology information. CMIP-based agents are provided for such products as VTAM V4R3, Communications Manager/2 and Communications Server/2, the 2217, and the 3746-9X0 Network Node Processor.

The 2210 and 2216 APPN implementations do not provide a CMIP over SNA agent, so their APPN topology cannot be managed directly, in a transparent way, from mainframe NetView. A new product, the TME 10 NetView for OS/390 APPN Topology Integrator, is available to bridge this gap.

APPN Topology Integrator: The Integrator is software that runs under OS/2 Warp. It uses CMIP over SNA to communicate with host NetView, and SNMP over IP to talk to one or more SNMP-managed APPN nodes, including the 2210 and the 2216. One integrator can interface to a significant number of APPN SNMP agents, the number being dependent on the available PC memory and processor power.

The full set of SNATM functions is provided for APPN nodes managed via the Integrator, including:

- Initial topology retrieval
- Topology status change notification
- Network topology
- Local topology
- Control of ports
- Control of link stations

The presence of one or more integrators is transparent to the NetView operator. Internally, VTAM uses entries in its CMIP directory definition file to direct topology requests for appropriate APPN nodes to an Integrator, which, acting as a proxy, accepts CMIP requests. The Integrator issues appropriate sequences of SNMP requests, before building a CMIP response. It also regularly polls its SNMP agents for APPN topology changes, and if any are detected, builds a status update notification and sends it to NetView using CMIP.

The APPN Topology Integrator is made available via the RPQ (Request for Price Quotation) process.

2.3 APPN Session Path Examples

This section uses diagrams to illustrate how the router supports ISR and HPR routing, and the components of APPN that are involved. It also illustrates the use of RTP for CP-CP sessions.

For the sake of illustration, a simple configuration based on two network nodes is used, one being a 2210 and the other a 2216. Each acts as a network node server for an end node. All examples use the same configuration. Note that the

partner network node can be any other product that implements the same network node function; it does not have to be a 2210 or 2216.

2.3.1 Using ISR Routing Only

Figure 1 illustrates the CP-CP session connectivity that is a prerequisite for any APPN communication between the end nodes. Note that the ISR function is not used in either network node.

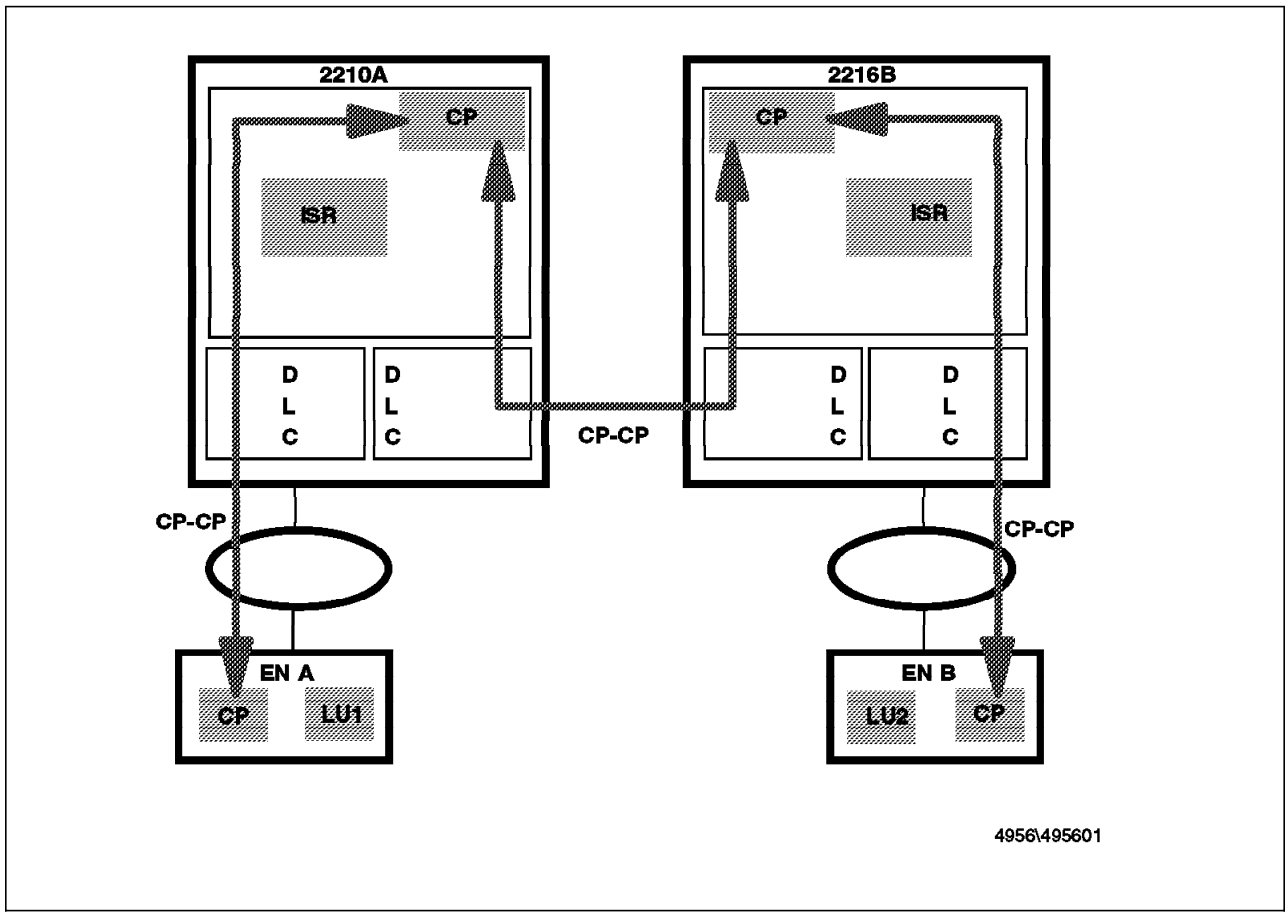


Figure 1. CP-CP Sessions - No HPR

Figure 2 on page 26 illustrates the path taken by an LU-LU session between the two end nodes when ISR routing is used. Note that the LU-LU sessions uses ISR function in both network nodes.

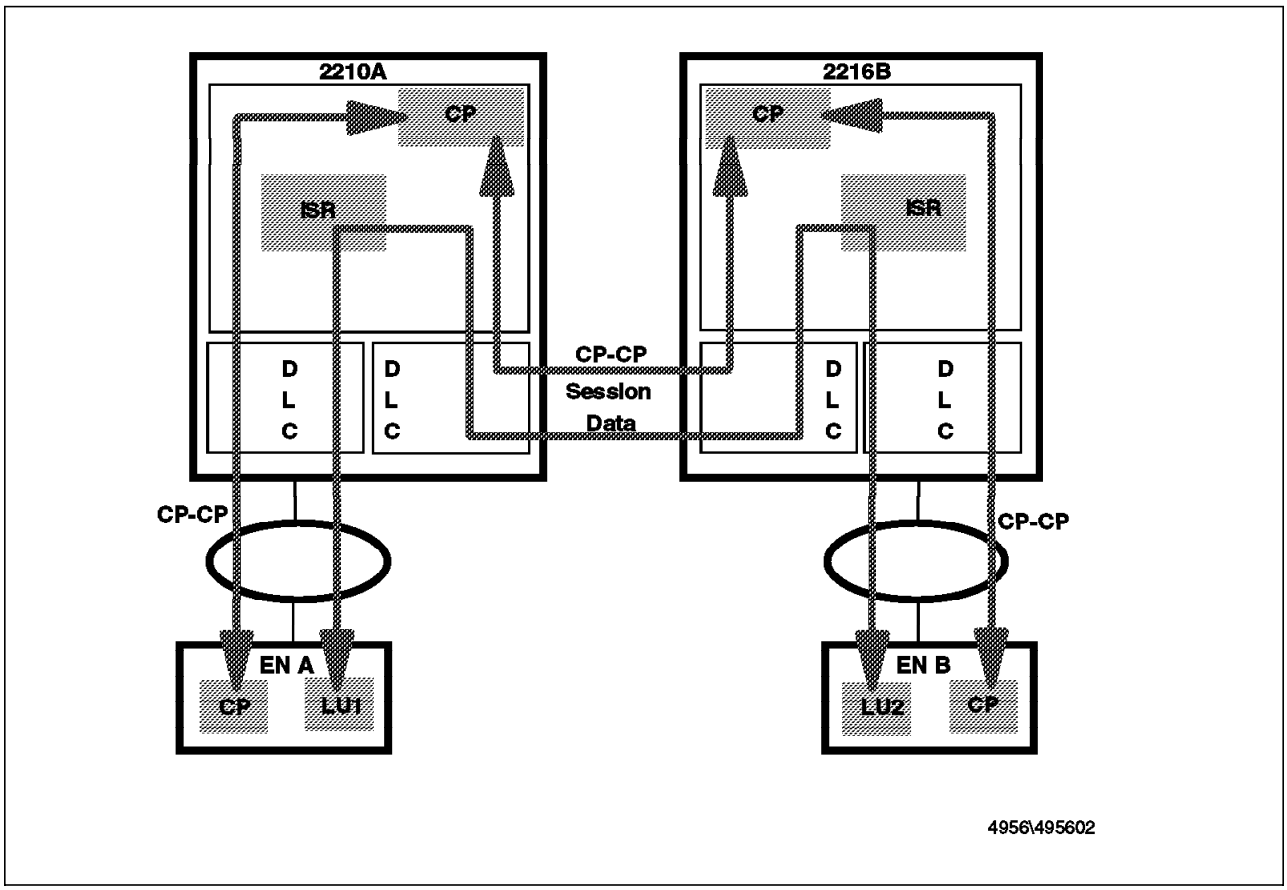


Figure 2. LU-LU Session Using ISR

2.3.2 Using HPR between the Routers

Figure 3 on page 27 is a variation of Figure 1 on page 25 where the CP-CP sessions between the two network nodes use RTP. These sessions use the RTP function in both routers, and also use the Network Connection Layer (NCL), which provides a routing function and the connection point for the RTP layer.

Note that the diagram is a little simplistic because it should also show an additional RTP pipe between the two routers. This second RTP connection is used for route setup purposes only.

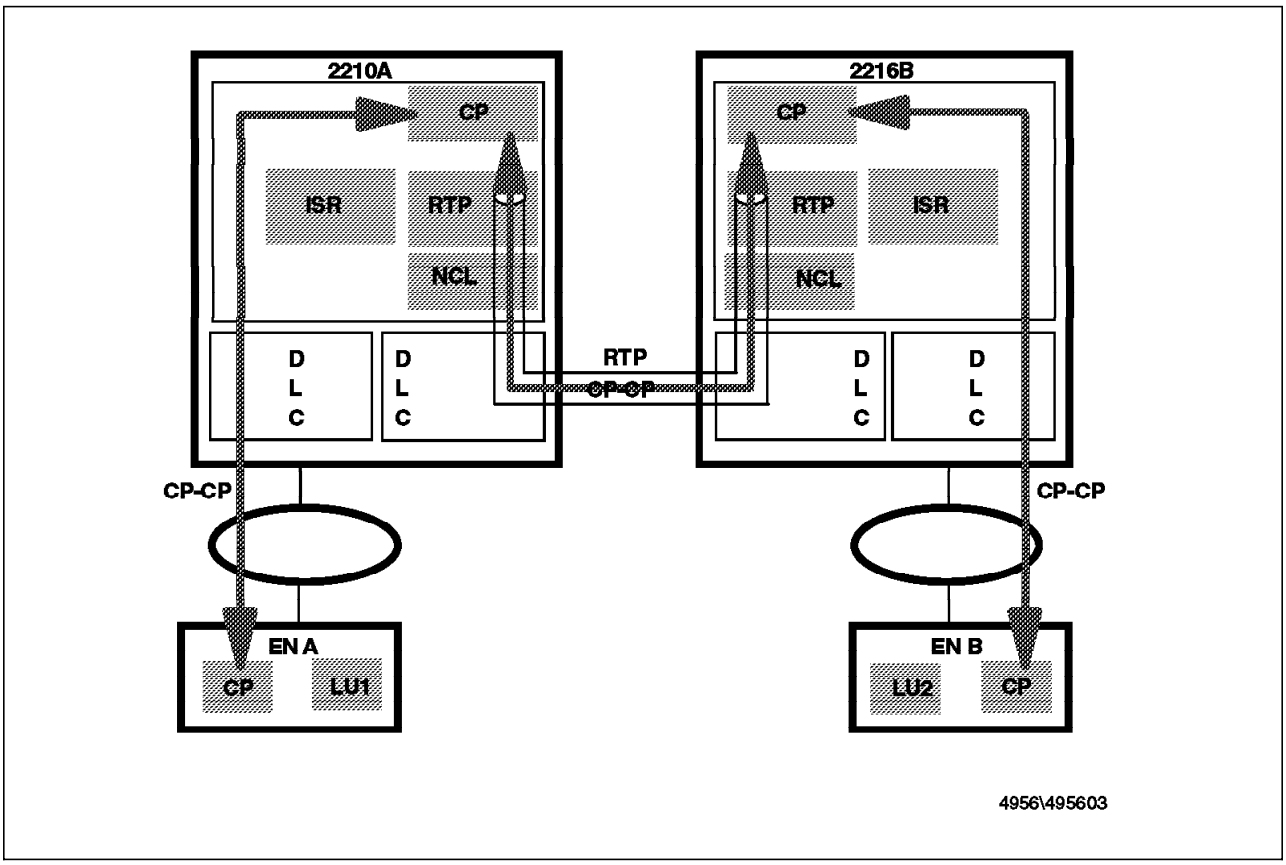


Figure 3. CP-CP over RTP (NN to NN)

Figure 4 on page 28 is a variation of Figure 2 on page 26 where both the CP-CP and LU-LU sessions use HPR between the two network nodes. The two end nodes are not HPR-capable in this example, so the routers have to convert from ISR to HPR. To do this, the sessions received via ISR are mapped onto RTP pipes.

Note that the diagram is a little simplistic, because in reality there would be at least three RTP pipes (including the one used for route setup) as the CP-CP sessions use a different COS from user sessions. Only sessions for one COS can share an RTP pipe.

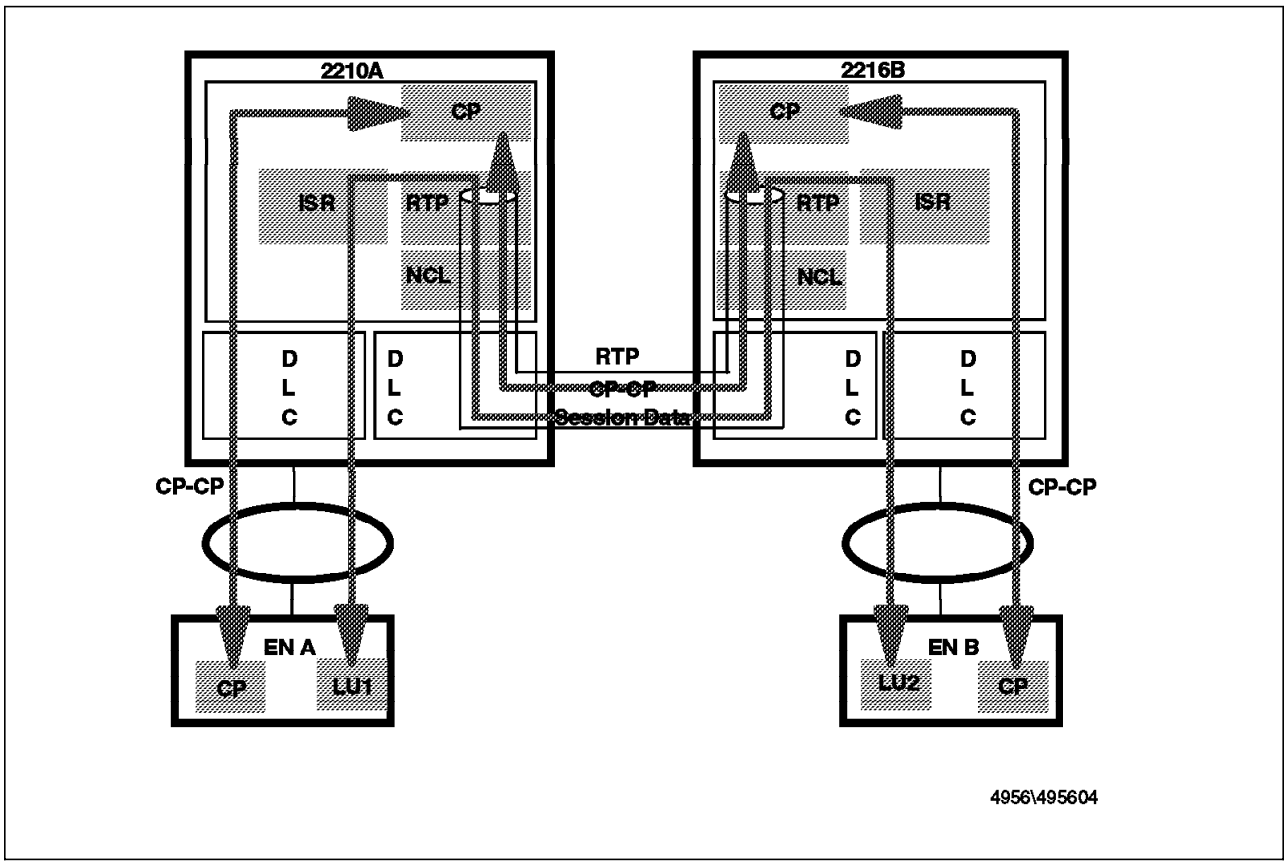


Figure 4. LU-LU Session Using HPR and ISR (HPR between NNs)

2.3.3 Extending HPR to One End Node

Figure 5 on page 29 is a variation of Figure 3 on page 27 where HPR is used by one of the end nodes as well as between the routers. Note that CP-CP sessions still exist between adjacent nodes.

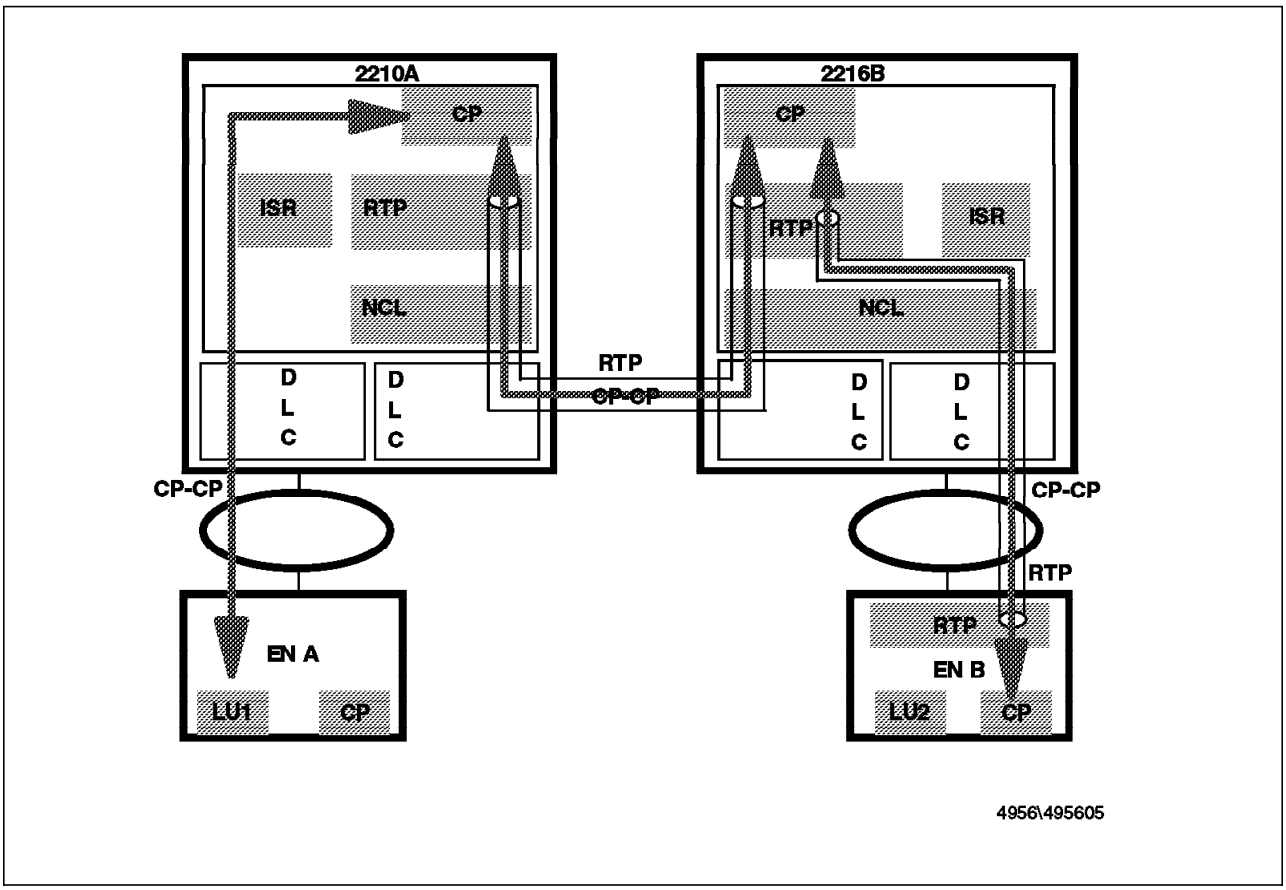


Figure 5. CP-CP over RTP (HPR to 1 x EN)

Figure 6 on page 30 is a variation of Figure 4 on page 28 where HPR (and CP-CP over RTP) is used by one of the end nodes, as well as between the routers. In this case, ANR routing is used in one of the routers for the LU-LU session between the end nodes. ANR routing is one of the main functions provided by the NCL. In the other router, the LU-LU session uses the ISR to HPR boundary function.

Again, the number of RTP pipes shown is a simplification of reality.

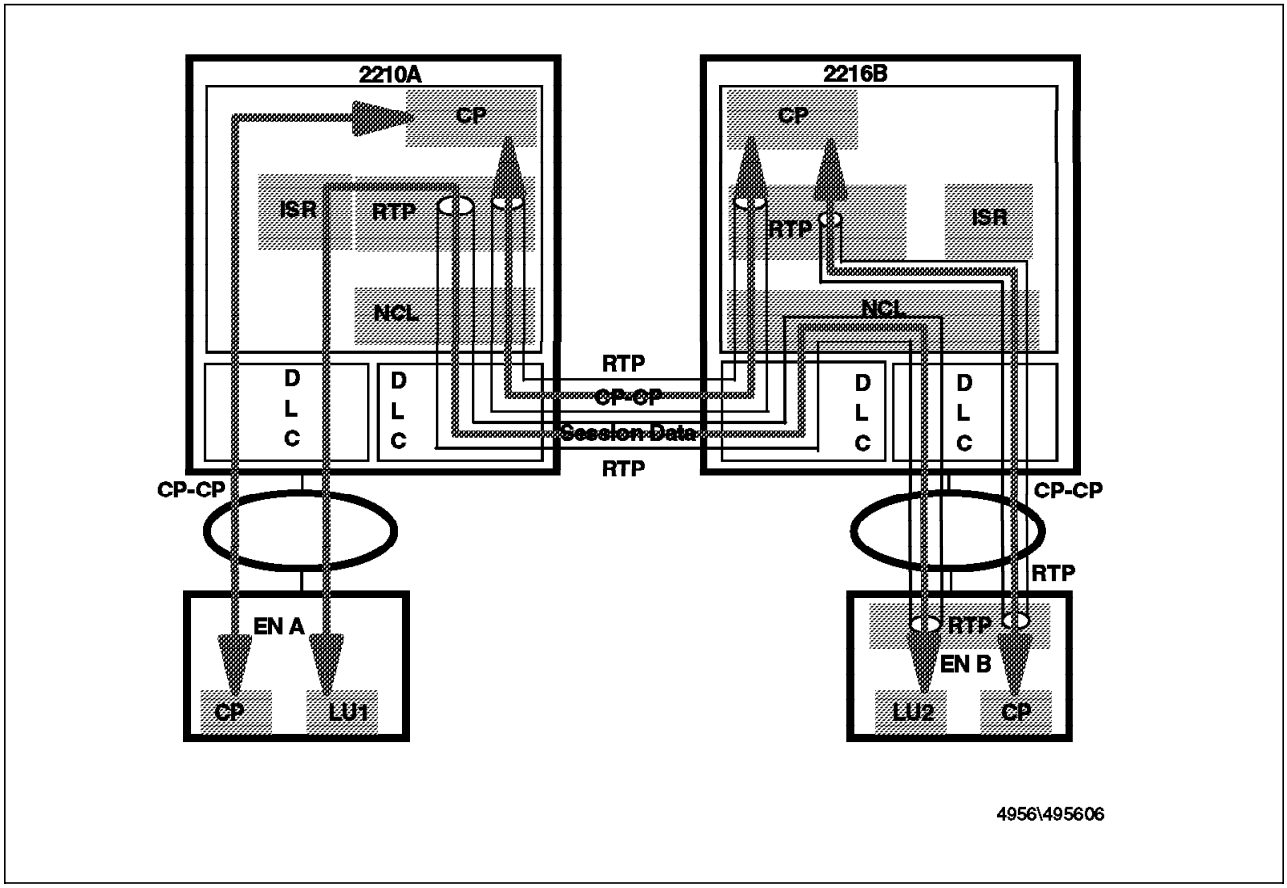


Figure 6. LU-LU Session Using ISR and HPR (HPR to 1 x EN)

2.3.4 Using HPR Throughout

Figure 7 on page 31 is an example where both end nodes implement HPR, including CP-CP over RTP. CP-CP sessions exist in the usual way between adjacent nodes.

Again, the number of RTP pipes is simplified.

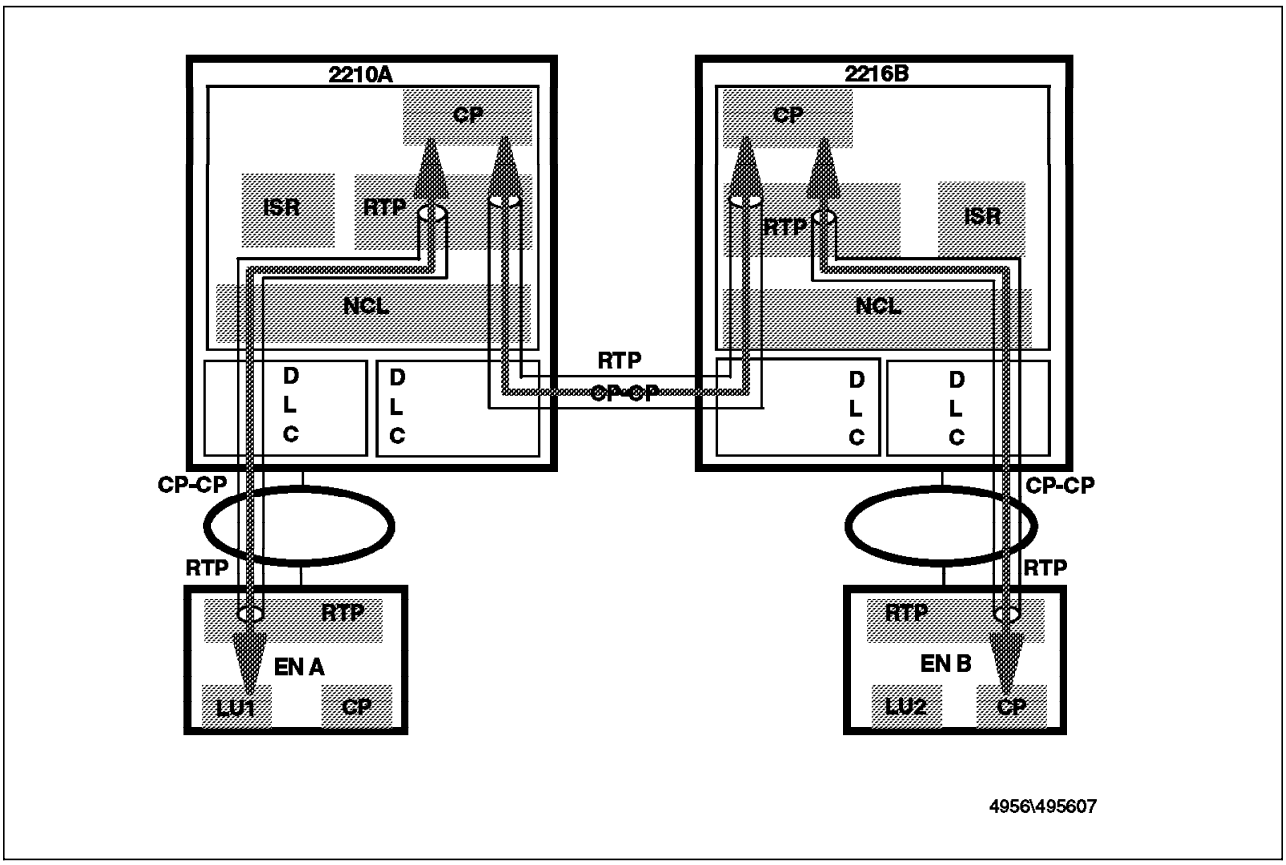


Figure 7. CP-CP over RTP (All Nodes HPR)

Figure 8 on page 32 shows an LU-LU session between the two end nodes. In this case, the LU-LU session uses ANR routing in both routers.

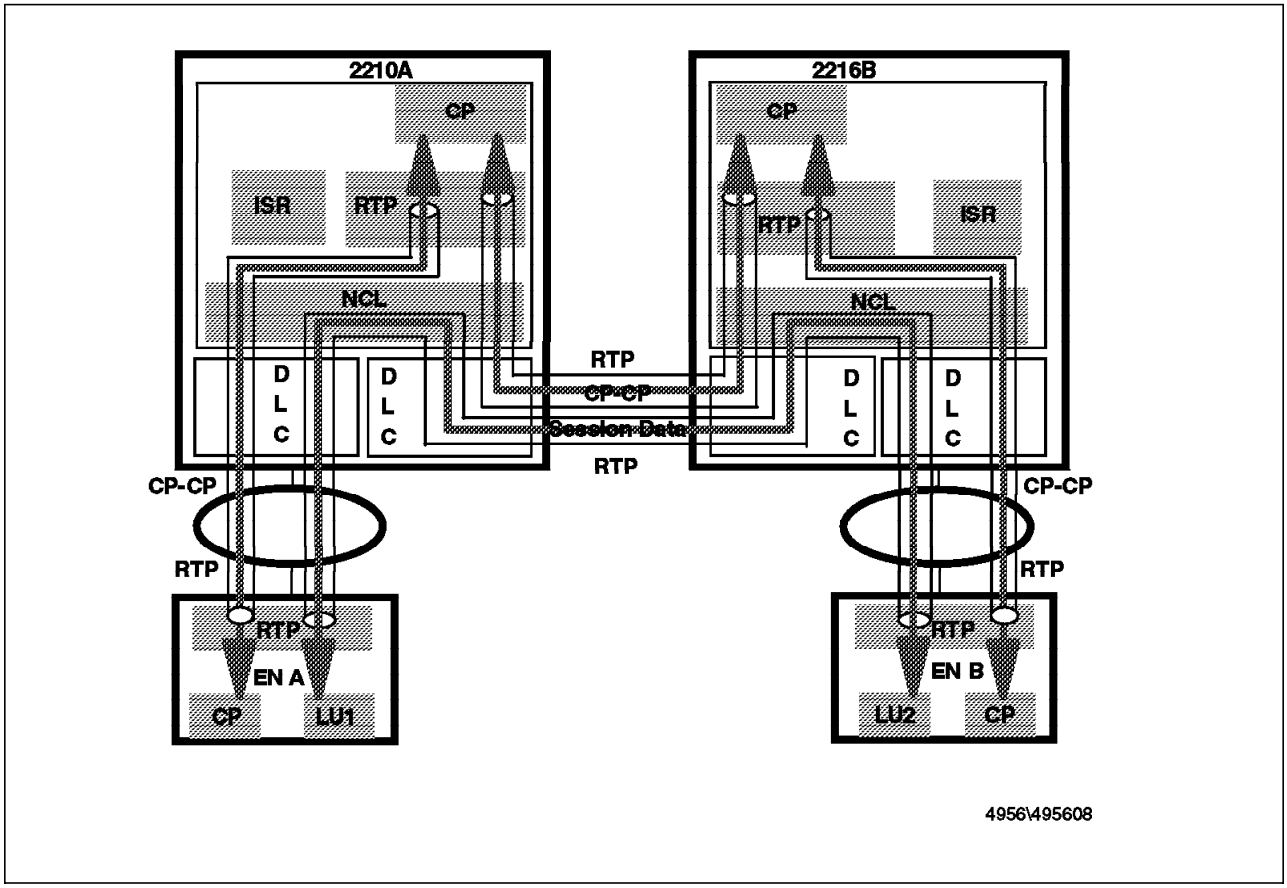


Figure 8. LU-LU Session Using HPR (All Nodes HPR)

2.3.5 Using APPN over DLSw

Figure 9 on page 33 shows an example where DLSw is used between the two network nodes. From the APPN perspective, this is just the same as in Figure 1 on page 25. The only difference is that the port that APPN uses to communicate between the routers is defined as the DLSw port rather than as a direct DLC connection.

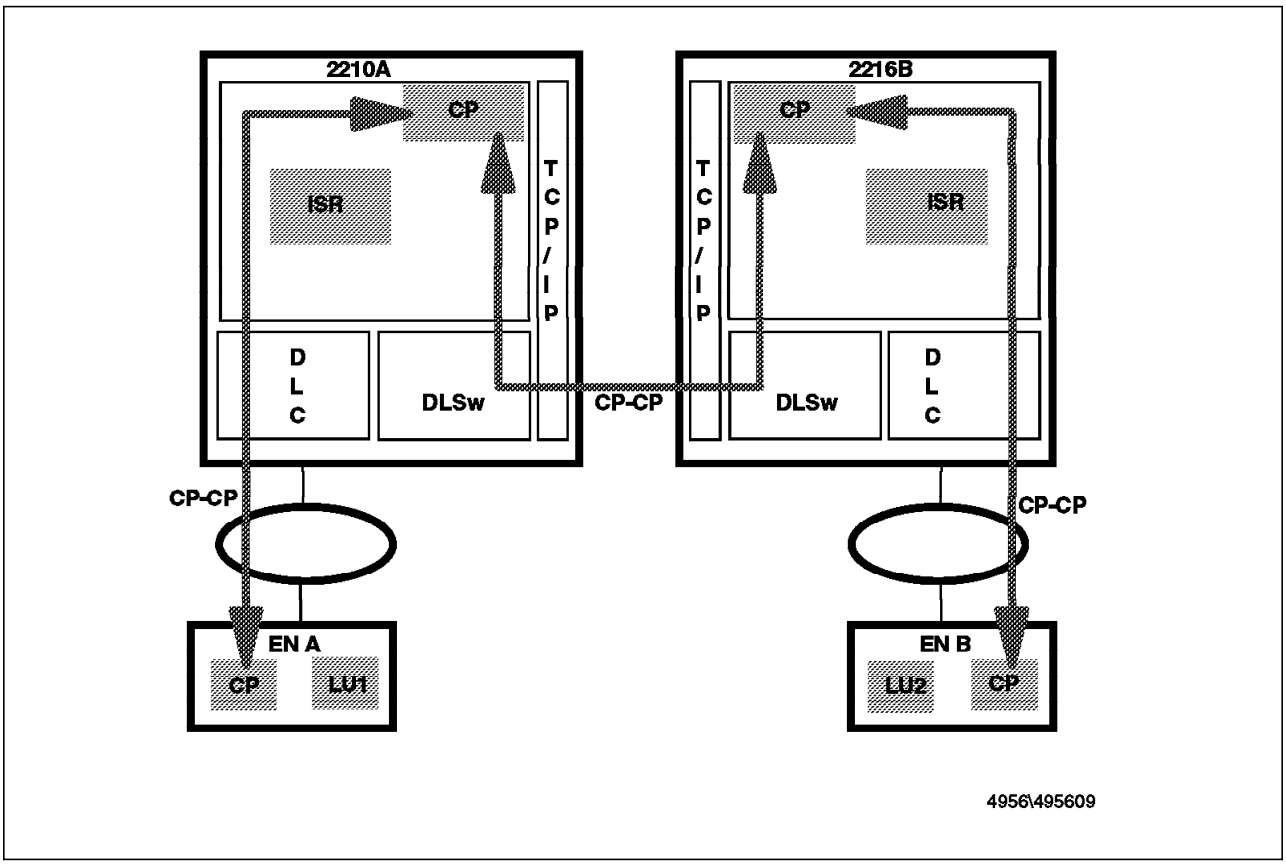


Figure 9. DLSw between NNs - CP-CP Sessions

Figure 10 on page 34 extends the DLSw example to show the flow for an LU-LU session between the two end nodes. From the APPN perspective, this is just the same as in Figure 2 on page 26, but the port that APPN uses to communicate between the routers is defined as the DLSw port rather than as a direct DLC connection. There is only one DLSw connection between the routers, and this is shared by all sessions.

Note that the end nodes in Figure 10 on page 34 can use HPR to communicate with the network nodes. In this case the flow for the LU-LU session would be almost the opposite of that shown in Figure 4 on page 28. In this case the routers would use the HPR to ISR conversion function to map the ISR session between the routers on to RTP pipes between each router and its end node.

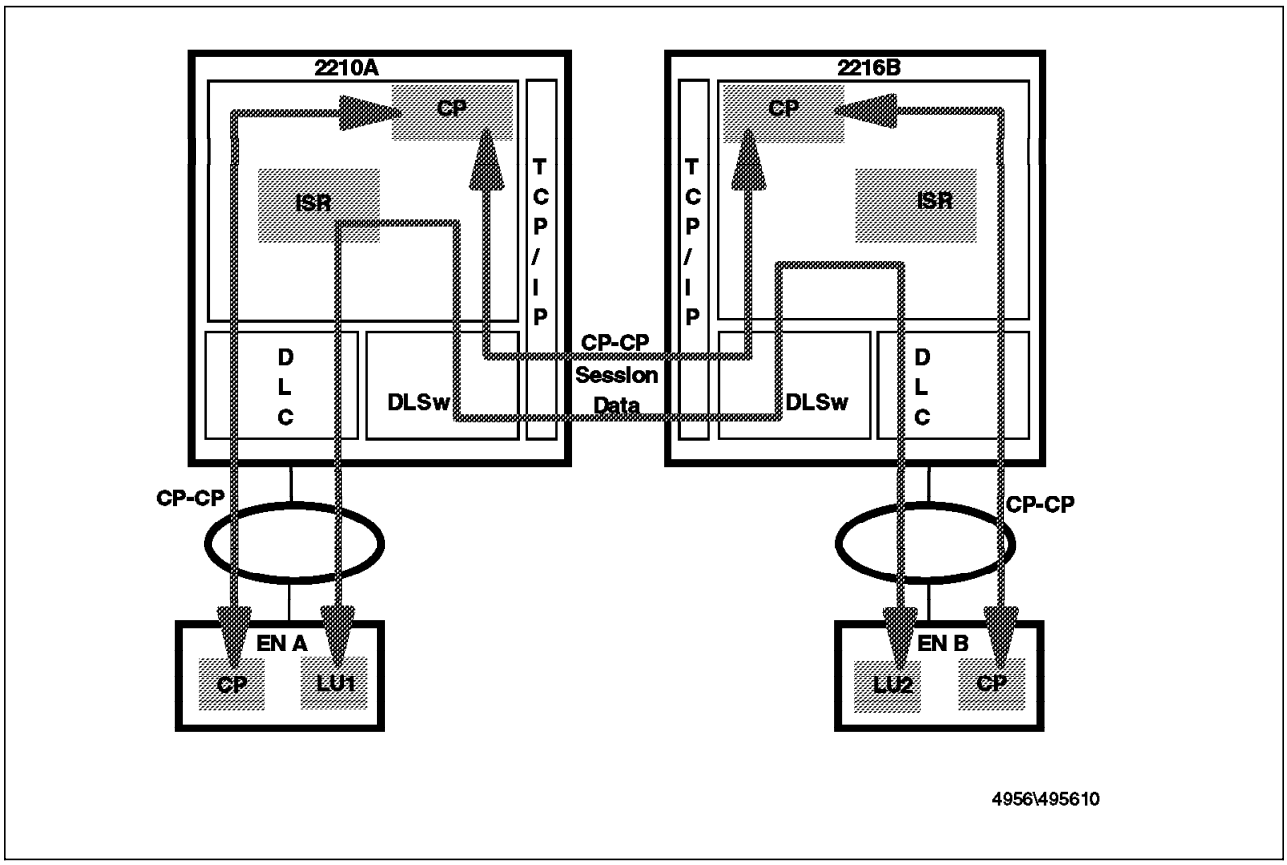


Figure 10. DLSw between NNs - LU-LU Session

Chapter 3. Basic APPN Configuration

This chapter discusses the basic steps required to configure APPN on the router. We look at the minimum configuration parameters for APPN, and then develop a scenario for ISR, followed by one for HPR.

We have also included a section on considerations when using APPN on a 2210 with only 8 MB of DRAM.

3.1 How to Start Configuring APPN

You normally configure APPN after having configured the hardware interfaces that you want to use and some of the other basic router functionality such as IP routing and SNMP. See *IBM 2210 Description and Configuration Scenarios - Volume 1* and *IBM 2216 Description and Configuration Scenarios - Volume 1* for more information on these activities. With these prerequisites in place, you can configure APPN in a similar way to the other supported routing protocols.

Just as these other protocols, APPN can be configured via the command line interface or via the Configuration Program. The examples in this book mainly use the command line interface because it is easier to represent the sequences and parameters involved in printed form. However, you may find the Configuration Program easier to use with its graphical interface, and its use from a central point makes configuration management much easier.

3.1.1 Invoking the Command Line Interface

From the base command line prompt, start APPN configuration by using the sequence shown in Figure 11.

```
*talk 6                                  1
Config>protocol appn                     2
APPN user configuration
APPN config>                             3
```

Figure 11. Starting APPN Configuration

Notes:

1. '*****' is the base command line prompt. `talk 6` is used to enter configuration mode for all aspects of configuration. The result is the `Config>` prompt.
2. This is used to enter APPN configuration mode.
3. This is the APPN configuration mode prompt. To leave this mode, type `exit` and return to base configuration mode.

3.1.1.1 APPN Configuration Command Summary

A summary of all the APPN configuration commands is shown in Table 3 on page 36. A limited number of these commands are used in this chapter, but the use of many of them is discussed and illustrated in the chapters that follow.

Note that all command and parameter names may be abbreviated to as few characters as makes the meaning unambiguous.

Table 3. APPN Configuration Command Summary

Command	Function
? (Help)	Lists all of the APPN configuration commands, or lists the options associated with specific commands.
Enable/Disable	Enables the following: • APPN • Dependent LU Requester • Port *port name*
Set	Sets the following: • Node • Traces • HPR • DLUR • Management • Tuning
Add	Adds or updates the following: • Ports • Link stations • LU names • Connection networks • Additional port to connection network • Mode names
Delete	Deletes the following: • Ports • Link stations • LU names • Connection networks • Additional port to connection network • Mode names
List	Lists the following from configuration memory: • All • Node • Traces • Management • HPR • DLUR • Ports • Link stations • LU names • Mode names • Connection networks
Activate_new_config	Reads the configuration into non-volatile configuration memory.
Exit	Exits the APPN Configuration process and returns to the `Config>` prompt.

When using the command line interface, default values are suggested when you are prompted for many of the parameters. Pressing the enter key results in the default value being used.

3.1.2 Using the Configuration Program

An alternative way of configuring APPN on the router is to use the Configuration Program. Figure 12 shows the APPN part of the navigation window. This gives a good summary view of the APPN functions that can be configured.

If you select one of the items in this menu, a window specific to that configuration task is displayed. Figure 16 on page 43 is an example of one of these detail windows. On each detail window, help is available for both the overall window and for each field.

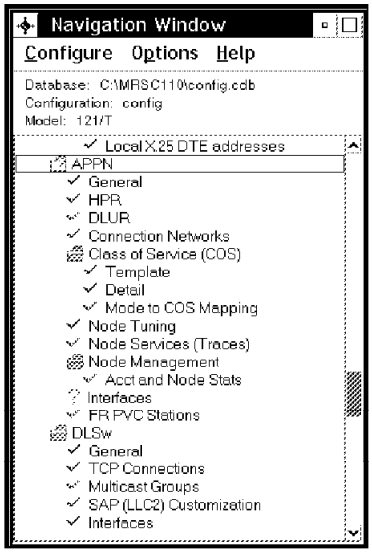


Figure 12. Navigation Window - APPN Items

3.2 Configuring the Router As an APPN Network Node

You can take various approaches to configuring the router as a basic APPN network node, depending on how you wish to initiate and constrain connections with other SNA nodes. We develop a basic configuration approach via three evolutionary stages:

- Minimum configuration

  The adjacent nodes are responsible for initiating connections to the router.
- Initiating connections to adjacent nodes

  The router is responsible for initiating some (or all) connections to adjacent nodes.
- Limiting connections to predefined nodes only

  All adjacent nodes are defined in the router and connections with undefined nodes are not allowed.

In practice, combinations of these approaches are likely to be used. We discuss how to configure the router using these three stages, and then use scenarios for APPN ISR and HPR to illustrate the actual commands and parameter values required.

This chapter discusses the configuration steps that enables APPN communication for independent LUs. Configuring the router to handle sessions

for dependent LUs in adjacent nodes is covered in 5.1, “Dependent LU Requester” on page 139.

Note: The APPN part of this book focuses on configuring APPN on the router. It assumes that the basic definition of the interfaces has already been done. See *IBM 2210 Description and Configuration Scenarios Volume I* or *IBM 2216 Description and Configuration Scenarios Volume I* for more details.

3.2.1 Minimum Configuration

This group of APPN configuration steps allows the network node to accept any request to establish a connection that it receives from another node.

If you choose this minimum configuration approach, adjacent nodes must initiate connections to the router network node. Because APPN nodes can initiate connections and CP-CP sessions with the router, these nodes do not need to be defined in the router′s configuration.

In general, when configuring APPN on the router, you can simplify the task considerably by allowing the router to accept connection requests from any node. Configuring the network node in this manner eliminates the need to define information about adjacent nodes, except in the following cases:

- You want the router network node to be able to initiate a connection and then CP-CP sessions with an adjacent APPN node.
- The adjacent node is a LEN end node and independent LUs it supports are initial targets of session requests from the APPN network. See 4.2.3, “Defining Independent LUs Located at LEN Nodes” on page 119 for more details.

In these cases, you must specify information about the adjacent nodes when enabling APPN routing on the specific port you use to connect to them. Follow the configuration steps described in 3.2.2, “Initiating Connections to Adjacent Nodes” on page 41.

Use the following steps for a minimum APPN configuration:

1. Enable the APPN network node and configure the following parameters:
   - Network ID.
   - Control point name.
   - Optionally, specify the XID ID number for subarea connection parameter.
   - Accept the default route additional resistance.
2. Optionally, if you want to use DLUR, we recommend that you enable it now, even if you allow most parameters to default at this stage. See 5.1, “Dependent LU Requester” on page 139 for how to do this.
3. Enable APPN routing on the router ports to be used by APPN with the Enable APPN on this port parameter.

   Since Service any node is enabled by default, the router accepts any request for a connection that it receives on this port.

Note: DLSw is one of the ports supported by APPN. DLSw as an APPN port would be useful, for example, if you have a partner router that is not APPN-capable (but DLSw-capable), or you have to go through one or more routers that are not APPN-capable.

If you are configuring APPN to use a DLSw port:

1. Enable bridging on the router.
2. Enable DLSw on the router.
3. Within APPN, define the single DLSw port and use the locally administered MAC address parameter to specify the MAC address to be used to access APPN from other DLSw-connected nodes.
4. Also define the underlying DLSw connectivity that is to be used by APPN.

See 6.2, “Configuring DLSw for APPN” on page 160 and Chapter 8, “Data Link Switching for SNA” on page 219 for more information on configuring DLSw.

Examples of the basic configuration steps are shown in Figure 13 on page 40 and Figure 14 on page 40. The information required for these is:

Network ID — The SNA network identifier (name) for the APPN subnetwork that contains the router. As the router does not provide APPN border node support, all adjacent network nodes must use the same network name unless the partner node provides border node support on the connection between the two nodes. Adjacent LEN or APPN end nodes can use the same or different network names.

Control point name — This is the name of the LU used by the router for control point functions. Follow the naming conventions appropriate to your network.

XID ID number for subarea — You may need to specify this value, but only if one of the adjacent nodes is a VTAM or NCP:

- In VTAM, you should normally identify connecting APPN nodes by using their CPNAME rather than the IDBLK/IDNUM combination. All these values are contained in the XID3s that flow at connection initiation time. However, it is still possible in VTAM to identify a connecting node by the IDBLK/IDNUM combination rather than CPNAME if you so wish.
- The value specified here corresponds to the IDNUM value in VTAM; the IDBLK value is fixed at 077 for both the 2210 and 2216.

Port name — A name to be used for the APPN port. This is visible and used at the network operations level, so consider using a naming convention that allows the association with the particular router and physical interface to be understood quickly.

In these basic examples, it is assumed that the router interfaces have already been configured. The full scenarios that are shown later include examples of this prerequisite interface configuration.

```
*talk 6
Config>protocol appn
APPN user configuration
APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? usibmra
Control point name (Max 8 characters) [  ]? ra2216a
Route addition resistance(0-255) [128]?                                  1
XID ID number for subarea connection (5 hex digits) [00000]?             2
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 13. Enabling APPN on the Router

Notes:

1. The use of a non-default value for this parameter is discussed in 4.4.2, “Changing the Node Resistance” on page 138.
2. Only modify the default if you are not using CPNAME to identify the connecting node in VTAM.

```
APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? t
Interface number(Default 0): [0]? 3                                      1
Port name (Max 8 characters) [TR000]? tkra3
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?                                       2
 High performance routing: (Y)es (N)o [Y]?                               3
 Maximum BTU size (768-2063) [2048]?                                     4
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 14. Enabling APPN on a Port - Accept Any Connection (2216 - Token-Ring)

Notes:

1. This relates the logical APPN port to the underlying interface. Type `list devices` at the CONFIG> prompt to see the number assigned to each interface.
2. This enables any adjacent node to connect to the router APPN function.
3. Note that HPR is enabled by default if supported by the port type.

4 There may be circumstances when you want to limit the maximum frame size for the port. 768 is the minimum size if HPR is to be used.

3.2.2 Initiating Connections to Adjacent Nodes

This stage builds on the minimum configuration, and adds the initiation of connections to adjacent APPN nodes. Normally, this should be done for adjacent network nodes, but it is probably easier to leave adjacent end nodes undefined. Instead, let the end nodes be responsible for initiating and maintaining the connection with their network node server.

With the addition of these configuration steps, this:

- Allows the network node to accept any request to establish a connection that it receives from another node.
- Enables the network node to initiate connections with other nodes that you specify, including LEN (and PU2.0) nodes.

In addition to the steps shown in 3.2.1, “Minimum Configuration” on page 38, define APPN link stations on the appropriate ports for the adjacent nodes to which this network node is to initiate a connection.

Notes:

1. Link stations do not have to be defined on every port, only those over which you want to initiate connections to adjacent nodes.
2. Because LEN nodes do not support CP-CP sessions, the definition of a connection to a LEN node may not in itself be sufficient (depending on the direction in which sessions are requested). See 4.2.3, “Defining Independent LUs Located at LEN Nodes” on page 119 for more details.

An example of the connection configuration process is shown in Figure 15 on page 42.

The additional information required includes:

Station name — This is the name for the link station that represents the connection to the adjacent node. This is also visible to network operators, so consider the use of a naming convention for this value. The name does not have to be unique across the APPN network.

Connection parameters — You need sufficient information to be able to define the connection to the adjacent node to be established. The information varies by port type, type of adjacent node, direction of connection establishment, and any extra validation considered necessary.

```
APPN config>add link
APPN Station
Port name for the link station [ ]? tkra3
Station name (Max 8 characters) [ ]? rak
 Activate link automatically (Y)es (N)o [Y]?
 MAC address of adjacent node [000000000000]? 400001240000
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node, 3 = PU 2.0 node [1]? 0                    1
 High performance routing: (Y)es (N)o [Y]?
 Edit Dependent LU Server: (Y)es (N)o [Y]?                   2
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?         3
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 15. Defining a Connection to an Adjacent Node (Token-Ring)

Notes:

1. The PU 2.0 option only appears if DLUR has been enabled at the node level.
2. The option to change the DLUS defaults for the individual connection only appears if DLUR has been enabled at the node level.
3. The adjacent CP name is required if:
   - The adjacent node type is set to LEN.
   - CP-CP sessions security is enabled.
   - The link is a limited resource link.

An example of configuring a link station using the Configuration Program is shown in Figure 16 on page 43. The hierarchical structure of the definitions is obvious from this particular example. Note that two stations have already been configured on the selected port.

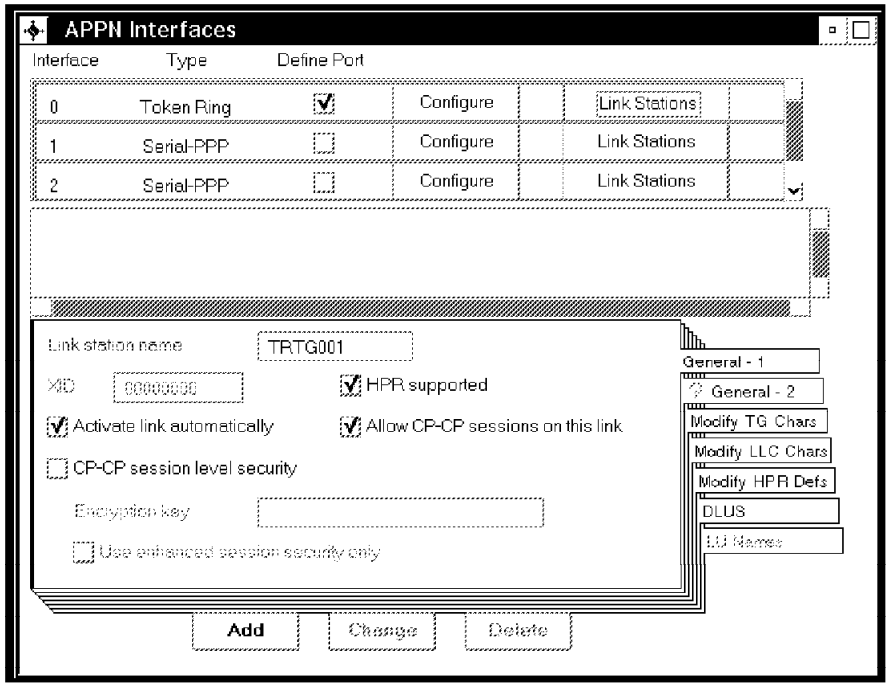


Figure 16. Using the Configuration Program to Define a Station

3.2.3 Limiting Connections to Defined Nodes Only

This variation builds on the previous two stages, but limits connections to other nodes to only those predefined. If desired, this approach can be used on individual ports rather than on all ports.

This approach allows the network node to accept connection requests only from nodes that you specify. It also enables the network node to initiate connections with other nodes that you specify, including LEN (and PU2.0) nodes.

This configuration provides a higher level of security because you explicitly define which nodes may communicate with this router network node. A connection request from an adjacent node will be accepted only if its fully qualified CP name (in the case of LEN and PU2.0 nodes, the IDBLK/IDNUM value) has been configured on the router.

Optionally, you may provide a higher level of security for APPN connections by configuring session-level security for the CP-CP sessions on a connection. See 4.2.5, “Using CP-CP Session Security” on page 123 for more information on this function.

In combination with the steps shown in 3.2.1, “Minimum Configuration” on page 38 and 3.2.2, “Initiating Connections to Adjacent Nodes” on page 41, use the following steps to limit connections to those predefined:

1. Select the ports on which you want to restrict connections to defined adjacent nodes only, and for these ports:
   - Set Enable APPN on this port.
   - Disable the Service any node option.
2. Define APPN link stations on the selected ports for any adjacent nodes:

- That may initiate a connection to this network node.
- With which you require this router to initiate a connection.

To do this, specify the following link station parameters:

- Fully qualified CP name (or IDBLK/IDNUM value if the node does not have a CP) of adjacent node (required).
- Any required addressing parameters for the adjacent node (port type dependent).
- Initially, accept all other defaults. See Chapter 4, "More Advanced APPN Configuration Options" on page 117 for details on when to use other than the defaults.

Examples of these two steps are shown in Figure 17 and Figure 18 on page 45.

```
APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? t
Interface number(Default 0): [0]? 4
Port name (Max 8 characters) [TR000]? tkra4
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]? N                                    1
 High performance routing: (Y)es (N)o [Y]?
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 17. Enabling APPN on a Port - Defined Connections Only (2216 - Token-Ring)

Note:

1 This stops any adjacent node connecting to the router APPN function unless it is represented by a defined station.

```
APPN config>add link
APPN Station
Port name for the link station [ ]? tkra3
Station name (Max 8 characters) [ ]? ws05600
 Activate link automatically (Y)es (N)o [Y]? n
 MAC address of adjacent node [000000000000]? 400052005600
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node, 3 = PU 2.0 node [1]?                          1
 High performance routing: (Y)es (N)o [Y]?
 Edit Dependent LU Server: (Y)es (N)o [Y]?                       2
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]? y
  Fully-qualified CP name of adjacent node (netID.CPname) []?  usibmra.rak
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>add link
```

Figure 18. Defining a Connection from an Adjacent Node (Token-Ring)

Notes:

1. The PU 2.0 option only appears if DLUR has been enabled at the node level.
2. The option to change the DLUS defaults for the individual connection only appears if DLUR has been enabled at the node level.

3.2.4 Other Configuration Options

There are a significant number of other options that may need to be configured before your router APPN configuration is complete. These include:

- Modifying High-Performance Routing parameters
- Configuring dependent LU requester
- Defining connection networks
- Defining new COS names or mode name mappings
- Tuning the performance of this node
- Collecting statistics for this network
- Performing node service trace diagnostics

These are discussed in more detail in Chapter 4, “More Advanced APPN Configuration Options” on page 117 and 5.1, “Dependent LU Requester” on page 139.

3.3 Configuring APPN (and TCP/IP) for an 8-MB Router

2210 Only

This section applies only to the IBM 2210.

To avoid exceeding the available Dynamic Random Access Memory (DRAM), feature code 5004 is used to support both APPN and TCP/IP protocols in an 8-MB

2210. The primary purpose of this feature code is to provide APPN/HPR/DLUR support in small branch office situations with up to eight LAN-attached APPN nodes at the lowest possible cost.

The 5004 feature code includes special provisions for minimizing DRAM requirements in 8-MB routers. This feature can also be used in routers with more than 8-MB of DRAM. The full set of APPN/HPR capabilities is included. Use of TCP/IP is limited to support functions, such as remote loading, dumping, and SNMP functions.

Note: ISDN and DLSw connections are not supported because they require more memory than is available.

The 5004 feature supports the following configuration in an 8-MB router:

- LAN-attached
  - Up to eight APPN T2.1 end nodes with an average of five sessions per end node (40 LU-LU sessions). LEN nodes and/or PU 2.0 nodes can be substituted for T2.1 nodes.
  - Up to four IP hosts may also be attached.
- WAN-attached
  - Two ports with an aggregate maximum of eight concurrent connections (that is, 8 APPN TGs) to, at most, four adjacent APPN nodes (NN, EN, PU 2.0 or LEN).
  - Up to four IP hosts may also be attached per port.

    Note: In large customer networks, 8-MB 2210s must depend on the services of an APPN border node to limit the amount of memory they need for storing network topology information. A 2210 cannot be a border node.

Use the following configuration settings for a load image that will function in 8-MB of DRAM.

1. Issue the `set global` command at the `Config>` prompt to limit the number of global buffers to a maximum of 50.
2. Type the `set tuning` command at the `APPN config>` prompt and set the following parameter values:
   - Set maximum shared memory to 1792. This action reduces the shared memory requirement to 1.75 megabytes.
   - Set percent buffer memory to 17.
   - Set maximum cached directory entries to 200.

See 4.2.6, “Adjusting the APPN Memory for Network Size” on page 124 for more information on these parameters.

3.4 A Sample Intermediate Session Routing Configuration Scenario

While we prefer to configure DLCs as APPN/HPR links, we first cover an ISR configuration example for situations where ISR may be the most appropriate protocol. Furthermore, there may be situations where ISR is the only choice. For example, in the initial releases of MRS and MAS, the following DLCs are supported only for ISR:

- SDLC

- Data Link Switching (DLSw)
- X.25 (QLLC)
- ESCON LSA

2216 Only

The 2210 cannot have an ESCON interface.

ESCON on the 2216 requires MAS V1R1.1. Note that ISR is not supported over ESCON MPC+.

Note that HPR is enabled by default for the port types that support it.

3.4.1 ISR Scenario Description

This scenario uses a three-router network to show an ISR configuration with the following DLCs:

- DLSw over X.25
- SDLC with a router in a secondary link role
- SDLC with a router in a primary link role
- SDLC with two routers on a negotiable link

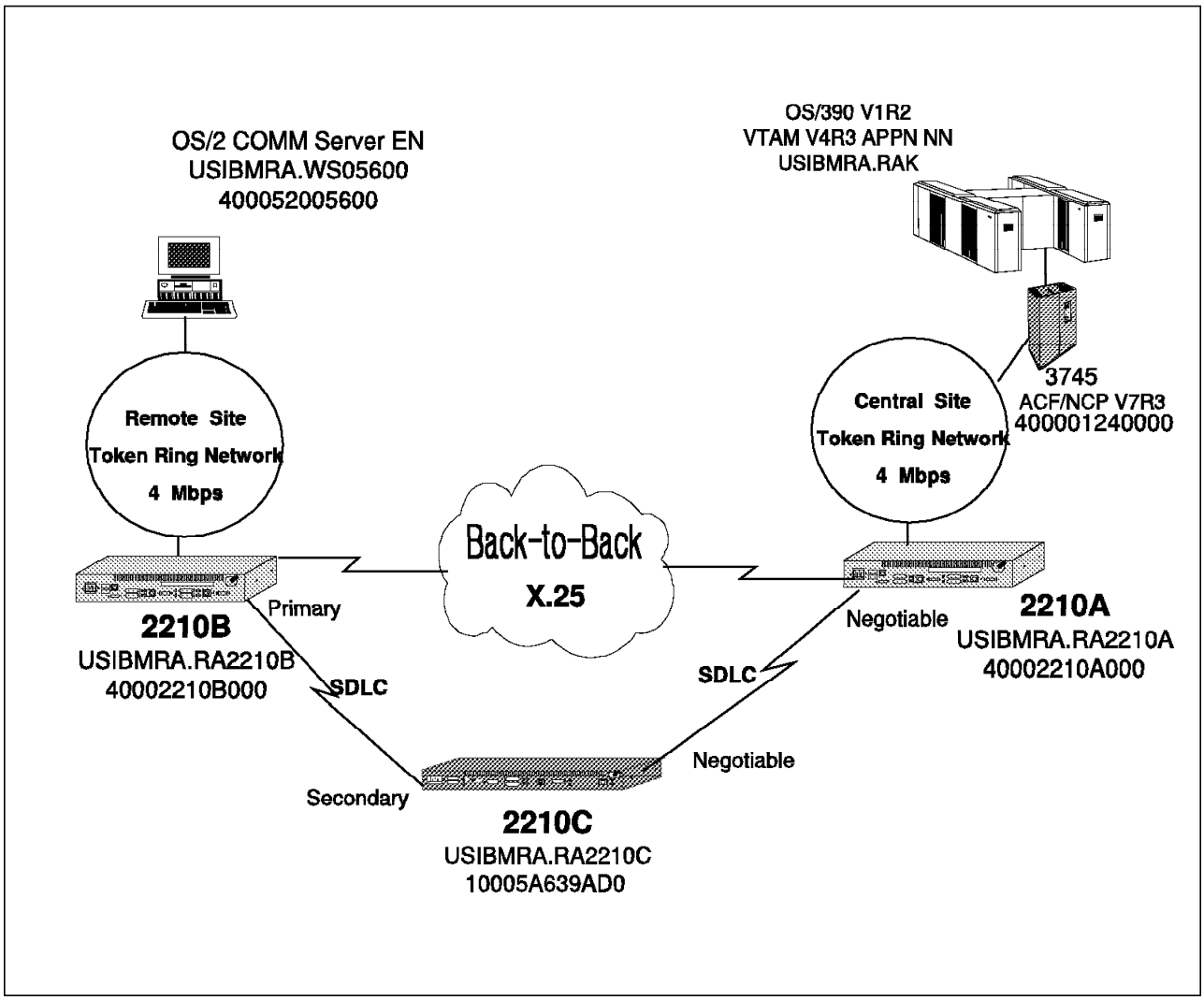


Figure 19. Logical Diagram of the ISR Scenario. This diagram shows ISR using X.25/DLSw and SDLC links.

The diagram of the scenario is shown in Figure 19. The key components in this setup are:

- Router 2210A is a Model 14T with 16 MB of DRAM. It has an X.25 port on interface 4 running DLSw. Interface 3 has SDLC on a negotiable link.
- Router 2210B is a Model 24T with 16 MB of DRAM. It has an X.25 port on interface 4 running DLSw and SDLC primary on interface 3.
- Router 2210C is a Model 12T with 8 MB of DRAM. Interface 1 is secondary SDLC while interface 2 is negotiable SDLC.
- The X.25 and SDLC links are back-to-back using RS-232 DTE and DCE cables.
- To test the scenario, we have an end node on a Communications Server/2 client on the remote token-ring LAN and a network node on a VTAM host.

3.4.2 Configuration Steps for 2210A

These steps show the configuration from the very beginning. The general steps in this configuration are:

1. Qconfig for the basic parameters in Figure 20 on page 50.
   - Interfaces 1 and 2 have not been used.
   - We have taken the defaults for the booting and service port parameters.
   - The router has not been restarted after Qconfig but after we have configured the other parameters.
2. Interface configuration of SDLC and X.25 in Figure 21 on page 53.
   - Interface 4 is configured for back-to-back X.25.
   - Interface 3 is configured for SDLC.
3. IP and OSPF configuration in Figure 22 on page 55. TCP/IP configuration is required because we are using DLSw.
4. Bridging and DLSw configuration in Figure 23 on page 57.
5. APPN port configuration in Figure 24 on page 59.
6. APPN link configuration in Figure 25 on page 60.
7. APPN node configuration in Figure 26 on page 61.

```
Config>qconfig

Router Quick Configuration for the following:
o   Interfaces
o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing/Transparent Bridge (SR/TB)
        Source Routing Transparent Bridge (SRT)
o   Protocols
        IP (including OSPF, RIP and SNMP)
o   Booting
Event Logging will be enabled for all configured subsystems
with logging level 'Standard'
Note:  Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration

*******************************************************
Interface Configuration
*******************************************************

Type 'Yes' to Configure Interfaces
Type 'No' to skip Interface Configuration
Type 'Quit' to exit Quick Config

Configure Interfaces? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Interface Configuration

Intf 0 is Token Ring
Speed in Mb/sec (4, 16): [4]
Connector (STP, UTP): [STP]

Intf 1 is WAN PPP
Encapsulation for WAN 1  (PPP, Frame Relay): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 2 is WAN PPP
Encapsulation for WAN 2  (PPP, Frame Relay): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 3 is WAN PPP
Encapsulation for WAN 3  (PPP, Frame Relay): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 4 is WAN PPP
Encapsulation for WAN 4  (PPP, Frame Relay): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]
```

Figure 20 (Part 1 of 3). Quick Configuration Steps for Router A

```
This is all configured device information:
Intf 0 is Token Ring, Speed 4 Mb/sec, Connector STP
Intf 1 is WAN 1 with PPP Encapsulation, RS-232 DTE cable
Intf 2 is WAN 2 with PPP Encapsulation, RS-232 DTE cable
Intf 3 is WAN 3 with PPP Encapsulation, RS-232 DTE cable
Intf 4 is WAN 4 with PPP Encapsulation, RS-232 DTE cable

Save this configuration? (Yes, No): [Yes]
Device configuration saved

************************************************************
Bridging Configuration
************************************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes] n

************************************************************
Protocol Configuration
************************************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config
Configure Protocols? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Protocol Configuration

Configure IP? (Yes, No): [Yes]
Type 'r' any time at this level to restart IP Configuration

Configuring Per-Interface IP Information
Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 9.24.104.93
Address Mask: [255.0.0.0] 255.255.255.0

Configuring Interface 1 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] n

Configuring Interface 2 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] n

Configuring Interface 3 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] n
```

Figure 20 (Part 2 of 3). Quick Configuration Steps for Router A

```
Configuring Interface 4 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 203.203.203.2
Address Mask: [255.255.255.0]

Per-Interface IP Configuration complete
Configuring IP Routing Information
Enable Dynamic Routing? (Yes, No): [Yes]
Enable OSPF? (Yes, No): [Yes]

OSPF Enabled with Max routes = 1000 and Max routers = 50
Routing Configuration Complete
Configuring SNMP Information
SNMP will be configured with the following parameters:
     Community: public
     Access:    read_trap
SNMP Configuration Complete

This is the information you have entered:
     Interface #     IP Address         Address Mask   1
          0          9.24.104.93        255.255.255.0
          4          203.203.203.2      255.255.255.0
OSPF is configured, and RIP is configured only for 'sending'.
SNMP has been configured with the following parameters:
     Community: public
     Access:    read_trap
Save this configuration? (Yes, No): [Yes]
IP configuration saved

*********************************************************
Booting Configuration
*********************************************************

Type 'Yes' to Configure Booting
Type 'No' to skip Booting Configuration
Type 'Quit' to exit Quick Config

Configure Booting? (Yes, No, Quit): [Yes] n

*********************************************************
Service Port Configuration
*********************************************************

Type 'Yes' to Configure Service Ports
Type 'No' to skip Service Ports Configuration
Type 'Quit' to exit Quick Config

Configure service ports? (Yes, No, Quit): [Yes] n
Quick Config Done
Restart the router for this configuration to take effect.

Restart the router? (Yes, No): [Yes] n
Type RESTART at the '*' prompt for the configuration to take effect.
```

Figure 20 (Part 3 of 3). Quick Configuration Steps for Router A

```
Config>set data x25
Interface Number [0]? 4
Config>net 4   2
X.25 User Configuration
X.25 Config>nat dis accept
X.25 Config>nat dis request
X.25 Config>nat dis flow
X.25 Config>nat dis throu
X.25 Config>set pvc lo 1
X.25 Config>set pvc high 9
X.25 Config>set add
address []? 22101111
X.25 Config>set svc low-t 0
X.25 Config>set svc high-t 0
X.25 Config>nat set stand v1988

X.25 Config>add pvc   3
Protocol [IP]?
Packet Channel [1]?
Destination X.25 Address []? 22102222
Window Size [2]?
Packet Size [128]?

X.25 Config>add add   3
Protocol [IP]?
IP Address [0.0.0.0]? 203.203.203.1
Enc Priority 1 []? none
Enc Priority 2 []? none
X.25 Address []? 22102222

X.25 Config>add protocol   3
Protocol [IP]?
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
Circuit Idle Time [30]?
Max VCs [4]?
X.25 Config>li all

X.25 Configuration Summary
Node Address:       22101111
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:               0        Clocking:  External
MTU:              2048        Cable:     RS-232 DTE
Lower DTR:   Disabled
Default Window:     2        SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC             low: 1    high: 9
Inbound         low: 0    high: 0
Two-Way         low: 0    high: 0
Outbound        low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400
```

Figure 21 (Part 1 of 2). Interface Configuration for Router A

```
X.25 National Personality Configuration
Follow CCITT: on        OSI 1984:     on        OSI 1988:       off
Request Reverse Charges:  off   Accept Reverse Charges:     off
Frame Extended seq mode:  off   Packet Extended seq mode:   off
Incoming Calls Barred:    off   Outgoing Calls Barred:      off
Throughput Negotiation:   off   Flow Control Negotiation:   off
Suppress Calling Addresses: off
DDN Address Translation:  off
Call Request Timer:     20 decaseconds
Clear Request Timer:    18 decaseconds (1 retries)
Reset Request Timer:    18 decaseconds (1 retries)
Restart Request Timer:  18 decaseconds (1 retries)
Min Recall Timer:       10 seconds
Min Connect Timer:      90 seconds
Collision Timer:        10 seconds
T1 Timer:  4.00 seconds     N2 timeouts: 20
T2 Timer:  0.00 seconds     DP Timer:    500 milliseconds
Standard Version:     1988      Network Type: CCITT
Disconnect Procedure: passive   4
Window Size     Frame:   7      Packet:  2
Packet Size     Default: 128    Maximum: 256

X.25 protocol configuration
Prot         Window      Packet-size        Idle     Max     Station
Number       Size      Default Maximum      Time     VCs      Type
0  -> IP      2          128     256         30       4        -

X.25 PVC configuration
Prtcl        X.25_address     Active Enc  Window    Pkt_len   Pkt_chan
0   (IP)     22102222           NONE      2         128       1

X.25 address translation configuration
IF #  Prot #       Active Enc  Protocol       -> X.25 address
4     0  (IP)         NONE     203.203.203.1  -> 22102222
X.25 Config>ex

Config>set data sdlc
Interface Number [0]? 3
Config>net 3   5
SDLC user configuration
Creating a default configuration for this link
SDLC 3 Config>set link role negotiable   5
SDLC 3 Config>add station   5
Enter station address (in hex) [C1]? d2
Enter station name [SDLC_D2]?
Include station in group poll list ([Yes] or No):
Enter max packet size [2048]?
Enter receive window [7]?
Enter transmit window [7]?
SDLC 3 Config>exit
```

Figure 21 (Part 2 of 2). Interface Configuration for Router A

```
Config>p ip
Internet protocol user configuration
IP config>set internal  6
Internal IP address [10.10.3.33]? 10.24.104.93
IP config>li all

Interface addresses
IP addresses for each interface:
   intf  0   9.24.104.93      255.255.255.0    Local wire broadcast, fill 1
   intf  1                                     IP disabled on this interface
   intf  2                                     IP disabled on this interface
   intf  3                                     IP disabled on this interface
   intf  4   203.203.203.2    255.255.255.0    Local wire broadcast, fill 1
Internal IP address: 10.24.104.93

Routing
Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: enabled
BGP: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
     intf  0   9.24.104.93      Send net, subnet, static and default routes
                                Received RIP packets are ignored.
     intf  1                    IP & RIP are disabled on this interface
     intf  2                    IP & RIP are disabled on this interface
     intf  3                    IP & RIP are disabled on this interface
     intf  4   203.203.203.2    RIP disabled for this interface
Accept RIP updates always for:
[NONE]
IP config>ex

Config>p ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>add neighbor  7
Interface IP address [0.0.0.0]? 203.203.203.2
IP Address of Neighbor [0.0.0.0]? 203.203.203.1
Can that router become Designated Router on this net [Yes]? n
Config>set non-broadcast 203.203.203.1  7
Poll Interval [120]?
```

Figure 22 (Part 1 of 2). TCP/IP and OSPF Configuration for Router A

```
OSPF Config>li all
                        --Global configuration--
                OSPF Protocol:          Enabled
                # AS ext. routes:       1000
                Estimated # routers:    50
                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
9.24.104.93       0.0.0.0             1      5       1     1     10     40
203.203.203.2     0.0.0.0             1      5       1     1     10     40

                        --NBMA configuration--
                Interface Addr    Poll Interval
                203.203.203.1     120

                        --Neighbor configuration--
                Neighbor Addr     Interface Address   DR eligible?
                203.203.203.1     203.203.203.2       no

OSPF Config>ex
```

Figure 22 (Part 2 of 2). TCP/IP and OSPF Configuration for Router A

```
Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable brid  8
ASRT config>dis trans  8
Port Number [1]? 1
ASRT config>enable source-rout
Port Number [1]?
Segment Number for the port in hex(1 - FFF) [  1]? 584  8
Bridge number in hex (0 - 9, A - F) [0]? e
ASRT config>enable dls  8
ASRT config>list bridge
               Source Routing Transparent Bridge Configuration
               ===============================================
Bridge:                 Enabled                 Bridge Behavior: SRB
                  +---------------------------+
------------------] SOURCE ROUTING INFORMATION ]------------------------------
                  +---------------------------+
Bridge Number:          0E                      Segments:          1
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1 N SRB:                Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
                  +-------------------+
------------------] SR-TB INFORMATION ]-----------------------------------------
                  +-------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
                  +-----------------------------------+
------------------] SPANNING TREE PROTOCOL INFORMATION ]----------------------
                  +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IBM-SRB proprietary
                  +-------------------------+
------------------] TRANSLATION INFORMATION ]---------------------------------
                  +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                  +-------------------+
------------------] PORT INFORMATION ]-----------------------------------------
                  +-------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled
2210A ASRT config>exit

Config>p dls
DLSw protocol user configuration
DLSw config>enable dls  9
DLSw config>set srb fab  9
```

Figure 23 (Part 1 of 2). DLSw Configuration for Router A

```
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 10.8.8.1   10
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]? e
Neighbor Priority (H/M/L) [M]?
DLSw config>open-sap   10
Interface # [0]?
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 0

DLSw config>list dls
DLSw is                              ENABLED
LLC2 send Disconnect is              ENABLED
Dynamic Neighbors is                 ENABLED
SRB Segment number                   FAB
MAC <-> IP mapping cache size        128
Max DLSw sessions                    1000
DLSw global memory allotment         141312
LLC per-session memory allotment     8192
SDLC per-session memory allotment    4096
NetBIOS UI-frame memory allotment    40960
Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor Priority              MEDIUM
DLSw config>ex
```

Figure 23 (Part 2 of 2). DLSw Configuration for Router A

```
Config>p appn
APPN user configuration
APPN config>add port  11
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? t
Interface number(Default 0): [0]?
Port name (Max 8 characters) [TR000]? tkra0
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add port  12
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? d
Port name (Max 8 characters) [DLS254]? dlsa4
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Locally administered MAC address (hex) [000000000000]? 40002210addd  12
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add port  13
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? s
Interface number(Default 0): [0]? 3
Port name (Max 8 characters) [SDLC003]? sdlca3
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 24. APPN Port Configuration for Router A

```
APPN config>add link   14
APPN Station
Port name for the link station [ ]? tkra0
Station name (Max 8 characters) [ ]? rak
 Activate link automatically (Y)es (N)o [Y]?
 MAC address of adjacent node [000000000000]? 400001240000
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add link   15
APPN Station
Port name for the link station [ ]? dlsa4
Station name (Max 8 characters) [ ]? r2210bd
 Activate link automatically (Y)es (N)o [Y]?
 MAC address of adjacent node [000000000000]? 40002210bddd
 SAP address of adjacent node(04-EC) [4]?
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add link   16
APPN Station
Port name for the link station [ ]? sdlca3
Station name (Max 8 characters) [ ]? r2210cs
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C1]? d1
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 25. APPN Link Configuration for Router A

```
APPN config>set node  17
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? usibmra
Control point name (Max 8 characters) [  ]? ra2210a
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]? 2210a  18
Write this record? [Y]?
The record has been written.
APPN config>list all
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210A
 XID: 2210A
 APPN ENABLED: YES
 MAX SHARED MEMORY: 4096
 MAX CACHED: 4000
DLUR:
 DLUR ENABLED: NO
 PRIMARY DLUS NAME:
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 --------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 ---------------------------------------------------
     0      TKRA0   IBMTRNET    YES      YES      YES
   254      DLSA4       DLS     NO      YES      YES
     3     SDLCA3      SDLC     NO      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
      RAK    TKRA0    400001240000       YES     YES       0
  R2210BD    DLSA4    40002210BDDD        NO     YES       0
  R2210CS   SDLCA3              D1        NO     YES       0
LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------
APPN config>exit
*restart
```

Figure 26. APPN Node Configuration for Router A

Notes:

1 Configure the IP addresses for the interfaces used. Address 9.24.104.93 is the token-ring address while 203.203.203.2 is the address of the X.25 interface.

2 This is the X.25 interface configuration for a back-to-back connection using RS-232 DTE and DCE cables.

3 Configure the PVC address, and the protocol for TCP/IP over the X.25 link.

4 For back-to-back X.25 links one 2210 should be configured for a passive disconnect procedure while the other 2210 should have active disconnect procedure.

5 Configure the SDLC port for a negotiable SDLC link.

6 Set the router's internal IP address for DLSw.

7 Add the OSPF neighbor on the non-broadcast X.25 link.

8 Configure the ASRT protocol for DLSw. Enable the bridge and DLSw.

9 Configure the DLSw protocol. Enable DLSw and set the virtual ring number to fab.

10 Add the DLSw neighbor address and open SAP for SNA.

11 Configure the token-ring port for APPN. Service any node means that the port will accept connections from any APPN node.

12 Configure the DLSw port for APPN and set the locally administered MAC address to 40002210ADDD (must be unique).

13 Configure the SDLC port for APPN.

14 Add and initiate the link to the VTAM APPN host.

15 Add and initiate the link to router 2210B on the DLSw over X.25 connection.

16 Add and initiate the link to router 2210C on the negotiable SDLC connection.

17 Configure the APPN node-level parameters.

18 This parameter corresponds to the ID number part of the node ID. The ID block portion of the node ID is hard coded as 077 for the 2210.

2210 Only

In the level of 2210 code that we used, the value specified using the command line interface was transposed. (The correct value is supplied by the Configuration Program.) This is only a problem if you do not follow our recommendation of using CPNAME to identify the 2210 to VTAM. Apply the fix for APAR NA02999.

The problem does not occur on the 2216.

3.4.3 Configuration Steps for 2210B

These steps show the APPN configuration from the very beginning. The general steps in this configuration are:

1. Qconfig for the basic parameters in Figure 27 on page 64. Interfaces 1, 2, and 5 have not been used.
2. Interface configuration of SDLC and X.25 in Figure 28 on page 67.
   - Interface 4 has been configured for X.25.
   - Interface 3 has been configured for SDLC.
3. IP and OSPF configuration in Figure 29 on page 70. TCP/IP configuration is necessary because we are using DLSw.
4. Bridging and DLSw configuration in Figure 30 on page 72.
5. APPN port configuration in Figure 31 on page 74.
6. APPN link configuration in Figure 32 on page 75.
7. APPN node configuration in Figure 33 on page 76.

```
2210B Config>q

Router Quick Configuration for the following:
o   Interfaces
o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing/Transparent Bridge (SR/TB)
        Source Routing Transparent Bridge (SRT)
o   Protocols
        IP (including OSPF, RIP and SNMP)
o   Booting
Event Logging will be enabled for all configured subsystems
with logging level 'Standard'
Note:  Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration

*********************************************************
Interface Configuration
*********************************************************

Type 'Yes' to Configure Interfaces
Type 'No' to skip Interface Configuration
Type 'Quit' to exit Quick Config

Configure Interfaces? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Interface Configuration

Intf 0 is Token Ring
Speed in Mb/sec (4, 16): [4]
Connector (STP, UTP): [STP]

Intf 1 is WAN PPP
Encapsulation for WAN 1  (PPP, Frame Relay): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 2 is WAN PPP
Encapsulation for WAN 2  (PPP, Frame Relay): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 3 is WAN PPP
Encapsulation for WAN 3  (PPP, Frame Relay): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 4 is WAN PPP
Encapsulation for WAN 4  (PPP, Frame Relay): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE] rs-232 dce
Internal clock speed (decimal) (2400 - 64000): [0] 64000

Intf 5 is Token Ring
Speed in Mb/sec (4, 16): [4]
Connector (STP, UTP): [STP]
```

Figure 27 (Part 1 of 3). Quick Configuration for Router B

```
This is all configured device information:

Intf 0 is Token Ring, Speed 4 Mb/sec, Connector STP
Intf 1 is WAN 1 with PPP Encapsulation, RS-232 DTE cable
Intf 2 is WAN 2 with PPP Encapsulation, RS-232 DTE cable
Intf 3 is WAN 3 with PPP Encapsulation, RS-232 DTE cable
Intf 4 is WAN 4 with PPP Encapsulation, RS-232 DCE cable,
 internal clock speed 64000 bits/second
Intf 5 is Token Ring, Speed 4 Mb/sec, Connector STP

Save this configuration? (Yes, No): [Yes]
Device configuration saved

*********************************************************
Bridging Configuration
*********************************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config
Configure Bridging? (Yes, No, Quit): [Yes] n

*********************************************************
Protocol Configuration
*********************************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Protocol Configuration
Configure IP? (Yes, No): [Yes]
Type 'r' any time at this level to restart IP Configuration

Configuring Per-Interface IP Information
Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 8.8.8.1
Address Mask: [255.0.0.0] 255.255.255.0

Configuring Interface 1 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] n
Configuring Interface 2 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] n
Configuring Interface 3 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] n

Configuring Interface 4 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 203.203.203.1
Address Mask: [255.255.255.0]

Configuring Interface 5 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes] n
```

Figure 27 (Part 2 of 3). Quick Configuration for Router B

```
Per-Interface IP Configuration complete
Configuring IP Routing Information
Enable Dynamic Routing? (Yes, No): [Yes]
Enable OSPF? (Yes, No): [Yes]
OSPF Enabled with Max routes = 1000 and Max routers = 50
Routing Configuration Complete

Configuring SNMP Information
SNMP will be configured with the following parameters:
     Community: public
     Access:    read_trap
SNMP Configuration Complete

This is the information you have entered:
     Interface #     IP Address         Address Mask   1
          0          8.8.8.1            255.255.255.0
          4          203.203.203.1      255.255.255.0
OSPF is configured, and RIP is configured only for 'sending'.
SNMP has been configured with the following parameters:
     Community: public
     Access:    read_trap
Save this configuration? (Yes, No): [Yes]
IP configuration saved

************************************************************
Booting Configuration
************************************************************
Type 'Yes' to Configure Booting
Type 'No' to skip Booting Configuration
Type 'Quit' to exit Quick Config
Configure Booting? (Yes, No, Quit): [Yes] n

************************************************************
Service Port Configuration
************************************************************
Type 'Yes' to Configure Service Ports
Type 'No' to skip Service Ports Configuration
Type 'Quit' to exit Quick Config
Configure service port? (Yes, No, Quit): [Yes] n

Quick Config Done
Restart the router for this configuration to take effect.
Restart the router? (Yes, No): [Yes] n
Type RESTART at the '*' prompt for the configuration to take effect.
```

Figure 27 (Part 3 of 3). Quick Configuration for Router B

```
Config>set data x25
Interface Number [0]? 4

Config>net 4   2
X.25 User Configuration
X.25 Config>set pvc lo 1
X.25 Config>set pvc high 9
X.25 Config>set svc low-t 0
X.25 Config>set svc high-t 0
X.25 Config>nat dis accept
X.25 Config>nat dis request
X.25 Config>nat dis flow
X.25 Config>nat dis through
X.25 Config>nat set stand v1988
X.25 Config>nat set discon active   4
X.25 Config>set equip dce
X.25 Config>set address
address []? 22102222

X.25 Config>add address  3
Protocol [IP]?
IP Address [0.0.0.0]? 203.203.203.2
Enc Priority 1 []? none
Enc Priority 2 []? none
X.25 Address []? 22101111

X.25 Config>add protocol   3
Protocol [IP]?
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
Circuit Idle Time [30]?
Max VCs [4]?

X.25 Config>add pvc   3
Protocol [IP]?
Destination X.25 Address []? 22101111
Window Size [2]?
Packet Size [128]?
```

Figure 28 (Part 1 of 3). X.25 and SDLC Configuration for Router B

```
X.25 Config>list all
X.25 Configuration Summary
Node Address:       22102222
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:           64000        Clocking:  Internal
MTU:              2048        Cable:     RS-232 DCE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DCE)
PVC              low: 1    high: 9
Inbound          low: 0    high: 0
Two-Way          low: 0    high: 0
Outbound         low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400
X.25 National Personality Configuration
Follow CCITT: on        OSI 1984:     on        OSI 1988:       off
Request Reverse Charges:  off   Accept Reverse Charges:     off
Frame Extended seq mode:  off   Packet Extended seq mode:   off
Incoming Calls Barred:    off   Outgoing Calls Barred:      off
Throughput Negotiation:   off   Flow Control Negotiation:   off
Suppress Calling Addresses: off
DDN Address Translation:  off
Call Request Timer:     20 decaseconds
Clear Request Timer:    18 decaseconds (1 retries)
Reset Request Timer:    18 decaseconds (1 retries)
Restart Request Timer:  18 decaseconds (1 retries)
Min Recall Timer:       10 seconds
Min Connect Timer:      90 seconds
Collision Timer:        10 seconds
T1 Timer:  4.00 seconds     N2 timeouts: 20
T2 Timer:  0.00 seconds     DP Timer:    500 milliseconds
Standard Version:     1988      Network Type: CCITT
Disconnect Procedure: active  4
Window Size     Frame:   7      Packet:  2
Packet Size     Default: 128    Maximum: 256

X.25 protocol configuration
Prot         Window      Packet-size        Idle     Max     Station
Number       Size      Default Maximum      Time     VCs      Type
0  -> IP      2          128     256         30       4        -

X.25 PVC configuration
Prtcl        X.25_address     Active Enc  Window    Pkt_len   Pkt_chan
0   (IP)     22101111           NONE      2         128       1

X.25 address translation configuration
IF #  Prot #       Active Enc  Protocol       -> X.25 address
4     0  (IP)         NONE     203.203.203.2  -> 22101111
X.25 Config>ex
```

Figure 28 (Part 2 of 3). X.25 and SDLC Configuration for Router B

```
Config>set data sdlc
Interface Number [0]? 3
Config>net 3
SDLC user configuration
Creating a default configuration for this link
SDLC 3 Config>set link role primary   5

SDLC 3 Config>add station   5
Enter station address (in hex) [C1]? d1
Enter station name [SDLC_D1]?
Include station in group poll list ([Yes] or No):
Enter max packet size [2048]?
Enter receive window [7]?
Enter transmit window [7]?

SDLC 3 Config>list link
Link configuration for: LINK_3   (ENABLED)
Role:        PRIMARY          Type:        POINT-TO-POINT
Duplex:      FULL             Modulo:      8
Idle state:  FLAG             Encoding:    NRZ
Clocking:    EXTERNAL         Frame Size:  2048
Speed:       0                Group Poll:  00
Cable:       RS-232 DTE
Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
           RTS hold delay:     DISABLED
           Inter-frame delay:  DISABLED
           Inactivity timeout: 30.0 sec
Counters:  XID/TEST retry:  8
           SNRM retry:      6
           Poll retry:      10

SDLC 3 Config>li sta all
Address    Name      Status    Max BTU  Rx Window  Tx Window
-------  --------  ----------  -------  ---------  ---------
  D1(00) SDLC_D1     ENABLED      2048       7          7

SDLC 3 Config>ex
```

Figure 28 (Part 3 of 3). X.25 and SDLC Configuration for Router B

```
Config>p ip
Internet protocol user configuration

IP config>set internal  6
Internal IP address [8.8.8.1]? 10.8.8.1

IP config>li all

Interface addresses
IP addresses for each interface:
   intf  0   8.8.8.1          255.255.255.0    Local wire broadcast, fill 1
   intf  1                                     IP disabled on this interface
   intf  2                                     IP disabled on this interface
   intf  3                                     IP disabled on this interface
   intf  4   203.203.203.1    255.255.255.0    Local wire broadcast, fill 1
   intf  5                                     IP disabled on this interface
Internal IP address: 10.8.8.1

Routing
Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: enabled
BGP: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
     intf  0   8.8.8.1          Send net, subnet, static and default routes
                                Received RIP packets are ignored.
     intf  1                    IP & RIP are disabled on this interface
     intf  2                    IP & RIP are disabled on this interface
     intf  3                    IP & RIP are disabled on this interface
     intf  4   203.203.203.1    RIP disabled for this interface
     intf  5                    IP & RIP are disabled on this interface
Accept RIP updates always for:
[NONE]

IP config>ex
```

Figure 29 (Part 1 of 2). TCP/IP and OSPF Configuration for Router B

```
Config>p ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>add neighbor  7
Interface IP address [0.0.0.0]? 203.203.203.1
IP Address of Neighbor [0.0.0.0]? 203.203.203.2
Can that router become Designated Router on this net [Yes]?

OSPF Config>set non-broadcast  7
Interface IP address [0.0.0.0]? 203.203.203.1
Poll Interval [120]?

OSPF Config>li all
                        --Global configuration--
                OSPF Protocol:          Enabled
                # AS ext. routes:       1000
                Estimated # routers:    50
                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
8.8.8.1           0.0.0.0              1      5       1     1     10     40
203.203.203.1     0.0.0.0              1      5       1     1     10     40
                        --NBMA configuration--
                Interface Addr      Poll Interval
                203.203.203.1       120
                        --Neighbor configuration--
                Neighbor Addr     Interface Address   DR eligible?
                203.203.203.2     203.203.203.1       yes

OSPF Config>exit
```

Figure 29 (Part 2 of 2). TCP/IP and OSPF Configuration for Router B

```
Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration

ASRT config>enable bridge  8
ASRT config>enable dls  8
ASRT config>enable source-rout  8
Port Number [1]?
Segment Number for the port in hex(1 - FFF) [  1]? ffb
Bridge number in hex (0 - 9, A - F) [0]? 2

ASRT config>disable transparent 1

ASRT config>list bridge
                Source Routing Transparent Bridge Configuration
                ===============================================
Bridge:                 Enabled                 Bridge Behavior: SRB
                   +----------------------------+
------------------] SOURCE ROUTING INFORMATION ]------------------------------
                   +----------------------------+
Bridge Number:          02                      Segments:          1
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1 N SRB:                Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
                   +-------------------+
------------------] SR-TB INFORMATION ]---------------------------------------
                   +-------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
                   +-----------------------------------+
------------------] SPANNING TREE PROTOCOL INFORMATION ]----------------------
                   +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IBM-SRB proprietary
                   +-------------------------+
------------------] TRANSLATION INFORMATION ]---------------------------------
                   +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                   +------------------+
------------------] PORT INFORMATION ]-----------------------------------------
                   +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled

ASRT config>ex
```

Figure 30 (Part 1 of 2). DLSw Configuration for Router B

```
Config>p dls
DLSw protocol user configuration
DLSw config>enable dls   9
DLSw config>set srb fab   9

DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 10.24.104.93   10
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]? e
Neighbor Priority (H/M/L) [M]?

DLSw config>open-sap   10
Interface # [0]?
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 0

DLSw config>list dls
DLSw is                             ENABLED
LLC2 send Disconnect is             ENABLED
Dynamic Neighbors is                ENABLED
SRB Segment number                  FAB
MAC <-> IP mapping cache size       128
Max DLSw sessions                   1000
DLSw global memory allotment        141312
LLC per-session memory allotment    8192
SDLC per-session memory allotment   4096
NetBIOS UI-frame memory allotment   40960
Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor Priority              MEDIUM

DLSw config>exit
```

Figure 30 (Part 2 of 2). DLSw Configuration for Router B

```
Config>p appn
APPN user configuration

APPN config>add port   11
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? t
Interface number(Default 0): [0]?
Port name (Max 8 characters) [TR000]? tkrb0
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add port   12
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? d
Port name (Max 8 characters) [DLS254]? dlsb4
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Locally administered MAC address (hex) [000000000000]? 40002210bddd
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add port   13
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? s
Interface number(Default 0): [0]? 3
Port name (Max 8 characters) [SDLC003]? sdlcb3
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 31. APPN Port Configuration for Router B

```
APPN config>add link  14
APPN Station
Port name for the link station [ ]? dlsb4
Station name (Max 8 characters) [ ]? r2210ad
 Activate link automatically (Y)es (N)o [Y]?
 MAC address of adjacent node [000000000000]? 40002210addd  14
 SAP address of adjacent node(04-EC) [4]?
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add link  15
APPN Station
Port name for the link station [ ]? sdlcb3
Station name (Max 8 characters) [ ]? r2210cs
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C1]? d2
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 32. APPN Link Configuration for Router B

```
APPN config>set node  16
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? usibmra
Control point name (Max 8 characters) [  ]? ra2210b
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]? 2210b  17
Write this record? [Y]?
The record has been written.
APPN config>li all
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210B
 XID: 2210B
 APPN ENABLED: YES
 MAX SHARED MEMORY: 4096
 MAX CACHED: 4000
DLUR:
 DLUR ENABLED: NO
 PRIMARY DLUS NAME:
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 ---------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 ------------------------------------------------------
     0      TKRB0   IBMTRNET    YES      YES      YES
   254      DLSB4        DLS     NO      YES      YES
     3     SDLCB3       SDLC     NO      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
  R2210AD    DLSB4    40002210ADDD        NO     YES       0
  R2210CS   SDLCB3              D2        NO     YES       0
LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------
APPN config>ex
*restart
```

Figure 33. APPN Node Configuration for Router B

,**********

Notes:

1 Configure the IP addresses for the interfaces used. Address 8.8.8.1 is the token-ring address while 203.203.203.1 is the address of the X.25 interface.

2 This is the X.25 interface configuration for a back-to-back connection using RS-232 DTE and DCE cables.

3 Configure the PVC address, and the protocol for TCP/IP over the X.25 link.

4 For back-to-back X.25 links, one 2210 should be configured for a passive disconnect procedure while the other 2210 should have active disconnect procedure.

5 Configure the SDLC port with the link role as primary.

6 Set the router's internal IP address for DLSw.

7 Add the OSPF neighbor on the non-broadcast X.25 link.

8 Configure the ASRT protocol for DLSw. Enable the bridge and DLSw.

9 Configure the DLSw protocol. Enable DLSw and set the virtual ring number to fab.

10 Add the DLSw neighbor address and open SAP for SNA.

11 Configure the token-ring port for APPN. Service any node means that the port will accept connection from any APPN node.

12 Configure the DLSw port for APPN and set the locally administered MAC address to 40002210BDDD (must be unique).

13 Configure the SDLC port for APPN.

14 Add and initiate the link to router 2210A on the DLSw over X.25 connection.

15 Add and initiate the link to router 2210C on the SDLC connection.

16 Configure the APPN node-level parameters.

17 This parameter corresponds to the ID number part of the node ID. The ID block portion of the node ID is hard coded as 077 for the 2210. Because 2210B is not connected to a subarea, this parameter is optional.

2210 Only

In the level of 2210 code that we used, the value specified using the command line interface was transposed. (The correct value is supplied by the Configuration Program.) This is only a problem if you do not follow our recommendation of using CPNAME to identify the 2210 to VTAM. Apply the fix for APAR NA02999.

The problem does not occur on the 2216.

3.4.4 Configuration Steps for 2210C

These steps show the APPN configuration for 2210C. The general steps in this configuration are:

1. Interface configuration of SDLC in Figure 34 on page 79.
2. APPN port configuration in Figure 35 on page 81.
3. APPN link configuration in Figure 36 on page 82.
4. APPN node configuration in Figure 37 on page 83.

```
Config>set data sdlc
Interface Number [0]? 1

Config>set data sdlc
Interface Number [0]? 2

Config>list dev
Ifc 0   Token Ring                    CSR 6000000, vector 28
Ifc 1   WAN SDLC                      CSR  81620, CSR2  80D00, vector 93
Ifc 2   WAN SDLC                      CSR  81640, CSR2  80E00, vector 92

Config>net 1
SDLC user configuration
Creating a default configuration for this link

SDLC 1 Config>set link role secondary  1

SDLC 1 Config>add station
Enter station address (in hex) [C1]? b3
Enter station name [SDLC_B3]?
Include station in group poll list ([Yes] or No):
Enter max packet size [2048]?
Enter receive window [7]?
Enter transmit window [7]?

SDLC 1 Config>set link cable rs-232 dce  1
SDLC 1 Config>set link clock internal
Must also set the line speed to a valid value
Line speed (2400 to 2048000) [0]? 56000

SDLC 1 Config>list link
Link configuration for: LINK_1   (ENABLED)
Role:        SECONDARY        Type:        POINT-TO-POINT
Duplex:      FULL             Modulo:      8
Idle state:  FLAG             Encoding:    NRZ
Clocking:    INTERNAL         Frame Size:  2048
Speed:       56000            Group Poll:  00
Cable:       RS-232 DCE
Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
           RTS hold delay:     DISABLED
           Inter-frame delay:  DISABLED
           Inactivity timeout: 30.0 sec
Counters:  XID/TEST retry:  8
           SNRM retry:      6
           Poll retry:      10

SDLC 1 Config>list station all
Address    Name      Status    Max BTU  Rx Window  Tx Window
-------  --------  ----------  -------  ---------  ---------
  B3(00) SDLC_B3     ENABLED      2048       7          7

SDLC 1 Config>ex
```

Figure 34 (Part 1 of 2). SDLC Interface Configuration for Router C

```
Config>n 2
SDLC user configuration
Creating a default configuration for this link

SDLC 2 Config>set link cable rs-232 dce  2
SDLC 2 Config>set link cloc internal
Must also set the line speed to a valid value
Line speed (2400 to 2048000) [0]? 56000
SDLC 2 Config>set link role negotiable  2

SDLC 2 Config>list link
Link configuration for: LINK_2   (ENABLED)
Role:        NEGOTIABLE       Type:        POINT-TO-POINT
Duplex:      FULL             Modulo:      8
Idle state:  FLAG             Encoding:    NRZ
Clocking:    INTERNAL         Frame Size:  2048
Speed:       56000            Group Poll:  00
Cable:       RS-232 DCE
Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
           RTS hold delay:     DISABLED
           Inter-frame delay:  DISABLED
           Inactivity timeout: 30.0 sec
Counters:  XID/TEST retry:  8
           SNRM retry:      6
           Poll retry:      10

SDLC 2 Config>add station
Enter station address (in hex) [C1]? a3
Enter station name [SDLC_A3]?
Include station in group poll list ([Yes] or No):
Enter max packet size [2048]?
Enter receive window [7]?
Enter transmit window [7]?

SDLC 2 Config>list station all
Address    Name      Status    Max BTU  Rx Window  Tx Window
-------  --------  ----------  -------  ---------  ---------
  A3(00) SDLC_A3     ENABLED      2048       7          7

SDLC 2 Config>ex
```

Figure 34 (Part 2 of 2). SDLC Interface Configuration for Router C

```
Config>p appn
APPN user configuration

APPN config>add port  3
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? t
Interface number(Default 0): [0]?
Port name (Max 8 characters) [TR000]? tkrc0
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add port  4
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? s
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]? sdlcc1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add port  5
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? s
Interface number(Default 0): [0]? 2
Port name (Max 8 characters) [SDLC002]? sdlcc2
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 35. APPN Port Configuration for Router C

```
APPN config>add link   6
APPN Station
Port name for the link station [ ]? sdlcc1
Station name (Max 8 characters) [ ]? r2210bs
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C1]? b3
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>add link   7
APPN Station
Port name for the link station [ ]? sdlcc2
Station name (Max 8 characters) [ ]? r2210as
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C1]? a3
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 36. APPN Link Configuration for Router C

```
APPN config>set node  8
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? usibmra
Control point name (Max 8 characters) [  ]? ra2210c
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]? 2210c  9
Write this record? [Y]?
The record has been written.

C APPN config>set tuning  10
Manual tuning
 WARNING!! These changes require a router reboot to take affect.
 Max. shared memory(1024-40960 KB) [4096]? 1792
 WARNING!! If DRAM is 8 Meg, GLOBAL-BUFFERS must not exceed 50,
nor max cashed directory entries exceed 200.
 Percent buffer memory(10-50) [13]? 17
 Max. cached directory entries(10-65535) [4000]? 200
Write this record? [Y]?
The record has been written.

APPN config>list all
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210C
 XID: 2210C
 APPN ENABLED: YES
 MAX SHARED MEMORY: 1792
 MAX CACHED: 200
DLUR:
 DLUR ENABLED: NO
 PRIMARY DLUS NAME:
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
```

Figure 37 (Part 1 of 2). APPN Node Configuration for Router C

```
MODE:
  MODE NAME  COS NAME
 --------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 ------------------------------------------------------
     0      TKRC0   IBMTRNET    YES      YES      YES
     1     SDLCC1       SDLC     NO      YES      YES
     2     SDLCC2       SDLC     NO      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
  R2210BS   SDLCC1              B3        NO     YES       0
  R2210AS   SDLCC2              A3        NO     YES       0
LU NAME:
       LU NAME          STATION NAME           CP NAME
 ------------------------------------------------------------

APPN config>exit

Config>set global 50  11
Number of global packet buffers has been updated successfully

*restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 37 (Part 2 of 2). APPN Node Configuration for Router C

Notes:

1 Configure the SDLC port with the link role as secondary. This is interface number 1, which provides the clocking on a back-to-back RS-232 link with router 2210B. Router 2210B acts as the primary on this SDLC link.

2 Configure the SDLC port with the link role as negotiable. This is interface number 2, which provides the clocking on a back-to-back RS-232 link with router 2210A. Router 2210A also has a negotiable SDLC link role.

3 Configure the token-ring port for APPN. Service any node means that the port will accept connection from any APPN node.

4 Configure the first SDLC port for APPN. Service any node means that the port will accept connection from any APPN node.

5 Configure the second SDLC port for APPN. Service any node means that the port will accept connection from any APPN node.

6 Add and initiate the link to router 2210B on the SDLC connection.

7 Add and initiate the link to router 2210A on the SDLC connection.

8 Configure the APPN node-level parameters.

9 This parameter corresponds to the ID number part of the node ID. The ID block portion of the node ID is hard coded as 077 for the 2210. Because 2210B is not connected to a subarea, this parameter is optional.

2210 Only

In the level of 2210 code that we used, the value specified using the command line interface was transposed. (The correct value is supplied by the Configuration Program.) This is only a problem if you do not follow our recommendation of using CPNAME to identify the 2210 to VTAM. Apply the fix for APAR NA02999.

The problem does not occur on the 2216.

10 Configure the tuning parameters. This is very important on routers with 8 MB of DRAM.

11 Set the global packet buffers. This is also very important on routers with 8 MB of DRAM.

3.4.5 ISR Monitoring and Testing

To see the APPN/ISR sessions and the network connectivity, we used the APPN monitor commands on the router. We also created data traffic in the network by using the end nodes on the remote and local LANs.

3.4.5.1 Monitor Information for Router 2210A

Figure 38 on page 86 shows the information gathered from the monitor commands of the 2210A router. Note that HPR is active only on the token-ring link between 2210A and the VTAM network node (USIBMRA.RAK), while ISR runs on the SDLC and X.25/DLSw links. However, in this setup the USIBMRA.RAK VTAM is only enabled for ANR (it is a VTAM V4R3 interchange node) and is not capable of acting as an RTP endpoint. Therefore, there is no active RTP session between 2210A and VTAM. The ISR sessions can be seen from the list isr_sessions output where we see an active ISR sessions from 2210A to the VTAM and 2210B.

```
*t 5
+p appn
APPN >list links
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=============================================================================
 R2210CS      SDLCA3    3    USIBMRA.RA2210C    NN  INACTIVE     ACT_LS
     RAK       TKRA0    0        USIBMRA.RAK    NN    ACTIVE     ACT_LS
 R2210BD       DLSA4  254    USIBMRA.RA2210B    NN  INACTIVE     ACT_LS

APPN >list isr
  Adjacent CP Name  TG Number   ISR Sessions
================================================
   USIBMRA.RA2210C      15             0
       USIBMRA.RAK      15             1
   USIBMRA.RA2210B      15             1

APPN >l rtp
No HPR information available

APPN >li cp
           CP Name      Type    Status  Connwiner ID    Conloser ID
=========================================================================
       USIBMRA.RAK       NN     Active    D37CD090        D37CD08F
   USIBMRA.RA2210B       NN     Active    D37CD0D0        D37CD0CF
   USIBMRA.RA2210C       NN     Active    D37CD0A6        D37CD0A5

APPN >ex
```

Figure 38. APPN Monitor for Router A

3.4.5.2 Monitor Information for Router 2210B

Figure 39 on page 87 shows the information gathered from the monitor commands of the 2210B router. Note that HPR is active only on the token-ring link between 2210B and the WS05600 workstation, while ISR runs on the SDLC and X.25 links. During the testing of this scenario, the active session went from EN-2210B-2210A-EN. This can be seen from the list isr_sessions output where we see an active ISR session between 2210B and 2210A. We have also displayed the RTP session on the HPR link between 2210B and WS05600 on the token-ring. Mode name #INTER is the mode used by the APING test utility.

```
*t 5
+p appn
APPN >list link
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=============================================================================
     @@0       TKRB0    0    USIBMRA.WS0560O    EN    ACTIVE     ACT_LS
 R2210CS      SDLCB3    3    USIBMRA.RA2210D    NN  INACTIVE     ACT_LS
 R2210AD       DLSB4  254    USIBMRA.RA2210A    NN  INACTIVE     ACT_LS

APPN >list isr
  Adjacent CP Name  TG Number   ISR Sessions
================================================
   USIBMRA.RA2210C      19             0
   USIBMRA.RA2210A      15             1
   USIBMRA.WS0560O      15             0

APPN >list cp
           CP Name      Type    Status  Connwiner ID    Conloser ID
=============================================================================
   USIBMRA.WS0560O       EN     Active    B6A235D7        B6A235D3
   USIBMRA.RA2210C       NN     Active    B6A23567        B6A23566
   USIBMRA.RA2210A       NN     Active    B6A23585        B6A23584

APPN >list rtp
RTP PARTNER TABLE:
 Remote Partner Name  Remote Boundary Name  TG Number
=====================================================
     USIBMRA.WS0560O         FFFFFFFF
RTP CONNECTION TABLE:
  TCID             CP Name  ISR  APPC  Pathswitch    Alive    COS TPF   TG Number
=============================================================================
317740B0   USIBMRA.WS0560O    1    0    00000708  00000262     #INTER      15
APPN >
```

Figure 39. APPN Monitor for Router B

3.4.5.3 Monitor Information for Router 2210C

Figure 40 on page 88 shows the information gathered from the monitor commands of the 2210C router. The active links are all SDLC and so only ISR routing is supported. This can be seen from the list isr_sessions output where we see active ISR sessions to 2210B and 2210A. During this testing, the SDLC links are acting as backup and are not carrying sessions.

```
APPN >li li
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=========================================================================
 R2210AS      SDLCC2    2    USIBMRA.RA2210A    NN  INACTIVE     ACT_LS
 R2210BS      SDLCC1    1    USIBMRA.RA2210B    NN  INACTIVE     ACT_LS

APPN >li cp
           CP Name      Type    Status  Connwiner ID    Conloser ID
=========================================================================
   USIBMRA.RA2210B       NN     Active    B6A2E2D1        B6A2E2D0
   USIBMRA.RA2210A       NN     Active    B6A2E2E6        B6A2E2E3

APPN >li isr
  Adjacent CP Name  TG Number   ISR Sessions
================================================
   USIBMRA.RA2210B      15             0
   USIBMRA.RA2210A      15             0
APPN >
```

Figure 40. APPN Monitor for Router C

3.4.5.4 ISR Connection Test

To test the APPN network, we have used the APING utility from the Communications Server client software and from VTAM. Shown in Figure 41 is the sample of an APING output from WS05600 (PC in 2210B's token-ring) to VTAM (mainframe in 2210A's token-ring).

```
c:\>aping usibmra.rak

IBM APING version 2.43.3c  APPC echo test with timings.
Licensed Materials - Property of IBM
(C) Copyright 1994,1995 by IBM Corp. All rights reserved.

Allocate duration:                          313 ms
Program startup and Confirm duration:      1531 ms

Connected to a partner running on: (UNKNOWN operating system)
        Duration        Data Sent        Data Rate        Data Rate
        (msec)          (bytes)          (KB/s)           (Mb/s)
        --------        ---------        ---------        ---------
             469              200              0.4            0.003
             344              200              0.6            0.005
Totals:      813              400              0.5            0.004
Duration statistics:   Min = 344   Ave = 406   Max = 469
```

Figure 41. APING Test from PC Workstation to VTAM

3.5 A Sample High-Performance Routing Configuration Scenario

APPN High-Performance Routing support has been included in the intial levels of Multiprotocol Routing Services for the IBM 2210 Nways Multiprotocol Router and Multiprotocol Access Services for the IBM 2216 Nways Multiaccess Connector. We develop an example scenario that uses HPR over the connection types supported by MRS V1R1.0 and MAS V1R1.0, which are:

- Token-ring
- Ethernet
- PPP
- Frame relay

2216 Only

MAS V1R1.1 adds HPR support for the ESCON MPC+.

The 2210 and 2216 distinguish between HPR and ISR traffic (see “Traffic Types” on page 16), and therefore can act both as an ANR and an ISR routing node.

3.5.1 HPR Scenario Description

This scenario illustrates basic HPR configuration for the three router network shown in Figure 42 on page 90.

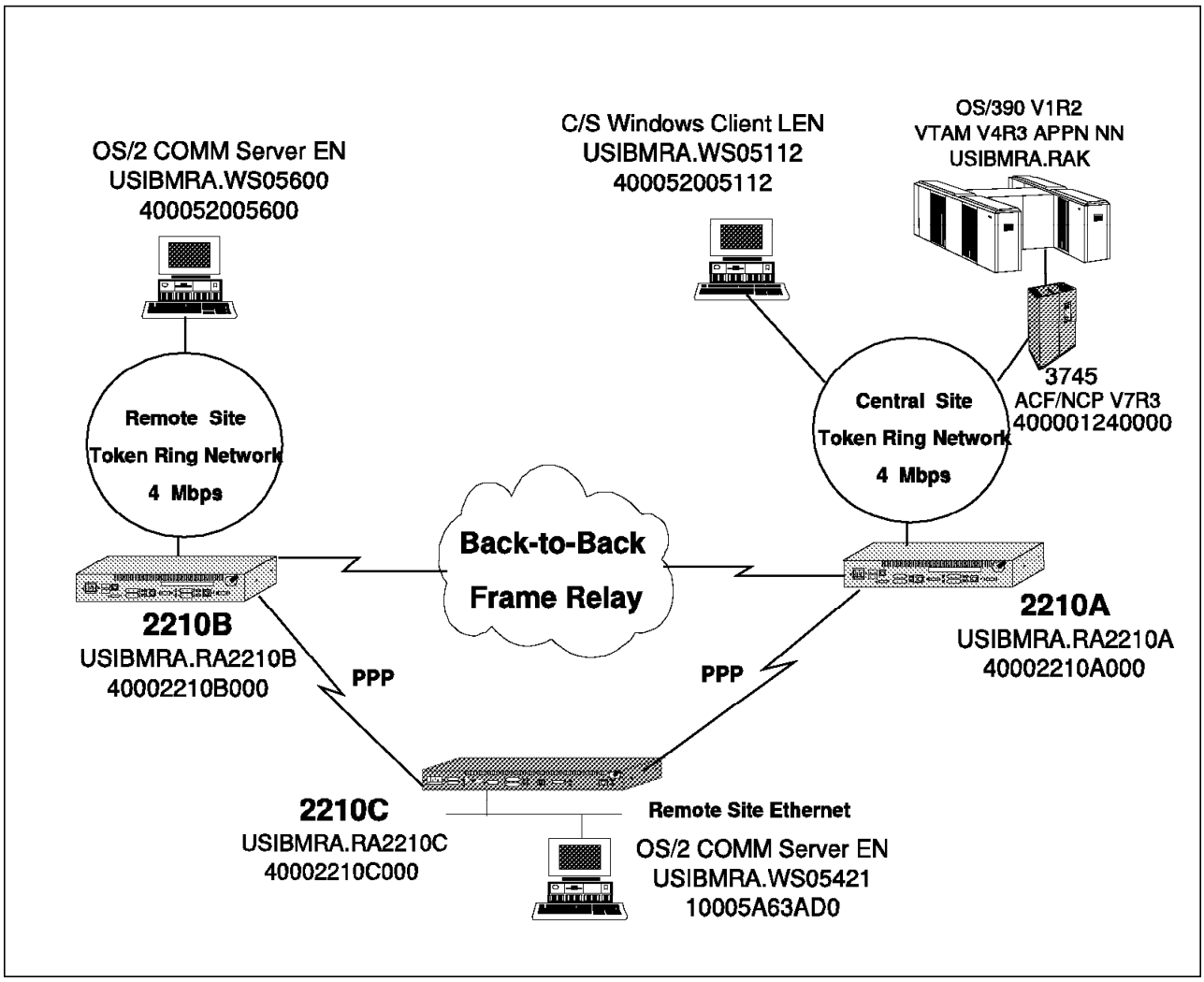


Figure 42. Logical Diagram of the HPR Scenario

The key components in this setup are:

- 2210A router - Model 14T with 8 MB DRAM and 4 MB Flash. Attached to the main token-ring LAN which connects the mainframes and other end nodes.
- 2210B router - Model 12T with 8 MB DRAM and 4 MB Flash. Attached to the remote token-ring LAN.
- 2210C router - Model 128 with 8 MB DRAM and 4 MB Flash. Attached to the remote Ethernet LAN.
- Network node on the main token-ring - VTAM mainframe host.
- The frame-relay link is a back-to-back connection using a V.35 modem eliminator.
- The PPP links are back-to-back connections using RS-232 DTE and DCE cables.

Configuration steps are shown using the 2210's command line interface. A blank response means we accepted the default value enclosed in square brackets.

3.5.2 HPR Configuration Steps for Router 2210A

These steps show the configuration for the APPN protocol. We have preconfigured the other required parameters including:

- Token-ring interface was set for 4 Mbps, STP, and MAC address of 40002210A000.
- Frame relay (back-to-back) on interface 1 through a V.35 modem eliminator.
- PPP (back-to-back) on interface 2 using RS-232 cables.

The general steps in this configuration are:

1. APPN/HPR port configuration in Figure 43 on page 92.
2. APPN/HPR link configuration in Figure 44 on page 94.
3. APPN/HPR node configuration in Figure 45 on page 96.

```
Config>P APPN
APPN user configuration

APPN config>ADD PORT

APPN Port

Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? T  1
Interface number(Default 0): [0]?
Port name (Max 8 characters) [TR000]? TKRA1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?  2
 High performance routing: (Y)es (N)o [Y]?  3
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>ADD PORT

APPN Port

Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? F  4
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [FR001]? FRA1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?  4
 Maximum BTU size (768-2048) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Support bridged formatted frames: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 43 (Part 1 of 2). APPN/HPR Port Configuration for Router A

```
APPN config>ADD PORT

APPN Port

ink Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? P    5
Interface number(Default 0): [0]? 2
Port name (Max 8 characters) [PPP002]? PPPA2
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?    5
 Maximum BTU size (768-2048) [2048]?
 Local SAP address (04-EC) [4]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?

Write this record? [Y]?
The record has been written.
```

Figure 43 (Part 2 of 2). APPN/HPR Port Configuration for Router A

```
APPN config>ADD LINK

APPN Station

Port name for the link station [ ]? TKRA1
Station name (Max 8 characters) [ ]? RAK   6
 Activate link automatically (Y)es (N)o [Y]?
 MAC address of adjacent node [000000000000]? 400001240000
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0   6
 High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?

Write this record? [Y]?
The record has been written.

APPN config>ADD LINK

APPN Station
Port name for the link station [ ]? TKRA1
Station name (Max 8 characters) [ ]? WS05112   7
 Activate link automatically (Y)es (N)o [Y]?
 MAC address of adjacent node [000000000000]? 10005AAC4296
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 2    7
 High performance routing: (Y)es (N)o [Y]? N    7
 XID node identification (8 hex digits) [00000000]? 05D05112
 Fully-qualified CP name of adjacent node (netID.CPname) []? USIBMRA.WS05112
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?

Write this record? [Y]?
The record has been written.
```

Figure 44 (Part 1 of 2). APPN/HPR Link Configuration for Router A

```
APPN config>ADD LINK

APPN Station
Port name for the link station [ ]? FRA1
Station name (Max 8 characters) [ ]? R2210B   8
 Activate link automatically (Y)es (N)o [Y]?
 DLCI number for link (16-1007) [16]?
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0   8
 High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?

The record has been written.

APPN config>ADD LINK

APPN Station

Port name for the link station [ ]? PPPA2
Station name (Max 8 characters) [ ]? R2210C   9
 Activate link automatically (Y)es (N)o [Y]?
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0   9
 High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?

Write this record? [Y]?
The record has been written.
```

Figure 44 (Part 2 of 2). APPN/HPR Link Configuration for Router A

```
APPN config>SET NODE   10

Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? USIBMRA
Control point name (Max 8 characters) [  ]? RA2210A
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]? 2210A   11
Write this record? [Y]?

The record has been written.

APPN config>ENABLE APPN

APPN config>SET TUNING   12

Manual tuning
 WARNING!! These changes require a router reboot to take affect.
 Max. shared memory(1024-40960 KB) [4096]? 1792
 WARNING!! If DRAM is 8 Meg, GLOBAL-BUFFERS must not exceed 50,
nor max cashed directory entries exceed 200.
 Percent buffer memory(10-50) [13]? 17
 Max. cached directory entries(10-65535) [4000]? 200

Write this record? [Y]? Y
The record has been written.
```

Figure 45 (Part 1 of 2). APPN/HPR Node Configuration for Router A

```
APPN config>LIST ALL
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210A
 XID: 2210A
 APPN ENABLED: YES
 MAX SHARED MEMORY: 1792
 MAX CACHED: 200
 LUR:
 DLUR ENABLED: NO
 PRIMARY DLUS NAME:
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ---------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 --------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 -------------------------------------------------------
     0      TKRA1   IBMTRNET    YES      YES      YES
     1       FRA1         FR    YES      YES      YES
     2      PPPA2        PPP    YES      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
      RAK    TKRA1    400001240000       YES     YES       0
  WS05112    TKRA1    10005AAC4296        NO      NO       2
   R2210B     FRA1              16       YES     YES       0
   R2210C    PPPA2    000000000000       YES     YES       0
LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------

APPN config>EXIT

Config>SET GLOBAL  13
What is the maximum number of global packet buffers [0]? 50
Number of global packet buffers has been updated successfully
*RESTART
```

Figure 45 (Part 2 of 2). APPN/HPR Node Configuration for Router A

Notes:

1 Configure the token-ring port (interface 0) for HPR.

2 Service any node means that this port will accept all requests for connection. If you want added security by ensuring that only authorized stations use this network node, specify No for this parameter. You then have to define explicit links to the authorized stations.

3 Enable HPR on this port.

4 Add and enable HPR on the frame-relay port at interface 1.

5 Add and enable HPR on the PPP port at interface 2.

6 Add and initiate a link to a VTAM host.

7 Add and initiate a link to the PC running Communication Server Client for Windows 3.1. This station is a LEN node and is not HPR-capable.

8 Add and configure the FR link to router 2210B (NN).

9 Add and configure the PPP link to router 2210C (NN).

10 Configure the node-level parameters including the router's network ID and CP name.

11 This parameter corresponds to the ID number part of the node ID. The ID block portion of the node ID is hard coded as 077 for the 2210.

2210 Only

In the level of 2210 code that we used, the value specified using the command line interface was transposed. (The correct value is supplied by the Configuration Program.) This is only a problem if you do not follow our recommendation of using CPNAME to identify the 2210 to VTAM. Apply the fix for APAR NA02999.

The problem does not occur on the 2216.

12 Tune the router's resource usage. This is very important for 2210s with only 8 MB of DRAM.

13 Set global buffers for tuning of an 8-MB router.

3.5.3 HPR Configuration Steps for Router 2210B

These steps show the configuration for the APPN protocol. We have preconfigured the other required parameters including:

- Token-ring interface was set for 4 Mbps, STP, and MAC address of 40002210B000.
- Frame relay (back-to-back) on interface 1 through a V.35 modem eliminator.
- PPP (back-to-back) on interface 2 using RS-232 cables.

The general steps in this configuration are:

1. APPN/HPR port configuration in Figure 46 on page 99.
2. APPN/HPR link configuration in Figure 47 on page 101.
3. APPN/HPR node configuration in Figure 48 on page 102.

```
Config>p appn
APPN user configuration

APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? T   1
Interface number(Default 0): [0]?
Port name (Max 8 characters) [TR000]? TKRB1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?   2
 High performance routing: (Y)es (N)o [Y]?   3
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>ADD PORT
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? F   4
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [FR001]? FRB1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?   4
 Maximum BTU size (768-2048) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Support bridged formatted frames: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 46 (Part 1 of 2). APPN/HPR Port Configuration for Router B

```
APPN config>ADD PORT
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? P   5
Interface number(Default 0): [0]? 2
Port name (Max 8 characters) [PPP002]? PPPB2
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?   5
 Maximum BTU size (768-2048) [2048]?
 Local SAP address (04-EC) [4]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 46 (Part 2 of 2). APPN/HPR Port Configuration for Router B

```
APPN config>ADD LINK

APPN Station
Port name for the link station [ ]? FRB1
Station name (Max 8 characters) [ ]? R2210A   6
 Activate link automatically (Y)es (N)o [Y]?
 DLCI number for link (16-1007) [16]?
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0   6
 High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?

The record has been written.

APPN config>ADD LINK

APPN Station
Port name for the link station [ ]? PPPB2
Station name (Max 8 characters) [ ]? R2210C    7
 Activate link automatically (Y)es (N)o [Y]?
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0   7
 High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?

The record has been written.
```

Figure 47. APPN/HPR Link Configuration for Router B

```
APPN config>SET NODE   8

Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? USIBMRA
Control point name (Max 8 characters) [  ]? RA2210B
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]? 2210B   9
Write this record? [Y]?

The record has been written.

APPN config>SET TUNING   10

Manual tuning
 WARNING!! These changes require a router reboot to take affect.
 Max. shared memory(1024-40960 KB) [4096]? 1792
 WARNING!! If DRAM is 8 Meg, GLOBAL-BUFFERS must not exceed 50,
nor max cashed directory entries exceed 200.
 Percent buffer memory(10-50) [13]? 17
 Max. cached directory entries(10-65535) [4000]? 200
Write this record? [Y]?

The record has been written.
```

Figure 48 (Part 1 of 2). APPN/HPR Node Configuration for Router B

```
APPN config>LI ALL
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210B
 XID: 00000
 APPN ENABLED: YES
 MAX SHARED MEMORY: 1792
 MAX CACHED: 200
DLUR:
 DLUR ENABLED: NO
 PRIMARY DLUS NAME:
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ---------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 --------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 -------------------------------------------------------
     0      TKRB1   IBMTRNET    YES      YES      YES
     1       FRB1         FR    YES      YES      YES
     2      PPPB2        PPP    YES      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
   R2210A     FRB1              16       YES     YES       0
   R2210C    PPPB2    000000000000       YES     YES       0
LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------
APPN config>EXIT

Config>SET GLOBAL    11
What is the maximum number of global packet buffers [0]? 50
Number of global packet buffers has been updated successfully

Config>
*RESTART
```

Figure 48 (Part 2 of 2). APPN/HPR Node Configuration for Router B

Notes:

1 Configure the token-ring port (interface 0) for HPR.

2 Service any node means that this port will accept all requests for connection. If you want added security by ensuring that only authorized stations use this network node, specify No for this parameter. You then have to define explicit links to the authorized stations.

3 Enable HPR on this port.

4 Add and enable HPR on the frame relay port at interface 1.

5 Add and enable HPR on the PPP port at interface 2.

6 Add and configure the FR link to router 2210A (NN).

7 Add and configure the PPP link to router 2210C (NN).

8 Configure the node-level parameters including the router's network ID and CP name.

9 This parameter corresponds to the ID number part of the node ID. The ID block portion of the node ID is hard coded as 077 for the 2210.

2210 Only

In the level of 2210 code that we used, the value specified using the command line interface was transposed. (The correct value is supplied by the Configuration Program.) This is only a problem if you do not follow our recommendation of using CPNAME to identify the 2210 to VTAM. Apply the fix for APAR NA02999.

The problem does not occur on the 2216.

10 Tune the router's resource usage. This is very important for 2210s with only 8 MB of DRAM.

11 Set global buffers for tuning of an 8-MB router.

3.5.4 HPR Configuration Steps for Router 2210C

These steps show the configuration for the APPN protocol. We have preconfigured the other required parameters including PPP (back-to-back) on interfaces 2 and 3 using RS-232 cables. The general steps in this configuration are:

1. APPN/HPR port configuration in Figure 49 on page 105.
2. APPN/HPR link configuration in Figure 50 on page 107.
3. APPN/HPR node configuration in Figure 51 on page 108.

```
Config>P APPN
APPN user configuration

APPN config>ADD PORT

APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? E   1
Interface number(Default 0): [0]?
Port name (Max 8 characters) [EN000]? ENC1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?   2
 High performance routing: (Y)es (N)o [Y]?   3
 Maximum BTU size (768-1289) [1289]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>ADD PORT

APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? P   4
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [PPP001]? PPPC1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?   4
 Maximum BTU size (768-2048) [2048]?
 Local SAP address (04-EC) [4]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 49 (Part 1 of 2). APPN/HPR Port Configuration for Router C

```
APPN config>ADD PORT

APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? P  5
Interface number(Default 0): [0]? 2
Port name (Max 8 characters) [PPP002]? PPPC2
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?  5
 Maximum BTU size (768-2048) [2048]?
 Local SAP address (04-EC) [4]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 49 (Part 2 of 2). APPN/HPR Port Configuration for Router C

```
APPN config>ADD LINK

APPN Station

Port name for the link station [ ]? PPPC1
Station name (Max 8 characters) [ ]? R2210B   6
 Activate link automatically (Y)es (N)o [Y]?
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0   7
 High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?

Write this record? [Y]?
The record has been written.

APPN config>ADD LINK

APPN Station
Port name for the link station [ ]? PPPC2
Station name (Max 8 characters) [ ]? R2210A   7
 Activate link automatically (Y)es (N)o [Y]?
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 High performance routing: (Y)es (N)o [Y]?   7
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?

The record has been written.
```

Figure 50. APPN/HPR Link Configuration for Router C

```
APPN config>SET NODE   8

Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? USIBMRA
Control point name (Max 8 characters) [  ]? RA2210C
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]? 2210C   9
Write this record? [Y]?

The record has been written.

APPN config>SET TUNING   10

Manual tuning
 WARNING!! These changes require a router reboot to take affect.
 Max. shared memory(1024-40960 KB) [4096]? 1792
 WARNING!! If DRAM is 8 Meg, GLOBAL-BUFFERS must not exceed 50,
nor max cashed directory entries exceed 200.
 Percent buffer memory(10-50) [13]? 17
 Max. cached directory entries(10-65535) [4000]? 200
Write this record? [Y]?

The record has been written.
```

Figure 51 (Part 1 of 2). APPN/HPR Link Configuration for Router C

```
APPN config>LIST ALL
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210C
 XID: 00000
 APPN ENABLED: YES
 MAX SHARED MEMORY: 1792
 MAX CACHED: 200
DLUR:
 DLUR ENABLED: NO
 PRIMARY DLUS NAME:
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ---------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 --------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 -----------------------------------------------------
     0       ENC1   ETHERAND    YES      YES      YES
     1      PPPC1        PPP    YES      YES      YES
     2      PPPC2        PPP    YES      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
   R2210B    PPPC1    000000000000       YES     YES       0
   R2210A    PPPC2    000000000000       YES     YES       0

LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------

APPN config>EXIT

Config>SET GLOBAL  11
What is the maximum number of global packet buffers [0]? 50
Number of global packet buffers has been updated successfully

*RESTART
Are you sure you want to restart the gateway? (Yes or [No]): YES
```

Figure 51 (Part 2 of 2). APPN/HPR Link Configuration for Router C

Notes:

1. Configure the token-ring port (interface 0) for HPR.

2. Service any node means that this port will accept all requests for connection. If you want added security by ensuring that only authorized stations use this network node, specify No for this parameter. You then have to define explicit links to the authorized station).

3. Enable HPR on this port.

4. Add and enable HPR on the PPP port at interface 1.

5. Add and enable HPR on the PPP port at interface 2.

6. Add and configure the PPP link to router 2210B (NN).

7. Add and configure the PPP link to router 2210A (NN).

8. Configure the node-level parameters including the router's network ID and CP name.

9. This parameter corresponds to the ID number part of the node ID. The ID block portion of the node ID is hard coded as 077 for the 2210.

2210 Only

In the level of 2210 code that we used, the value specified using the command line interface was transposed. (The correct value is supplied by the Configuration Program.) This is only a problem if you do not follow our recommendation of using CPNAME to identify the 2210 to VTAM. Apply the fix for APAR NA02999.

The problem does not occur on the 2216.

10. Tune the router's resource usage. This is very important for 2210s with only 8 MB of DRAM.

11. Global buffers tuning for an 8 MB router.

3.5.5 HPR Monitoring and Testing

To see the APPN/HPR connectivity, we used the APPN monitor commands on the router. We also tested the network by using the end nodes on the remote and local LANs.

3.5.5.1 2210A Link and Session Information

The APPN monitor information for 2210A is shown in Figure 52 on page 111. From the link information, we can see the active HPR connections to the B and C routers and the defined ENs. The monitor commands also allow us to look at CP-CP sessions, ISR sessions, and RTP sessions.

```
*t 5
+p appn
APPN >list links
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=============================================================================
  R2210C       PPPA2    2    USIBMRA.RA2210C    NN    ACTIVE     ACT_LS
  R2210B        FRA1    1    USIBMRA.RA2210B    NN    ACTIVE     ACT_LS
 WSO5112       TKRA1    0    USIBMRA.WSO5112    EN  INACTIVE     ACT_LS
     RAK       TKRA1    0        USIBMRA.RAK    NN    ACTIVE     ACT_LS


A APPN >list cp-cp_sessions
           CP Name      Type    Status  Connwiner ID    Conloser ID
=============================================================================
       USIBMRA.RAK       NN     Active    D37AE6C1        D37AE6BF
   USIBMRA.RA2210C       NN     Active    D37AE747        D37AE746
   USIBMRA.RA2210B       NN     Active    D37AE6A4        D37AE6A2


A APPN >list isr_sessions

  Adjacent CP Name  TG Number   ISR Sessions
================================================
       USIBMRA.RAK      15              0
   USIBMRA.WSO5112      0              0


A APPN >list rtp_sessions
RTP CONNECTION TABLE:
  TCID             CP Name  ISR  APPC  Pathswitch    Alive    COS TPF   TG Number
=================================================================================
3176CC08   USIBMRA.RA2210C    0    2    00000708  00000708    CPSVCMG      16
3176B0D8   USIBMRA.RA2210B    0    0    00000000  00000708     RSETUP      15
316AAB88   USIBMRA.RA2210B    0    2    00000708  00000708    CPSVCMG      15
```

Figure 52. APPN/HPR Monitor for Router A

3.5.5.2 2210B Link Information

The APPN monitor information for 2210B is shown in Figure 53. From the link information, we can see the active HPR connections to the A and C routers and the Communications Server client on the remote token-ring LAN.

```
APPN >list links
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=============================================================================
     @@0       TKRB1    0    USIBMRA.WSO560O    EN    ACTIVE     ACT_LS
  R2210C       PPPB2    2    USIBMRA.RA2210C    NN    ACTIVE     ACT_LS
  R2210A        FRB1    1    USIBMRA.RA2210A    NN    ACTIVE     ACT_LS
```

Figure 53. APPN/HPR Monitor for Router B

3.5.5.3 2210C Link Information

For router 2210C, the active HPR links go to the A and B routers and to the Communications Server client on the remote Ethernet LAN.

```
APPN >list links
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=========================================================================
     @@0       TKRC1    0    USIBMRA.WS05241    EN    ACTIVE     ACT_LS
  R2210A       PPPC2    2    USIBMRA.RA2210A    NN    ACTIVE     ACT_LS
  R2210B       PPPC1    1    USIBMRA.RA2210B    NN    ACTIVE     ACT_LS
```

Figure 54. APPN/HPR Monitor for Router C

3.5.5.4 HPR Connection Test: Token-Ring to Frame Relay to Token-Ring

To test HPR between the routers, we used the APPC APING utility under the CS/2 client software. APING was successful from PC EN to PC EN and from PC EN to VTAM NN. Below is a sample OS/2 APING result from WS05600 (the PC in 2210B's token-ring) to WS05112, the Communications Server Windows client (the PC in 2210A's token-ring).

```
Token-Ring PC.
c:\>aping usibmra.ws05112

IBM APING version 2.43.3c  APPC echo test with timings.
Licensed Materials - Property of IBM
(C) Copyright 1994,1995 by IBM Corp. All rights reserved.

Allocate duration:                          250 ms
Program startup and Confirm duration:       375 ms

Connected to a partner running on: Windows
        Duration        Data Sent        Data Rate        Data Rate
        (msec)          (bytes)          (KB/s)           (Mb/s)
        --------        ---------        ---------        ---------
              63              200              3.1            0.025
              93              200              2.1            0.017
Totals:      156              400              2.5            0.020
Duration statistics:   Min = 63   Ave = 78   Max = 93
```

Figure 55. APING Test from the Remote Token-Ring PC to the Local

We have also displayed the HPR connections as seen by WS05600 (PC in 2210B's token-ring) using the CMCONNS (or HPRCONNS) command. This Communications Server utility allows us to see the end-to-end HPR connections.

```
c:\>cmconns
CMCONNS: DISPLAY HPR CONNECTIONS  to/from  USIBMRA.WS0560O
TCID (Transport Connection Identifier): 11A
Class Of Service:                       #INTER
Local RTP NCE:                          80
Partner RTP NCE:                        8280
Active Outbound Sessions:               1,0

 RTP      USIBMRA.WS0560O
  |
  |
 ANR      RA2210B 21
  |
  |
 RTP      USIBMRA.RA2210A 21
```

Figure 56. HPR Connections from the Remote Token-Ring Workstation

3.5.5.5 HPR Reroute

To invoke HPR's nondisruptive rerouting capability, we broke the frame-relay link between 2210A and 2210B while an APING session was in progress. The APING between 2210B and 2210A was still successful, and from the CMCONNS display on the OS/2 workstation, we can see the new route bypassing the frame-relay link from 2210A to 2210B. The new route now uses the PPP link to 2210C before reaching 2210A.

```
c:\>cmconns
CMCONNS: DISPLAY HPR CONNECTIONS  to/from  USIBMRA.WS0560O
TCID (Transport Connection Identifier): 11A
Class Of Service:                       #INTER
Local RTP NCE:                          80
Partner RTP NCE:                        8280
Active Outbound Sessions:               1,1

 RTP      USIBMRA.WS0560O
  |
  |
 ANR      RA2210B 21
  |
  |
 ANR      RA2210C 21
  |
  |
 RTP      USIBMRA.RA2210A 21
```

Figure 57. HPR Connections during Re-Route

3.5.5.6 HPR Connection: Ethernet to PPP to Token-Ring

We also tested HPR from the Ethernet LAN of 2210C to the token-ring LAN of 2210B. Below is the APING result from WS05241 (the PC connected to 2210C's Ethernet) to WS05600 (the PC connected to 2210B's token-ring).

```
IBM APING version 2.43.3c  APPC echo test with timings.
Licensed Materials - Property of IBM
(C) Copyright 1994,1995 by IBM Corp. All rights reserved.

Allocate duration:                          250 ms
Program startup and Confirm duration:      1563 ms

Connected to a partner running on: OS/2
        Duration        Data Sent        Data Rate        Data Rate
        (msec)          (bytes)          (KB/s)           (Mb/s)
        --------        ---------        ---------        ---------
              62              200              3.2            0.025
              94              200              2.1            0.017
Totals:      156              400              2.5            0.020
Duration statistics:   Min = 62   Ave = 78   Max = 94
```

Figure 58. APING Test from the Remote Ethernet Workstation

```
CMCONNS: DISPLAY HPR CONNECTIONS  to/from  USIBMRA.WSO5241
TCID (Transport Connection Identifier): 110
Class Of Service:                       #INTER
Local RTP NCE:                          80
Partner RTP NCE:                        80
Active Outbound Sessions:               1,0

 RTP      USIBMRA.WSO5241
  |
 ANR      RA2210C 21
  |
 ANR      RA2210B 21
  |
 RTP      USIBMRA.WSO560O 21
_____________________________________________________________
TCID (Transport Connection Identifier): 10B
Class Of Service:                       SNASVCMG
Local RTP NCE:                          80
Partner RTP NCE:                        80
Active Outbound Sessions:               1,24

 RTP      USIBMRA.WSO5241
  |
 ANR      RA2210C 21
  |
 ANR      RA2210B 21
  |
 RTP      USIBMRA.WSO560O 21
_____________________________________________________________
TCID (Transport Connection Identifier): 107
Class Of Service:                       #INTER
Local RTP NCE:                          80
Partner RTP NCE:                        8280
Active Outbound Sessions:               1,18

 RTP      USIBMRA.WSO5241
  |
 ANR      RA2210C 21
  |
 RTP      USIBMRA.RA2210A 21
_____________________________________________________________
TCID (Transport Connection Identifier): 106
Class Of Service:                       SNASVCMG
Local RTP NCE:                          80
Partner RTP NCE:                        8280
Active Outbound Sessions:               1,18

 RTP      USIBMRA.WSO5241
  |
 ANR      RA2210C 21
  |
 RTP      USIBMRA.RA2210A 21
```

Figure 59. HPR Connections from the Remote Ethernet Workstation

Chapter 4. More Advanced APPN Configuration Options

The previous chapter explained how to configure and activate basic APPN capability on the router. However, in a real network, you will need to configure some of the optional APPN capabilities or change some of the default parameter values. This chapter explains why this may be necessary, and gives examples of how to do it. The topics have been divided into three categories:

- Common configuration options

  One or more of these APPN functions or parameter value changes will be used in most networks.

- Fine adjustments

  These are options or parameter value changes that may be used to improve performance or efficiency. They may be appropriate in any network.

- Advanced configuration

  These APPN functions or parameter value changes are less likely to be used in the typical network, and may need a higher level of APPN knowledge in order to exploit correctly.

Note: This chapter provides brief explanations of a number of APPN functions and options. For a more complete explanation of these, see the *APPN Architecture and Product Implementations Tutorial*.

4.1 Configuration Changes That Require the APPN Function to Restart

The majority of the APPN configuration changes that you make once the router is operational as an APPN node can be implemented dynamically without needing to disrupt APPN processing. However, certain changes do require a restart of APPN, and you should keep these in mind when planning configuration changes.

The particular parameter changes that require an APPN restart are:

- Network ID of the network node
- Control point name of the network node
- XID number (of the network node) for subarea connection
- Adjacent node type (of a link station)
- Any parameters under the following options:
  - High-Performance Routing (HPR) at the node level
  - Dependent LU Requester (DLUR) at the node level
  - Connection network
  - Class of service
  - Mode name mappings
  - Node tuning
  - Node management

All other APPN configuration changes may be made dynamically.

4.2 Common Configuration Options

You will almost certainly need to use one or more of these options or parameter value changes in your network in order to provide the function required. Assess the relevance of each to your particular network.

4.2.1 Enabling DLUR

DLUR is required if you want dependent LUs in adjacent nodes (that do not themselves provide DLUR capability) to use the router as their entry to the APPN network. Many implementations will require DLUR in one or more routers. See 5.1, “Dependent LU Requester” on page 139 for a complete explanation of how to configure DLUR.

4.2.2 Exploiting Connection Networks

If LANs are to be used for APPN connections to other nodes, then in most cases you should use connection networks on those LANs.

4.2.2.1 Why Are Connection Networks Useful?

A connection network is an APPN technique for significantly reducing the definition effort required on LANs when there is a significant use of peer-to-peer communication between nodes on the same LAN. For a more in-depth explanation of why connection networks are beneficial and an overview of the architectural concepts, see 2.2.2.3, “APPN Connection Network” on page 19.

4.2.2.2 Configuring Connection Networks

For APPN nodes to participate in a connection network, from an architectural perspective they need to define a link to the Virtual Routing Node (VRN) that represents a particular connection network. That is not the way it is normally configured on most APPN implementations, and the router is no different.

Having defined a LAN port, then the configuration process involves adding the particular LAN port to a named connection network. See Figure 60 on page 119 for an example of how to do this.

The connection network name is required. This is the network qualified name of the particular connection network. The same name is used on all nodes for the LAN ports that are to participate in the particular connection network. Different LAN ports on the router may belong to different connection networks, and more than one port may belong to the same connection network.

The network ID of the connection network must be the same as that of the router control point. Let the other parameters default at this stage.

```
APPN config>add connection-network
APPN Connection Networks
Fully-qualified connection network name (netID.CNname) []? usibmra.cna
Port Type: (E)thernet, (T)okenRing []? t
  Limited resource timer for HPR (1-2160000 seconds) [180]?
Edit TG Characteristics: (Y)es (N)o [N]?
APPN Connection Networks Port Interface
Port name [ ]? tkra1                                          1
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 60. Adding a LAN Port to a Connection Network

Note:

1 This is a previously defined LAN port.

4.2.3 Defining Independent LUs Located at LEN Nodes

If some of the SNA nodes connecting to the router contain *independent* LUs, but those nodes only implement LEN rather than APPN, then it may be necessary to define the location of those LUs to the router. If you will be connecting LEN nodes, then review the following to see whether LEN definitions are required in your case.

4.2.3.1 Why Are LEN LU Definitions Required?

When a LEN node connects to an APPN network node, there are no CP-CP sessions between the NN and the LEN node. As a result, if an independent LU on the LEN node is to be the target of a session initiation request, then there is no way for the router NN to know that the ILU is located at the LEN node unless it previously discovered the location of that ILU.

It may already know that the ILU resides at the LEN node for various reasons:

- The ILU is also the CP of the LEN node. This name is discovered as part of the XID3 interchange that occurs at connection initiation.
- The router previously received a session initiation request (BIND) on behalf of that ILU, and the location of the ILU has been retained in the directory cache on the router.

If neither of these apply, then predefinition is required at the router to tell it where to find the ILU. Unless you are sure that an ILU that is not the CP of a LEN node *always* initiates the first session with any partner, then it is necessary to use predefinition in the router. To know whether or not the ILU always starts the first session depends on an understanding of how the software in use on the LEN node initiates application-to-application communication.

4.2.3.2 Configuring LEN LUs

If one or more ILUs at a LEN node require to be predefined in the router, then see Figure 61 on page 120 for an example of how to do this. Before you can define ILU names on the router, you must define a station to represent the connection to the LEN node, even if the LEN node is always responsible for (re-)initiating the connection to the router.

If there are a number of ILUs at a LEN node with names that begin with the same character sequence, then it is possible to represent multiple ILUs by a single definition using the wildcard character '*' following the common part of the name. Such an entry in the APPN directory is referred to as a *partial wildcard*. In order to use a partial wildcard, a suitable LU naming convention must be in use because the partial name must be unique to the particular LEN node.

There is also a concept within APPN of a *full wildcard*, where the whole of the LU name is represented by the wildcard character. However, there *must* only be *one* full wildcard in the whole of the APPN network, or strange results will occur (and alerts will be produced). So, we recommend you avoid using a full wildcard, even though the router allows one to be defined.

The following additional information is required:

Independent LU name
This is the network qualified name of an ILU that is located at the LEN node. There may be more than one such ILU at a particular LEN node.

The network ID of the LEN node will typically be the same as that of the router, but it can be different.

The LU part of the name can be the complete name, or one or more initial characters followed by the wildcard character.

Station name
This is the name of the station that defines the connection from the router to the LEN node.

This is a required value, and means that a station to represent the connection from the router to the LEN node has to be defined before the ILU names can be added to the router configuration. See Chapter 6, "APPN Data Link Controls" on page 159 for the information required to define stations on the various types of DLC.

```
APPN config>add lu-name
LEN End Node LU Names
  Fully-qualified LU name []? usibmra.lena1              1
  Station name []? lena                                  2
Write this record? [Y]?
The record has been written.
APPN config>

APPN config>add lu-name
LEN End Node LU Names
  Fully-qualified LU name []? usibmra.lenb*              3
  Station name []? lenb
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 61. Defining an Independent LU on a LEN Node

Notes:

1. This is the name of an independent LU that is located at the adjacent LEN node (or is accessible via the adjacent LEN node).
2. This is a previously defined link-station.
2. This is an example of a partial wildcard definition.

4.2.4 Defining Additional Mode to COS Mapping

If the router is an intermediate node for sessions from independent LUs in adjacent LEN or APPN end nodes, then it may be necessary for you to define additional mode (name) to COS (name) mapping in the router. You should review the following to assess whether this is required in your network.

4.2.4.1 Why Is Mode to COS Mapping Required?

When the router is acting as a network node server (NN) for attached end nodes or LEN nodes, and it receives a session initiation request from an independent LU in the attached node, the session request may or may not include the name of the requested COS. If there is no COS name in the request, the router will attempt mode to COS mapping.

If the session initiation request contains a mode, then the mode is used as the input to mode to COS mapping. However, if there is no requested mode, 'BLANK' (eight blank characters) is used for the mode name. Similarly, if the requested mode is not contained in the mapping table, the entry for 'BLANK' is used. Note that in either of these cases, the priority and COS used may not be as you desire.

By default, mode to COS mapping is provided for the architected modes, as shown in Table 4. Non-architected modes are often used for independent LUs, and mappings for these may have to be defined in some cases, particularly for attached LEN nodes. However, many APPN EN implementations do this mapping themselves.

Notes:

1. The router *only* does mode to COS mapping when it is acting as a network node server (NN) for a session initiation request.
2. Mappings for sessions with dependent LUs are *not* required in the router.
3. We recommended that you start to use the architected modes where possible when setting up additional ILU to ILU communication.

Table 4 also lists the pacing window values associated with the default (architected) modes and the transmission priorities associated with the COSs to which they are mapped.

Table 4. Default Mode to APPN COS Mappings

Mode	Pacing	COS	Priority
'BLANK'	3	#CONNECT	Medium
#BATCH	3	#BATCH	Low
#BATCHSC	3	#BATCHSC	Low
#INTER	7	#INTER	High
#INTERSC	7	#INTERSC	High

Notes:

1. If no mode name is specified, or the mode specified is not in the table, then the 'BLANK' entry is used.
2. The character '#' represents the hexadecimal value '7B'.
3. Internally, support is also provided for the control modes CPSVCMG, which maps to a COS of CPSVCMG, and CPSVCMGR and SNASVCMG, both of which map to a COS of SNASVCMG. The network transmission priority is used for these control COSs.

4.2.4.2 Configuring a Mode to COS Mapping Table Entry

An example of adding a new mode to COS mapping entry is shown in Figure 62.

The following additional information is required:

Mode name — This is the new mode that is to be added to the router mapping table.

COS name — This is the existing COS to which the mode is to be mapped. It must be one of the default architected COSs, or a user COS that has been added to the router.

We strongly recommend the use of the architected COSs unless the use of a special COS cannot be avoided. See 4.4.1, "Adding Non-Standard COSs" on page 138 for more information.

Pacing window size — Unless you have a specific value in mind, set the pacing window size according to the transmission priority associated with the COS, using the values shown in Table 4 on page 121.

```
APPN config>add mode
 Mode name [ ]? user1                                    1
 COS name [ ]? #inter                                    2
 Session-level pacing window size (1-63) [7]?            3
 Write this record? [Y]? y
 The record has been written.
APPN config>
```

Figure 62. Adding a Mode to COS Mapping Table Entry

Notes:

1. This is the mode to be mapped.
2. This is the COS to which it is to be mapped.
3. This is the pacing window value.

4.2.5 Using CP-CP Session Security

If you want to be more certain that APPN nodes that connect to the router are who they say they are, then use CP-CP session security.

4.2.5.1 Why Use CP-CP Session Security?

Even if you restrict the nodes that may connect to a particular port (see 3.2.3, “Limiting Connections to Defined Nodes Only” on page 43), this may not be considered particularly secure. CP-CP session security provides enhanced security by exploiting the LU 6.2 session security function for CP-CP sessions. This uses a single (secret) 64-bit encryption key that is known to both nodes, but is not transferred over the network connection between them. At CP-CP session initiation, each node chooses a random number, sends it to the partner, which then encrypts it and returns the result for validation. It is only possible to start CP-CP sessions if both nodes know the same key.

There has been an enhancement to the original protocol used for this interchange, and this is referred to as enhanced session security. The enhanced protocol is similar to the basic one, but the encrypted data exchanged is derived from more variables. The router supports this improved protocol, and it is used automatically if the adjacent node also supports it. The use of the enhanced protocol may be forced, if required, and if the adjacent node does not support it, CP-CP session initiation is not possible.

4.2.5.2 Configuring CP-CP Session Security

The example in Figure 63 on page 124 shows how to enable CP-CP session security for a particular adjacent node.

The following additional information is required:

Adjacent CP name — The network qualified CP name of the adjacent node.

Encryption key — This is the hexadecimal representation of the 64-bit encryption key that is defined in both nodes.

Enhanced session security? — Does the partner node support the enhanced session security protocol? If it does, then use of the enhanced protocol is negotiated and agreed, whatever the setting of this parameter. Alternatively, it is possible to force the use of the enhanced protocol, in which case CP-CP session initiation fails if the adjacent node does not support it.

```
APPN config>add link-station
APPN Station
 Port name for the link station [ ]? tkra1
 Station name (Max 8 characters) [ ]? ws05600
 Activate link automatically (Y)es (N)o [Y]? y
 MAC address of adjacent node [000000000000]? 400052005600
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node, 3 = PU 2.0 node [1]? 1
 High performance routing: (Y)es (N)o [Y]?
 Edit Dependent LU Server: (Y)es (N)o [N]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]? y                          1
 Encryption key(16 hex digits) [0000000000000000]? 2345543212345678      2
   Use enhanced session security only (Y)es (N)o [N]? y                  3
 Fully-qualified CP name of adj node (netID.CPname) []? usibmra.ws05600  4
 Edit TG Characteristics: (Y)es (N)o [N]?
 Edit LLC Characteristics: (Y)es (N)o [N]?
 Edit HPR defaults: (Y)es (N)o [N]?
 Write this record? [Y]? y
The record has been written.
APPN config>
```

Figure 63. Enabling CP-CP Session Security for an Adjacent Node (Token-Ring)

Notes:

1. This ensures CP-CP session security is enabled with this station.
2. This is the 64-bit key that is defined in both nodes.
3. Enabling this option forces the use of the enhanced protocol.
4. The CP name of the adjacent node is required. This node must be an APPN network node or end node, as CP-CP sessions are not possible with LEN or PU 2.0 nodes.

4.2.6 Adjusting the APPN Memory for Network Size

You need to review the amount of memory allocated to APPN in the light of your planned use and network size, and the memory size of the router. As a result, it may be necessary to adjust the amount of shared memory that is used for APPN.

4.2.6.1 Why Is Storage Tuning Required?

APPN uses shared memory to contain the control blocks required to represent connections to adjacent nodes and the resources they contain, any active ISR sessions, the directory cache, any collected session data, and the buffer space required to handle message traffic. You probably need to change the size of this storage to reflect your network, particularly if the network size is greater than the intermediate size assumed by default, or if you are using a 2210 with limited memory.

The maximum amount of APPN shared memory is 26000 KB for the 2210 and 40960 KB for the 2216. Note that the 2216 software level that we used limited it to 26000, but that was changed to the higher value before the General Availability date. The new upper limit can be used via the command line interface, but the matching Configuration Program update was not available at General Availability.

Once APPN is started, you can display how much shared memory it is using, and this provides additional input into your tuning decisions. See 7.1.3.7, “Memory Use” on page 206 for more information on how to do this.

4.2.6.2 Changing the Memory Used by APPN

The amount of shared memory used by APPN can be changed as shown in Figure 64 on page 126, but how do you know what size to allocate? The Configuration Program provides a tuning function that *estimates* the requirement, based on the inputs shown in Table 5. The window for this function is shown in the APPN Node Tunning screen.

It is important to realize that the tuning function only provides an estimate; the actual memory required at any instant of time will depend on many factors. The inputs into the tuning algorithm fall into three categories: the number of adjacent nodes, the number of ISR sessions to be handled concurrently and the size of the network topology database.

Table 5. Inputs to Memory Sizing Algorithm

Variable	Explanation	Increment [1]
Maximum number of sessions	This is the maximum number of concurrent ISR sessions that the router is expected to support. Do not include sessions that use ANR routing.	3.86
Percent of sessions with HPR data connections	This is the percentage of the ISR sessions for which the router acts as an ISR to HPR conversion node.	0.001
Percent of sessions serving DLUR LUs	This is the percentage of ISR sessions handled by DLUR on the router.	0.0
Maximum number of adjacent nodes	This is the maximum number of adjacent SNA nodes (all types) to which the router is expected to connect concurrently.	21.91
Percent HPR nodes with CP-CP sessions	This is the percentage of adjacent nodes that use CP-CP sessions over HPR.	4.19
Percent of adjacent nodes as DLUR PUs	This is the percentage of adjacent nodes for which the router provides DLUR support.	0.41
Maximum network nodes with same network ID	This is to allow for the network node entries in the network topology database, and needs to allow for all the network nodes in the APPN topology subnetwork.	1.91
Maximum TGs connecting NNs with same network ID	This is to allow for the TG entries in the network topology database, and needs to allow for all the TGs between the network nodes in the APPN topology subnetwork.	0.39

Note:

[1] This column contains the *approximate* storage increment in KB for each resource of that type. These increments were produced by experimenting with the MRS and MAS Configuration Programs at the level available at the time the content for this volume was produced.

For the percentage variables, *add* these increments to the base requirement for that resource type for the resources for which the option applies.

The output from the tuning algorithm and the input required for the process shown in Figure 64 on page 126 are:

Maximum shared memory The amount of shared memory to be used by APPN.

Percent buffer memory The percentage of the APPN shared memory that is to be reserved for data buffering.

Maximum directory entries The maximum number of APPN directory entries that the router can retain in its directory cache. If the cache overflows, the oldest entries are discarded. The only implication of discarding entries is that a subsequent session initiation request for an LU that is not in the cache will result in a directed search to a central directory server, if there is one, or a broadcast search. So, the size needs to reflect the number of partner LUs for LUs served by this network node, and is obviously affected by the network size. The default value is probably high for many networks.

You should use the Configuration Program to calculate appropriate values, even if you then set the values via the command line interface.

```
APPN config>set tuning
 Manual tuning
   WARNING!! These changes require a router reboot to take affect.
   Max. shared memory(1280-26000 KB) [5108]? 8400                    1
   Percent buffer memory(10-50) [11]? 15                             2
   Max. cached directory entries(0-65535) [4000]? 2000               3
 Write this record? [Y]? y
The record has been written.
APPN config>
```

Figure 64. Modifying the Storage Used by APPN

Notes:

1. This sets the shared memory size.

   2216 Only

   By the General Availability date, the maximum value for the 2216 had been increased to 40960.

2. This reserves a percentage of the shared memory for buffering message data that is in transit through the router.

3. This sets the limit for the number of APPN directory cache entries.

4.3 Fine Adjustments

It may be desirable to change some of the default values to improve the efficiency or performance of the APPN function on the router. This section covers some of the more common areas where this applies.

4.3.1 Using Topology Safe Store

2216 Only

The 2210 does not implement topology safe store.

Once a 2216 goes into production, you should enable topology safe store.

4.3.1.1 Why Is Topology Safe Store Useful?

When a network node restarts, it resynchronizes its view of the network topology with adjacent network nodes. If it has no existing knowledge of the network topology at that time, then each adjacent network node sends it the whole of the network topology database. However, with topology safe store, the router reloads previously known information, and then resynchronizes with each neighbor, such that it only receives the updates since the topology checkpoint was taken. This can reduce the amount of topology data that flows on restart, particularly in a large network, and also speeds up restart.

The other advantage is that the age of entries in the topology database is retained over restarts rather than being reset to 15 days every time it receives them again at each restart. This makes it more likely that garbage entries get deleted over time, and less likely that they are propagated to other nodes.

Once any initial trial and error testing is over, we suggest that this option be enabled so that the router has a better chance to allow unrefreshed entries to expire.

4.3.1.2 Enabling Topology Safe Store

To enable topology safe store, use the sequence shown in Figure 65 on page 128. By default, the topology is saved every 100 updates, but the frequency can be changed by using the Configuration Program (but not via the command line interface).

If topology safe store is enabled, and invalid or obsolete entries appear in the network topology database, then it is necessary to restart APPN with topology safe store disabled to clear out such entries.

```
APPN config>set management
Node Management
  Collect intermediate session information (Y)es (N)o [N]?
  Save RSCV information for intermediate sessions (Y)es (N)o [N]?
  Create intermediate session records (Y)es (N)o [N]?
  Record creation thresholds(0-4294967) [0]?
Recording media
Memory (Y)es (N)o [N]?
Topology safe store
  Maintain backup copy of topology database (Y)es (N)o [N]? y        1
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 65. Enabling Topology Safe Store

Note:

1 This enables topology safe store.

4.3.2 Using Limited Resource Links

Once established, APPN connections are normally maintained until they fail. This may not be appropriate if you use switched circuits, and if this is the case, review the relevance of using limited resource links in your network.

The limited resource capability can only be used for dial-on-demand link types, which are:

- PPP over ISDN or V.25 bis
- Frame relay over ISDN
- X.25 (QLLC) SVC

Links initiated using connection network techniques are automatically set to be limited resource links.

For more information on dial-on-demand circuits, see the *Software User's Guide*.

4.3.2.1 Why Are Limited Resource Links Useful?

A limited resource link is a connection that is established on demand, and is then disconnected once the session count reduces to zero. One use of limited resource links is to provide an alternative higher bandwidth switched connection (or perhaps just a separate connection) for infrequent file transfers when the primary connection is low speed.

PU 2.1 Node Considerations: When configuring an APPN link station for PU 2.1 nodes over a dial-on-demand link, you should specify yes for the limited resource link station parameter. This allows APPN to:

- Consider this link as a viable link to be used for route computation, even though the link is not actually active. The link will automatically be activated during LU-LU session activation if a session needs to use it.
- Deactivate the link station when there are no active sessions using the link.

You should disable CP-CP sessions over a dial-on-demand link. CP-CP sessions are persistent sessions. That is, they should remain active as long as the link is active. Since the active session count will not go to zero in this case, the link will remain active.

Since CP-CP sessions are not normally used on a limited resource link, there needs to be some other permanent connection with the node if it is an APPN node. To cause the initiation of a limited resource link connection, it is necessary for APPN route selection to choose the limited resource link as the route to (or through) the adjacent node. Careful use of the APPN class of service (COS) mechanism and the setting of non-default TG characteristics for the link may be necessary to achieve this.

Note: If you specify yes for the limited resource parameter for an APPN node, you must specify an adjacent CPNAME and a TG number in the range of 1 to 20.

PU 2.0 Node Considerations: When configuring a link station for PU 2.0 nodes over a dial-on-demand link, you can specify yes limited resource link station parameter. This allows APPN to deactivate the link station when there are no active sessions using it.

Note: If limited resource is enabled, link activation for this link station must be initiated by either the DSPU (the PU 2.0) or by VTAM.

Considerations When Using DLUR for T2.0 or T2.1 Devices: For T2.0 or T2.1 nodes utilizing DLUR for dependent session traffic, an SSCP-PU and an SSCP-LU session must be active in order to establish an LU-LU session. These sessions are included in the session count for the link to the DSPU. Therefore, if limited resource is set to yes, the link will remain active as long as the SSCP-PU session is active or LU-LU sessions are active over this link. Use the DISCNT parameter in the VTAM switched node definition to control when VTAM terminates the SSCP-PU and SSCP-LU sessions.

If you specify no for the limited resource parameter, link deactivation is controlled by the node that initiated the connection.

If the link to the DSPU was activated due to the DSPU calling into the DLUR node or the DLUR node calling out to the DSPU (that is, the link station to the DSPU has been configured in the router and activate link automatically is set to yes), when the active session count goes to zero the link is deactivated by APPN DLUR only if the DSPU requested DACTPU. In this case, if the DLUS sends a DACTPU request to DLUR, DLUR will deactivate the SSCP-PU session. However, it will not deactivate the link to the DSPU. DLUR will attempt to re-establish the SSCP-PU session to the DLUS or the backup DLUS until it is successful or until the DSPU no longer needs this session.

If the link to the DSPU was activated by the DLUS and the session count goes to zero, the link is deactivated by APPN DLUR only if the DLUS sends a DACTPU request to DLUR.

4.3.2.2 Enabling Limited Resources

Limited resource link is one of the characteristics that may be assigned at both port and station level. Enabling it at the port level sets the default for stations using that port but this may be overridden at the station level.

Figure 66 on page 130 and Figure 67 on page 130 provide examples of configuring limited resource links.

```
APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [  ] ? p
Interface number(Default 0): [0 ] ? 9
Port name (Max 8 characters) [PPP009 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
 Service any node: (Y)es (N)o [Y ] ?
 Limited resource: (Y)es (N)o [Y ] ?                          1
 High performance routing: (Y)es (N)o [Y ] ?
 Maximum BTU size (768-2044) [2044 ] ?
 Local SAP address (04-EC) [4 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>
```

Figure 66. Enabling Limited Resources on a Port (PPP)

Note:

1 Use this to set limited resource for dial-on-demand links. It is the default in this case because the underlying interface is dial-on-demand.

```
APPN config>add link-station
APPN Station
Port name for the link station [ ] ? ppp009
Station name (Max 8 characters) [ ] ? to15dod
 Limited resource: (Y)es (N)o [Y] ?                                    1
 TG Number (1-20) [1] ?                                                2
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node [0] ?
 High performance routing: (Y)es (N)o [Y] ?
 Allow CP-CP sessions on this link (Y)es (N)o [Y] ? N                   3
Fully-qualified CP name of adj node (netID.CPname) [] ? usibmra.ws05603 4
Edit TG Characteristics: (Y)es (N)o [N] ?
Edit LLC Characteristics: (Y)es (N)o [N] ?
Edit HPR defaults: (Y)es (N)o [N] ?
Write this record? [Y] ?
The record has been written.
APPN config>
```

Figure 67. Setting Limited Resource for a Station

Notes:

1 This enables limited resource. The default is taken from the port setting.

2 A TG number is required for a limited resource connection to an APPN node.

3 CP-CP sessions should be disallowed. If not, then they may become established over the limited resource connection because of a failure elsewhere in the network. If they do become established over the link, the active session count will never drop to zero, and the connection will be maintained permanently.

4 The name of the adjacent node is required so that an entry can be built in the topology database *before* the connection is initiated. The link then becomes eligible for APPN route selection, and the connection will be made dynamically if it is chosen for a session.

4.3.3 Modifying the TG Characteristics

Although the defaults for the APPN TG characteristics are sensible, they may not be set to optimum values for your network. You should review the values in use for each port, and change as appropriate.

4.3.3.1 Why Change the TG Characteristics

The TG characteristics are used in route selection and also in HPR during RTP connection initiation.

If only one route can be selected for a particular session, the TG characteristics do not affect the route chosen. However, if there are alternative routes, it is important that the characteristics reflect the difference (or similarity) in the routes, or undesirable routes may be chosen. The key parameter to get more correct in such cases is the effective capacity. The router assumes defaults according to the port type:

- X‘45’ (64 kbps) for all serial ports (SDLC, frame relay, PPP, or X.25)
- X‘75’ (4 Mbps) for DLSw or 4 Mbps token-ring
- X‘80’ (10 Mbps) for Ethernet
- X‘85’ (16 Mbps) for 16 Mbps token-ring

If required, route selection can be influenced by changing other TG characteristics. However, this should be done only when the theory of COS and route selection is fully understood.

If the TG is used for HPR traffic, the effective capacity also influences the initial rate at which RTP starts sending data on a new RTP connection. If it is set much lower than the actual speed, it may take too long for a short-lived RTP connection that is used for file transfer to achieve the highest possible throughput rate.

Note that when a route is selected through the router, the TG values defined in the router are only used for the TG outbound from the router. In a similar way, the characteristics for the inbound TG are set by the node at the other end of this TG.

4.3.3.2 Changing the TG Characteristics

TG characteristics can be specified at both the port and station levels, with the port values setting the defaults for defined stations and the values used for undefined connections. Figure 68 on page 132 shows an example of modifying the parameter values for a previously defined port.

You should make the effective capacity more accurate if you have any of the following:

- Serial links that are slower than 64 kbps.
- Serial links that are considerably faster than 64 kbps.
- DLSw connections that use physical links that are significantly slower than LAN speeds.

```
APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw []? t
Interface number(Default 0): [0]? 0
Port name (Max 8 characters) [TROOON]? tkra1
WARNING!! You are changing an existing record.
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
  Service any node: (Y)es (N)o [Y]?
  High performance routing: (Y)es (N)o [Y]?
  Maximum BTU size (768-2063) [2048]?
  Maximum number of link stations (1-976) [512]?
  Percent of link stations reserved for incoming calls (0-100) [0]?
  Percent of link stations reserved for outgoing calls (0-100) [0]?
  Local SAP address (04-EC) [4]?
  Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]? y                          1
  Cost per connect time (0-255) [0]?
  Cost per byte (0-255) [0]?
  Security:(0 = Nonsecure 1 = Public Switched Network
    2 = Underground Cable 3 = Secure Conduit 4 = Guarded Conduit
    5 = Encrypted 6 = Guarded Radiation) [0]?
  Propagation delay:(0 = Minimum 1 = Lan 2 = Telephone
    3 = Packet Switched Network 4 = Satellite 5 = Maximum) [1]?
  Effective capacity (0-ff) [75]?                                   2
  First user-defined TG characteristic (0-255) [128]? 50            3
  Second user-defined TG characteristic (0-255) [128]?
  Third user-defined TG characteristic (0-255) [128]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 68. Changing the TG Defaults for a Port (Token-Ring)

Notes:

1. This enables the TG parameters to be changed.
2. If the default value represents a speed very different from the actual speed, then change the effective capacity to reflect the actual speed.
3. Changing this value (or one of the other user-defined characteristics) may be required if user-defined COSs are used.

4.3.4 Changing the LLC Parameters

Although the LLC defaults are sensible, they may not be set to optimum values for your network. You should review the values in use on each port, and change as appropriate.

4.3.4.1 Why Change the LLC Defaults?

The LLC values affect the efficiency of frame transfer across a link and may influence the performance, both response time and throughput, that you achieve. They also affect the duration of error recovery activity before a connection is considered to have failed.

Be cautious when making changes, particularly if your level of understanding of the particular LLC protocol is low.

4.3.4.2 Changing the LLC Parameters

The parameters vary with the LLC type. Figure 69 shows an example of how to specify new values. Note that values may be specified at both the port and individual station level. The port level values are used for undefined inbound connections and as the defaults for any defined stations, while the station level values are used for predefined nodes. In either case, the values that are actually used are negotiated at connection initiation for Type 2.1 nodes (both LEN and APPN), and both nodes influence the values agreed. Typically, the lesser of the values suggested is chosen.

```
APPN config>add link-station
APPN Station
Port name for the link station [ ]? tkra1
Station name (Max 8 characters) [ ]? ws05600
  Activate link automatically (Y)es (N)o [N]? y
  MAC address of adjacent node [000000000000]? 400052005600
  Adjacent node type: 0 = APPN network node,
    1 = APPN end node or Unknown node type
    2 = LEN end node [1]? 1
  High performance routing: (Y)es (N)o [Y]?
  Allow CP-CP sessions on this link (Y)es (N)o [Y]?
  CP-CP session level security (Y)es (N)o [N]?
  Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]? y                          1
  Remote SAP(04-EC) [4]?
  Maximum number of outstanding I-format LPDUs (1-127) [26]? 5
  Receive window size (1-127) [26]? 5
  Inactivity timer(1-254 seconds) [30]? 60
  Reply timer (1-254 half seconds) [2]?
  Maximum number of retransmissions(1-254) [8]?
  Receive acknowledgement timer (1-254 half seconds) [1]?
  Acknowledgements needed to increment working window(1-127) [1]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 69. Changing the LLC Parameters for a Station (Token-Ring)

Note:

1 This allows the values to be modified, in this case from the port level defaults.

4.3.5 Modifying the HPR Parameters

Changing the HPR parameters should only be done with care, but it may be relevant to do so in your particular network.

4.3.5.1 Why Change the HPR Parameter Defaults?

There are a number of reasons why you might wish to change the HPR parameters. Perhaps the most likely parameters you might wish to change are the RTP path switch (timeout) timers.

For example, you may decide that high priority sessions should be terminated in a shorter time than the default (say one minute rather than three), as you do not want interactive users to see no response (other than a session hang) for such a long period.

By the same token, you may decide that low priority sessions, which are typically batch transfers, can afford to wait much longer before being terminated, as no users are directly involved, and a successful path switch, even after such an extended period, eliminates the need to retransmit what may be a considerable volume of data in some cases.

Note

RTP parameters in the router only apply to RTP pipes (connections) that start from the router.

You should only make changes to the router HPR parameters as part of a network-wide policy, because we do not recommend uncoordinated changes at the individual node level.

If you do *reduce* any of the path switch timer defaults, then you should also review the retry counts and timer values at the port (or station) level (for LLC characteristics and HPR defaults, see Figure 69 on page 133 and Figure 71 on page 135). It is important to ensure that a permanent failure of a connection can be detected and reported to the topology database well before the path switch timer ends. Route selection can only select a less optimum (but now the best operative) alternative route if this has happened before a path switch is retried. A path switch is retried at intervals during the path switch timer period.

We suggest that the other HPR parameters be left unchanged.

4.3.5.2 Changing the HPR Parameters

Figure 70 on page 135 shows how to change the values that apply to the whole node. There are other HPR parameters that apply at the port and station level, with the port level defaults being used unless overridden at the individual station level. An example of this is shown in Figure 71 on page 135.

```
APPN config>set hpr
Maximum sessions per HPR connection(1-65535)? [100]? 50
Edit HPR Timer and Retry Options [N]? y
Low transmission priority traffic:
  RTP inactivity timer(1-60min)? [3]?
  Path switch timer(0-7200 seconds)? [180]? 600              1
  Max.RTP retries(0-10)? [6]?
Medium transmission priority traffic:
  RTP inactivity timer(1-60min)? [3]?
  Path switch timer(0-7200 seconds)? [180]?                  1
  Max.RTP retries(0-10)? [6]?
High transmission priority traffic:
  RTP inactivity timer(1-60min)? [3]?
  Path switch timer(0-7200 seconds)? [180]? 90               1
  Max.RTP retries(0-10)? [6]?
Network transmission priority traffic:
  RTP inactivity timer(1-60min)? [3]?
  Path switch timer(0-7200 seconds)? [180]?
  Max.RTP retries(0-10)? [6]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 70. Changing the HPR Parameters for the Node

Note:

1 These are the path switch timer values that it may be appropriate to change, but only do so as part of your network-wide policy.

```
APPN config>add link-station
APPN Station
Port name for the link station [ ]? tkra1
Station name (Max 8 characters) [ ]? ws05600
WARNING!! You are changing an existing record.
  Activate link automatically (Y)es (N)o [Y]?
  MAC address of adjacent node [400052005600]?
  Adjacent node type: 0 = APPN network node,
  1 = APPN end node or Unknown node type
  2 = LEN end node [1]?
  High performance routing: (Y)es (N)o [Y]?
  Allow CP-CP sessions on this link (Y)es (N)o [Y]?
  CP-CP session level security (Y)es (N)o [N]?
  Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]? y                         1
  Inactivity timer override for HPR(1-254 seconds) [2]?
  Reply timer override for HPR(1-254 half seconds) [2]?
  Maximum number of retransmissions for HPR(1-254) [3]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 71. Changing the HPR Parameters for a Station (Token-Ring)

Note:

1 This allows the port or station level defaults to be changed.

4.3.6 Collecting ISR Session Data

By default, the router does not collect or save data about intermediate sessions. You may wish to enable various levels of session data collection.

4.3.6.1 What Session Data Is Available?

Intermediate sessions are LU-LU sessions that pass through the APPN network node, but whose endpoints (origin and destination) lie outside the network node. Information about intermediate sessions is generated by the ISR component in the network node and falls into two categories:

- Intermediate session names and counters
- Route selection control vector (RSCV)

The counters reflect the traffic flowing on the session, and RSCV data is useful for monitoring session routes. If RSCV data is collected, the list session_information command issued at the APPN console uses the RSCV data to display the endpoints of active ISR sessions.

In both cases, you can retrieve the data on active sessions by using SNMP. SNMP can also be used to alter the session information collection parameters dynamically. See the *Software User's Guide* for a list of the MIB variables that control session data collection. Changes in parameter values made via the command line interface or the Configuration Program are only effective after an APPN restart.

Note: This function can use a significant amount of APPN memory. You should configure APPN with the needed memory before you enable the collection of ISR information.

For accounting purposes, you can collect records for intermediate sessions passing through the network node. The records are stored in router memory. SNMP must be used to retrieve data from these accounting records stored in the router's local memory.

To capture this accounting information, enable the creation of records and define how the records should be collected and stored. Each record provides a snapshot of intermediate session activity on the node during a period of time. Records are created when a session ends, or, for long-running sessions, when the data volume on the session reaches a specified threshold. If RSCV information is being saved, RSCV data is included in each data record.

Notes:

1. Data on intermediate session RSCVs is obtained by examining the BIND request used to activate a session between two LUs. Consequently, RSCV data is not collected for sessions that have already been established before enabling collection, because the BIND information for these sessions is not available.
2. Intermediate session data is not collected for sessions using ANR routing through the router, because such sessions are unknown at intermediate HPR nodes. However, if the router provides HPR-to-ISR boundary function, intermediate session data is collected for sessions traversing the boundary.

4.3.6.2 How to Activate ISR Session Data Collection

The process of activating session data collection is illustrated in Figure 72. You should be careful and assess any memory implications before enabling any of these options.

```
APPN config>Set management
Node Management
  Collect intermediate session information (Y)es (N)o [N]? y          1
  Save RSCV information for intermediate sessions (Y)es (N)o [N]? y   2
  Create intermediate session records (Y)es (N)o [N]? y               3
  Record creation thresholds(0-4294967) [0]? 50000                    4
Recording media
Memory (Y)es (N)o [N]? y                                              5
  Maximum memory buffers(0-1) [1]?                                    6
  Maximum memory records per buffer(0-2000) [100]?                    6
  Memory Buffers full (0 = Stop recording 1 = Wrap) [0]?              6
  Memory Record format (0 = ASCII 1 = Binary) [0]?                    7
Topology safe store
  Maintain backup copy of topology database (Y)es (N)o [N]?
Write this record? [y]?
The record has been written.
APPN config>
```

Figure 72. Changing the Session Data Collection Parameters

Notes:

1. This enables the collection of session names and traffic counts. This is enabled implicitly if intermediate session records are to be created.
2. This enables the collection of RSCV information.
3. This enables the collection of session (accounting) records. If the collection of intermediate session information is not enabled, then it is forced implicitly if record collection is enabled.
4. This specifies the session data volume threshold in bytes, which when exceeded causes a record to be created even though the session has not ended.
5. This specifies if the session data records are buffered in router memory.
6. These parameters specify how many session data records are to be buffered in memory, and what is to happen when the buffering space is full.
7. This specifies the format of the data in the accounting records.

4.4 Advanced Configuration

The following options or parameter changes are less likely to be used, but you should assess the necessity to do so in your network. Some of these functions may require you to have a higher APPN skill level in order to select the correct values to be used.

4.4.1 Adding Non-Standard COSs

If at all possible, you should avoid defining non-standard APPN COSs, as they may need to be defined in every network node. However, they can be defined for the router.

4.4.1.1 When Non-Standard COSs Are Required?

Non-standard COSs should only be required if you need to ensure that particular sessions use a route that is not the optimum route for a standard COS, and cannot be made so by changing the TG characteristics of individual links (see 4.3.3, “Modifying the TG Characteristics” on page 131) or the resistance of particular nodes (see 4.4.2, “Changing the Node Resistance”).

Defining user COSs for such purposes requires an extensive understanding of how APPN route selection is done and how APPN COSs are used. This is a *complex* area, to be avoided if possible.

4.4.1.2 Creating Non-Standard COS Definitions

User COS tables cannot be defined through the command line interface; you must use the Configuration Program to define a user COS. If you do create a user COS, you select an IBM defined one as a template, and then make changes with that as the base.

4.4.2 Changing the Node Resistance

You only need to change the route additional resistance of the router if you are trying to influence the routes APPN selects for sessions. This is irrelevant unless there are alternate routes, some of which involve the router, and you want to alter the relative desirability of routing through the router.

If you need to influence route selection, we suggest that you first try do it by modifying the effective capacity of TGs. However, if all the TGs involved are equal, then it is probably easier to change the node resistance.

Figure 73 shows how to specify a different resistance for the router, with a lower value implying relatively more desirable.

```
APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [USIBMRA]?
Control point name (Max 8 characters) [RA2216A]?
Route addition resistance(0-255) [128]? 50                    1
XID ID number for subarea connection (5 hex digits) [00000]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 73. Changing the Node Resistance

Note:

1 This changes the route additional resistance for the router.

Chapter 5. Dependent LU Support

As an important part of its APPN support, the router provides Dependent LU Requester (DLUR) support for adjacent SNA nodes. The DLUR support allows dependent LUs in nodes that do not provide DLUR support to use the router as the entry point into an APPN network and access VTAM-based applications across the APPN network.

2216 Only

IBM has stated its intention to provide TN3270E Server function in a future level of the IBM 2216. This will provide an additional way of connecting to the DLUR function in the 2216 if the user requirement is limited to 3270-type access and the 3270 capabilities provided by TN3270E are sufficient.

5.1 Dependent LU Requester

For an overview of DLUR and information on the functions and restrictions of the router implementation, see 2.2.2.2, “Dependent LU Requester” on page 17.

You will almost certainly need to use DLUR in at least some of the routers in your network in order to provide support for nodes that do not provide DLUR support for their (internal) dependent LUs.

5.1.1 Configuring DLUR

DLUR capability is not enabled by default. To implement DLUR on the router, there are a number of steps to the configuration process:

- Enable DLUR at the node level.
- Specify the name of the primary Dependent LU Server (DLUS) with which the router DLUR function is to connect.

  Optionally, an alternate (backup) DLUS may be specified.
- Optionally (but highly recommended), change the DLUR retry values.
- Optionally, specify a different primary or alternate DLUS for an individual station.

The assumption that we have made is that you will allow adjacent nodes to initiate connections to the router and request dependent LU support. However, it is possible to initiate all communication with DSPUs from VTAM, in which case the DLUS does not have to be defined in the router.

5.1.1.1 Enabling DLUR

See Figure 74 on page 140 for an example of how to enable DLUR, and Figure 75 on page 141 for how to specify different DLUSs for an individual station.

The additional information required is:

Primary DLUS name This is the network-qualified name of the VTAM control point that is to be the primary provider of DLUS function. The DLUS can have a

different network ID from the router, though there must be an APPN route between the DLUR and the DLUS.

Backup DLUS name

This is the network-qualified name of the VTAM control point that is to be the backup provider of DLUS function.

Retry values

If the control sessions between the DLUR and a DLUS are disrupted, they have to be restarted (to the same or an alternate DLUS) before new sessions can be initiated on behalf of DLUR supported dependent LUs. The control sessions are also required before dependent LUs on newly connecting nodes can be activated.

The default retry parameter values may not be appropriate for your network. See the discussion in 5.1.1.2, “Changing the DLUR-to-DLUS Session Retry Parameters” on page 141 to help you decide whether to use the defaults or some alternative values.

We strongly recommend that you specify the use of retries rather than take the default.

```
APPN config>set dlur
Enable DLUR (Y)es (N)o [N]? y
Fully-qualified CP name of primary DLUS []? usibmra.rak          1
Fully-qualified CP name of backup DLUS []? usibmra.raz           2
Perform retries to restore disrupted pipe [N]?                   3
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 74. Enabling DLUR

Notes:

1. This is the primary DLUS VTAM CP name.
2. The alternate DLUS is optional.
3. Although the default provides basic DLUR capability, see 5.1.1.2, “Changing the DLUR-to-DLUS Session Retry Parameters” on page 141 for a discussion of how you should set this parameter.

```
APPN config>add link-station
APPN Station
Port name for the link station [ ]? tkra1
Station name (Max 8 characters) [ ]? ws05601
  Activate link automatically (Y)es (N)o [Y]?
  MAC address of adjacent node [000000000000]? 400052005601
  Adjacent node type: 0 = APPN network node,
  1 = APPN end node or Unknown node type
  2 = LEN end node, 3 = PU 2.0 node [1]?                          1
  High performance routing: (Y)es (N)o [Y]?
Edit Dependent LU Server: (Y)es (N)o [N]? y                       2
  Fully-qualified CP name of primary DLUS [USIBMRA.RAK]? usibmra.ray 3
  Fully-qualified CP name of backup DLUS [USIBMRA.RAZ]?           4
  Allow CP-CP sessions on this link (Y)es (N)o [Y]?
  CP-CP session level security (Y)es (N)o [N]?
  Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 75. Specifying a Different DLUS for a Station (Token-Ring)

Notes:

1. Note that all node types are supported by DLUR, not just PU 2.0 nodes. APPN end nodes or network nodes (that do not themselves provide DLUR support), and LEN nodes may contain dependent LUs that require DLUR support in the router in order to traverse the APPN network.
2. This allows the default DLUSs to be overridden.
3. This overrides the node-wide (default) primary DLUS for this station.
4. This allows the node-wide alternate DLUS to be overridden for this station.

5.1.1.2 Changing the DLUR-to-DLUS Session Retry Parameters

DLUR attempts to start a session with a DLUS when the first node requesting SSCP support connects. Also, when it loses contact with a DLUS, it usually attempts to recover the connection. In both cases, the retry parameters selected will influence the logic, timing, and duration of attempts to connect.

The logic used in this processing is illustrated in Figure 76 on page 143. Before you study that logic, keep a number of points in mind:

Nondisruptive UNBIND

A nondisruptive UNBIND is one that contains a sense code of X'08A0000A'. A DLUS will terminate the DLUS-DLUR control sessions with this sense code if an error is detected in the DLUR-to-DLUS protocols.

In such circumstances, it is clearly undesirable for the DLUR to immediately try to reconnect to the DLUS, or a tight error loop may develop.

Immediate retries are *never* used when this sense code is received, but if retries are enabled, the delay

before initiating retries value is used to delay trying to find a DLUS.

An immediate retry sequence is always attempted in all other circumstances.

Retry sequence In the diagram, a retry sequence, although shown as a single decision box, represents an immediate attempt to start a session with the primary DLUS, followed immediately by an attempt to start a session with the backup DLUS (if one is specified). Usually, the DLUS will be the one specified at the node level, though the same logic applies if an individual station has a different DLUS specified.

Short retry delay The value used for the short retry delay shown in the diagram is the lower of the specified short retry timer and delay before initiating retries values.

Note that long retry recovery only continues if there is still a connected DSPU that requires SSCP service.

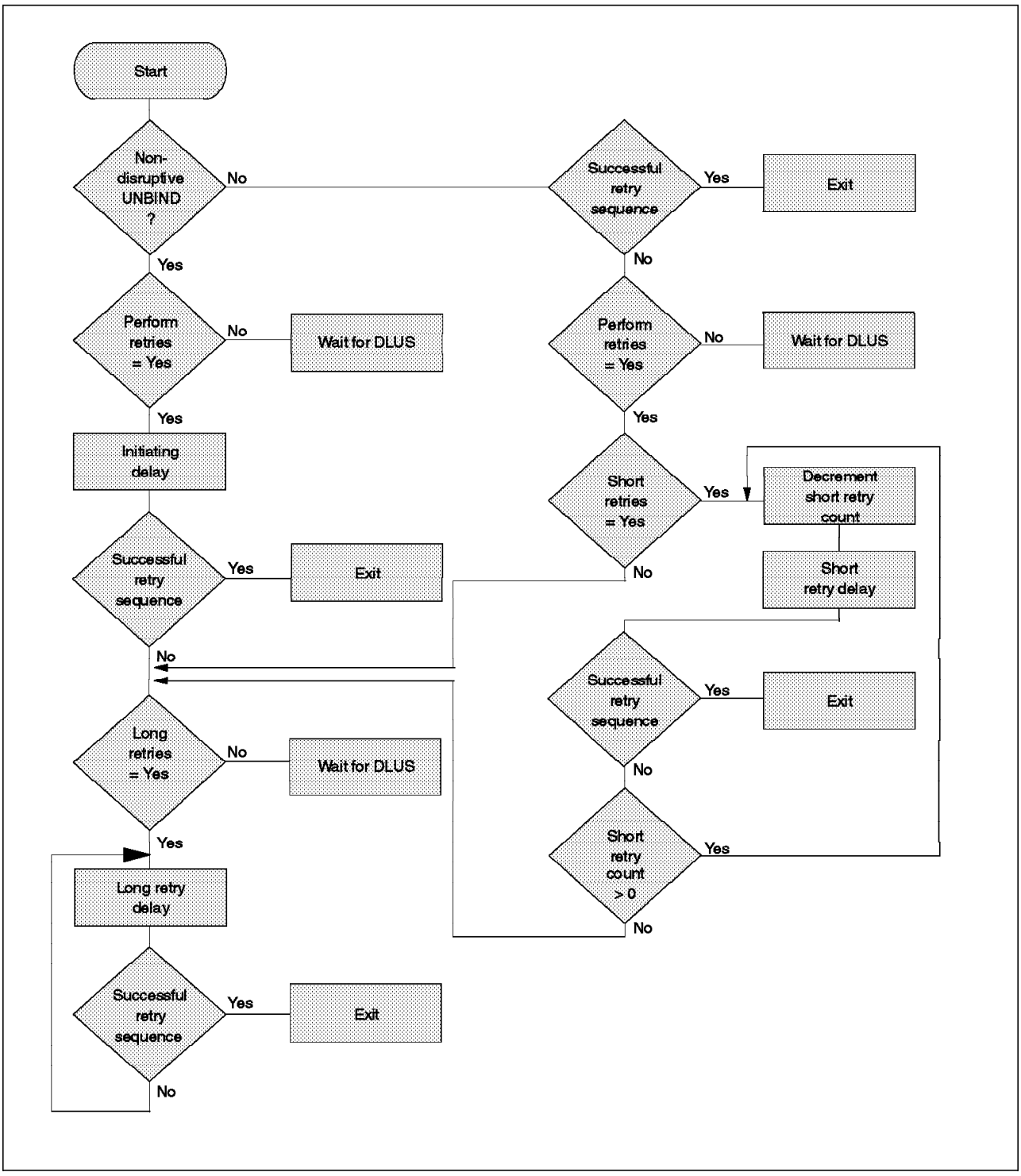


Figure 76. DLUR-to-DLUS Session Recovery Logic

An example of changing the DLUR retry parameters is shown in Figure 77 on page 144. You should consider the following points and then specify the retry parameter values that are appropriate for your network.

- We suggest that you always enable retries, as DSPUs will initiate the connection to the router in most cases.

- Consider adjusting the delay before initiating retries value if the operational procedures used in your network result in giveback, followed by takeover, that requires longer than the default of 120 seconds.
- If an alternate DLUS is not normally available, then it may be appropriate to reduce the short retry timer value because the default value of 120 seconds implies an average delay of one minute before SSCP service is restored after the DLUS (re-)start.
- You should assess how long it takes to make a DLUS available in normal restart circumstances, and adjust the short retry timer (assuming this is less than the delay before initiating retries value) and Short retry count values so that relatively frequent recovery attempts continue for at least this period. If the restart of a DLUS takes longer than this, then once a DLUS does become available, it will not be used for, on an average, half the long retry timer value (if long retries are enabled).
- We suggest that you enable long retries, as this will ensure a DLUS is eventually discovered on restart after a long network outage. Remember, this may be the case over special holiday periods rather than being failure caused. Long retries also cater for a forgotten takeover.

  The default value for long retry timer of five minutes is probably appropriate, but can be changed.

```
APPN config>set dlur
Enable DLUR (Y)es (N)o [Y]?
Fully-qualified CP name of primary DLUS [USIBMRA.RAK]?
Fully-qualified CP name of backup DLUS [USIBMRA.RAZ]?
Perform retries to restore disrupted pipe [N]? y                    1
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [N]? y              2
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [N]? y                 3
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 77. Modifying the DLUR-to-DLUS Session Retry Parameters

Notes:

1. This enables retries (beyond the single attempt if the UNBIND is not nondisruptive).
2. This enables short retries.
3. This enables long retries. Short retries are not a prerequisite for long retries.

The alternative way to configure DLUR is by using the Configuration Program. The DLUR configuration window is shown in Figure 78 on page 145.

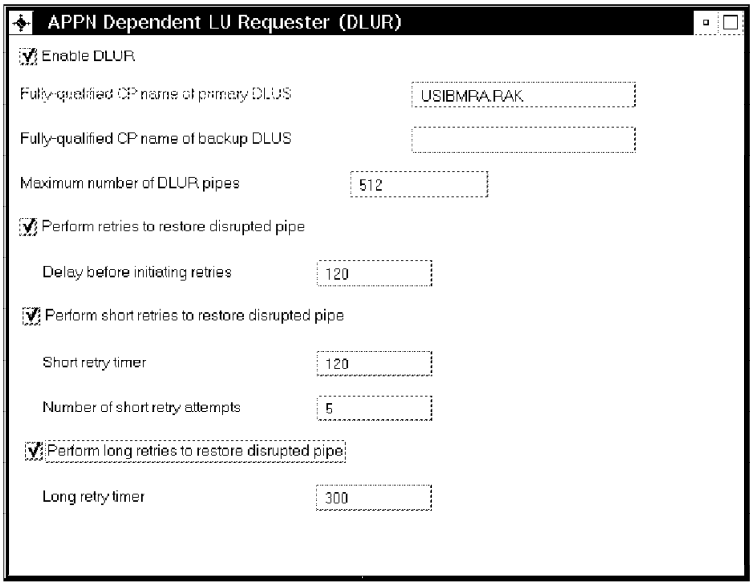


Figure 78. Dependent LU Requester Definition Window

5.1.2 VTAM Definitions for DLUR

For connecting nodes that use the DLUR function on the router to provide support for their dependent LUs and supporting PU 2.0 function, it is often necessary to provide definitions in the DLUS VTAM for the PU and associated dependent LUs.

5.1.2.1 Identifying DLUR Served Nodes to VTAM

VTAM identifies nodes that connect in via DLUR by using exactly the same techniques as for all other types of dial-in connections. It identifies the node by either CP name or the IDBLK/IDNUM combination. APPN nodes and most LEN nodes provide their CP name at connection time as part of the XID process, and all switched nodes (physical or logical) also supply an IDBLK/IDNUM at the same time.

However, there are some PU 2.0 nodes that do not support XID, such as some leased SDLC implementations. The DLUS processing requires such nodes to provide XID information because all DLUR-connected DSPUs appear to VTAM as being on switched connections, even if the underlying physical connectivity is leased. To cater to this, the router allows an IDBLK/IDNUM value to be specified on the station definition for such nodes. DLUR passes this value to VTAM at node activation time. See Figure 79 on page 146 for an example of how this is specified.

```
APPN config>add link-station
APPN Station
Port name for the link station [ ]? sdlc004
Station name (Max 8 characters) [ ]? l4c1
  Activate link automatically (Y)es (N)o [Y]?
  Station address(1-fe) [C1]?
  Adjacent node type: 0 = APPN network node,
  1 = APPN end node or Unknown node type
  2 = LEN end node, 3 = PU 2.0 node [1]? 3
  XID node identification (8 hex digits) [00000000]? 01712345          1
Edit Dependent LU Server: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Figure 79. Specifying an XID Value for a Leased SDLC DSPU

Note:

1 This enables an IDBLK and IDNUM to be specified for a PU 2.0 node that does not supply one at connection initiation time. It only applies to nodes on leased connections, such as leased SDLC lines.

5.1.2.2 Eliminating the Need for Definitions in a DLUS VTAM

If the node containing the dependent LUs initiates the connection to the router, there are techniques in VTAM that may enable the definitions to be reduced or even eliminated completely. If VTAM initiates the connection from the DLUR in a router to a node containing dependent LUs, it is possible to eliminate the need for LU definitions in VTAM.

The following VTAM functions, which are *not* unique to DLUR-supported PU 2.0s, enable definitions to be built dynamically:

- The VTAM *Selection of Definitions for Dependent LUs* (SDDLU) exit enables LU definitions to be built dynamically at either connection time or LU enable time. To use this exit, a connecting node must provide *Dynamic Definition of Dependent LU* (DDDLU) support. Examples of products that provide this support include 3174 Configuration Support C, Personal Communications/3270, Communications Server/2, and the IBM 2217. The exit is passed information provided by the remote node when a particular LU is enabled for use, and uses this to select a set of model LU parameter values as well as a specific LU name.
- The VTAM *Configuration Services XID* exit allows both the PU and LU definitions to be built dynamically when the remote node initiates the connection to the router DLUR. The exit is passed the information from the XID that flows at connection time, and uses this to select model definitions for both the PU and LUs, as well as the specific resource names to be used.

For further information on the dynamic definition of resources for switched nodes, see the *VTAM Network Implementation Guide*.

5.1.2.3 VTAM Definitions for Nodes Using DLUR

If definitions for both the DLUR-supported PU and its LUs cannot be built dynamically, some definitions are required in VTAM:

- As a minimum, a PU statement is required.
- If the connection between the router and the DLUR-supported node is to be initiated by VTAM rather than by the node connecting to the router, at least one PATH statement must also be defined to indicate to VTAM the name of the router containing the DLUR function that is to initiate the connection.

  The DLCADDR parameters on the PATH statement are used to tell the DLUR which port it should use to connect to the DSPU, and to pass the parameter values that would be required if a link station is defined on the router. In most cases, you do not need to define the station on the router, though this is required if the port defaults are not appropriate and the particular parameter cannot be overridden by the values from the VTAM PU definition.
- If neither of the VTAM exits is used to dynamically build the LU definitions, the LUs need to be defined below the PU statement (following any required PATH statements).

Sample VTAM Switched Major Node Statements: The following are example VTAM switched major node definitions for DLUR. You should note that PATH statements are necessary only if VTAM is initiating the connection to the DSPU.

The parameter values shown on the PU statements are intended to be illustrative rather than specific recommendations. You should use values appropriate for the node that contains the dependent LUs.

Refer to the *VTAM Resource Definition Reference* for details of the switched major node definition statements.

```
DABDLURX VBUILD TYPE=SWNET,MAXGRP=20,MAXNO=20,MAXDLUR=20
*********************************************************************
*IN THE DLCADDR, THE 'SUBFIELD_ID' = CV SUBFIELD OF THE CV91          *
* MINUS 0X90.                                                         *
*FOR EXAMPLE, THE CV94 SUBFIELD IS CODED ON DLCADDR=(4,X,...          *
*********************************************************************
*********************************************************************
* Following are PU Statements for PU 2.0 and Type 2.1 nodes
*********************************************************************
*********************************************************************
* PU STATEMENT for PU 2.0
*********************************************************************
*PU20RT   PU   ADDR=05,PUTYPE=2,MAXPATH=8,ANS=CONT,USSTAB=AUSSTAB,
*              ISTATUS=ACTIVE,MAXDATA=521,IRETRY=YES,MAXOUT=7,
*              PASSLIM=5,IDBLK=017,IDNUM=00035,MODETAB=AMODETAB
*              LOGAPPL=ECHO71,DLOGMOD=M23278I                    1
*********************************************************************
* PATH statements are not required if the DSPU is initiating the
* connection to VTAM
*  - for call-out from VTAM, one or more PATH statements are required
*  - PATH statements go here
*********************************************************************
* LU statements
*********************************************************************
*PU20LU1  LU    LOCADDR=2                                           12
*PU20LU2  LU    LOCADDR=3
*PU20LU3  LU    LOCADDR=4
*********************************************************************
* PU STATEMENT for TYPE 2.1 Node
*********************************************************************
*PU21RT   PU   ADDR=06,PUTYPE=2,CPNAME=PU21RT,ANS=CONT,MAXPATH=8,
*              ISTATUS=ACTIVE,USSTAB=AUSSTAB,MODETAB=AMODETAB
*              LOGAPPL=ECHO71,DLOGMOD=M23278I                    1
*********************************************************************
* PATH statements are not required if the DSPU is initiating the
* connection to VTAM
*  - for call-out from VTAM, one or more PATH statements are required
*  - any PATH statements go here
*********************************************************************
* LU statements
*********************************************************************
*PU21LU1  LU    LOCADDR=2                                           12
*PU21LU2  LU    LOCADDR=3
*PU21LU3  LU    LOCADDR=4
```

Figure 80 (Part 1 of 3). Sample VTAM Definitions for DLUR Supported Nodes

```
*************************************************************************
*
*************************************************************************
*
* Examples of PATH statements for various DLC types
*
* There is no difference in the PATH statement definitions
* between a PU 2.0 and a Type 2.1 node
*
* PATH statements are required if VTAM is initiating the connection
* to the DSPU.
*
*************************************************************************
*
*************************************************************************
* SDLC
*************************************************************************
*PSDLC   PATH  PID=1,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,SDLCNS),
*              DLCADDR=(2,I,S3),              2 * port name
*              DLCADDR=(3,X,C1)               4 * station address
*************************************************************************
* Frame Relay BNN
*************************************************************************
*PFRBNN  PATH  PID=2,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,FRPVC),
*              DLCADDR=(2,I,FR3),             2 * port name
*              DLCADDR=(3,X,04),              3 * SAP address
*              DLCADDR=(4,X,0024)             5 * DLCI
*************************************************************************
* Frame Relay BAN
*************************************************************************
*PFRBAN  PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,FRPVC),
*              DLCADDR=(2,I,FR),              2 * port name
*              DLCADDR=(3,X,04),              3 * SAP address
*              DLCADDR=(4,X,0024),            5 * DLCI
*              DLCADDR=(6,X,400000000001)     6 * MAC addr
*************************************************************************
* Token Ring
*************************************************************************
*PTR      PATH  PID=1,
*               DLURNAME=RED,
*               DLCADDR=(1,C,TR),
*               DLCADDR=(2,I,TR000),          2 * port name
*               DLCADDR=(3,X,04),             3 * SAP address
*               DLCADDR=(4,X,400000011088)    7 * MAC address
```

Figure 80 (Part 2 of 3). Sample VTAM Definitions for DLUR Supported Nodes

```
*************************************************************************
* Ethernet
*************************************************************************
*PET     PATH  PID=1,
*               DLURNAME=PURPLE,
*               DLCADDR=(1,C,ETHERNET),
*               DLCADDR=(2,I,ENO00),          2  * port name
*               DLCADDR=(3,X,20),             3  * SAP address
*               DLCADDR=(4,X,400000011063)    7  * MAC address
*************************************************************************
* X25 QLLC SVC
*************************************************************************
*PSVC    PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,X25SVC),
*              DLCADDR=(2,I,X25003),          2   * port name
*              DLCADDR=(4,X,C3),              9   * Protocol identifier
*              DLCADDR=(21,X,000566666)       10  * Destination DTE address
*************************************************************************
* X25 QLLC PVC
*************************************************************************
*PPVC    PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,X25PVC),
*              DLCADDR=(2,I,X25003),           2   * port name
*              DLCADDR=(3,X,0001)              11  * Logical channel number
*************************************************************************
```

Figure 80 (Part 3 of 3). Sample VTAM Definitions for DLUR Supported Nodes

Notes:

1 The major difference between the PU statements shown is:

- For PU 2.0 node definitions, the PU statement uses IDBLK=...,IDNUM=....
- For type 2.1 node definitions, the PU statement uses CPNAME=....

The assumption is that VTAM has been started with the start option SMNORDER=CPNAME (the default), so that connecting nodes are identified by CPNAME, if they supply one, and if not, by IDNUM/IDBLK. PU 2.0 nodes cannot supply a CPNAME at connection time, whereas Type 2.1 nodes do.

There are other differences, such as MAXDATA, in the examples shown. MAXDATA is ignored for Type 2.1 nodes; the value to be used is negotiated in the XID3 process that occurs at connection setup. Other values, such as MAXOUT and PASSLIM, are also negotiated for Type 2.1 nodes, though the negotiation may be influenced by specifying values that will be used as upper bounds in the XID3 negotiation process.

2 The router requires the name of the port to be used to connect to the DSPU, and it must receive it in ASCII.

- With data type I, VTAM translates the characters to ASCII for you.

  - Your VTAM may need maintenance to support this data type.
  - To use the ASCII data type, VTAM V4R2 or V4R3 requires the fix for APAR OW19815. The fix for APAR OW20333 is recommended as well.
- Alternatively, use data type X, but you must specify the hexadecimal representation of the ASCII character values.

3 SAP of DSPU (noncanonical, except for Ethernet).

4 Station address for SDLC.

5 DLCI must have four digits because it is a halfword.

6 MAC address of the DSPU (noncanonical) for frame relay BAN.

7 MAC address of the DSPU (noncanonical, except for Ethernet MAC address, which is canonical).

8 DLSw appears to VTAM like a token-ring DLC.

9 Protocol identifier for QLLC.

10 Destination DTE address (00llnnn...nn), where:

- 00 is fixed.
- ll is the length of the following DTE address.
- nnn...nn is the DTE address.

11 Logical channel number. It must have four digits because it is a halfword field.

12 LU coding, as required.

5.1.3 Sample Dependent LU Requester Configuration Scenarios

In 3.4, “A Sample Intermediate Session Routing Configuration Scenario” on page 46 and 3.5, “A Sample High-Performance Routing Configuration Scenario” on page 89, we developed the detail configuration steps for both ISR and HPR cases. We now add DLUR function to those base examples.

5.1.3.1 DLUR Configuration for the ISR Scenario

This scenario, shown in Figure 81 on page 152, adds the dependent LU requester function to the ISR setup in 3.4, “A Sample Intermediate Session Routing Configuration Scenario” on page 46. The DLUR support was configured on the 2210B router.

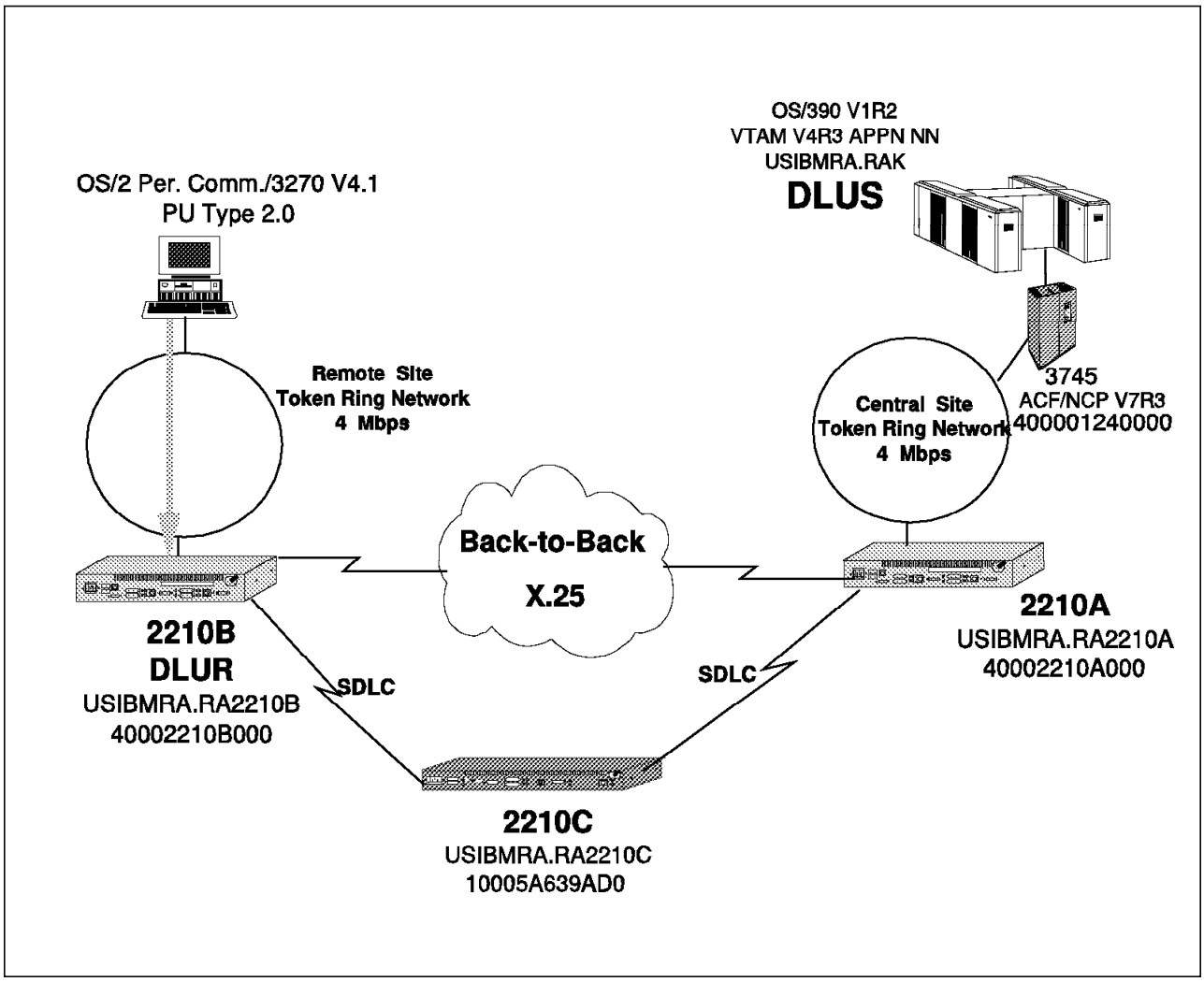


Figure 81. DLUR Scenario on an ISR Network

This will enable WS05600, the PC client with Personal Communications V4.1 for OS/2, to access the host via 2210B DLUR. Personal Communication for OS/2 was configured to access the host by going to the MAC address of 2210B (4000 2210 B000) using the token-ring link. To test this scenario, we logged on to the host and accessed our OfficeVision/VM mail and files.

The DLUR configuration steps for router 2210B is shown in Figure 82 on page 153. Note that only the DLUR configuration is shown here and all the other APPN configurations are in 3.4, “A Sample Intermediate Session Routing Configuration Scenario” on page 46.

```
APPN config>set dlur
Enable DLUR (Y)es (N)o [N]? y  1
Fully-qualified CP name of primary DLUS []? usibmra.rak   2
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [N]?
Write this record? [Y]?
The record has been written.

APPN config>li all
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210B
 XID: 2210B
 APPN ENABLED: YES
 MAX SHARED MEMORY: 1792
 MAX CACHED: 200
DLUR:
 DLUR ENABLED: YES   1
 PRIMARY DLUS NAME: USIBMRA.RAK   2
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 ---------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 ------------------------------------------------------
     0      TKRB0   IBMTRNET    YES      YES      YES
   254      DLSB4        DLS     NO      YES      YES
     3     SDLCB3       SDLC     NO      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
  R2210AD    DLSB4    40002210ADDD        NO     YES       0
  R2210CS   SDLCB3              D2        NO     YES       0
LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------
APPN config>
*restart
```

Figure 82. DLUR Configuration Steps for Router B

Notes:

1. Enable the DLUR function.

2. Configure the primary DLUS name.

3. For this scenario, which uses DLSw as an APPN port, we found it necessary to set the packet size of router 2210A. The PIU size configured in WS05600′s PerComm/3270 is 2012. The 2210A router was configured using the following commands:

```
Config>set packet 2069
*restart
```

5.1.3.2 DLUR Configuration for the HPR Scenario

This scenario, shown in Figure 83 on page 155, adds the dependent LU requester function to the HPR setup in 3.5, “A Sample High-Performance Routing Configuration Scenario” on page 89. The DLUR support was configured for:

- 2210A. This will enable WS05112, the PC client with Personal Communications V4.1 for Windows, to access the host via the 2210A DLUR. Personal Communication for Windows was configured to access the host by going to the MAC address of 2210A (4000 2210 A000) using the token-ring link.
- 2210B. This will enable WS05600, the PC client with Personal Communications V4.1 for OS/2, to access the host via 2210B DLUR. Personal Communication for OS/2 was configured to access the host by going to the MAC address of 2210B (4000 2210 B000) using the token-ring link.

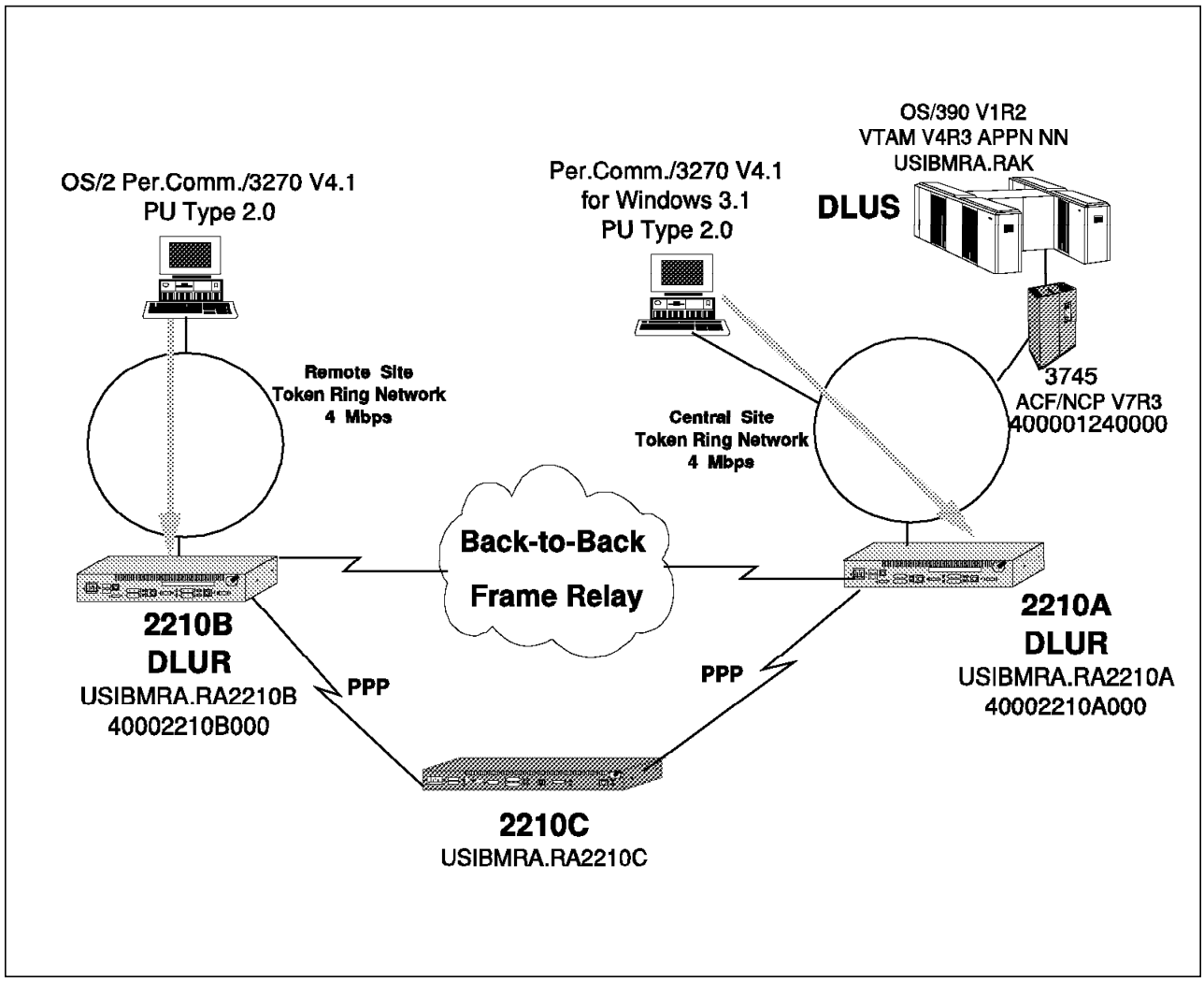


Figure 83. DLUR Scenario on an HPR Network

To test this scenario, we logged on to the host and accessed our OfficeVision/VM mail and files. To use HPR, we also did a file transfer by downloading from the host to the PC. While the file transfer was in progress, we broke the 2210A-2210B frame-relay link which was carrying the data traffic. The file transfer continued by rerouting through the PPP links via 2210C.

The configuration for 2210B is shown in Figure 84 on page 156. The configuration for 2210A is shown in Figure 85 on page 157.

```
APPN config>SET DLUR
Enable DLUR (Y)es (N)o [N]? Y   1
Fully-qualified CP name of primary DLUS [ ]? USIBMRA.RAK   2
Fully-qualified CP name of backup DLUS [ ]?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.

APPN config>exit
*restart
```

Figure 84. DLUR Configuration Steps for Router B

Notes:

1 Enable the DLUR function.

2 Configure the primary DLUS name.

```
APPN config>SET DLUR
Enable DLUR (Y)es (N)o [Y]?  1
Fully-qualified CP name of primary DLUS []? USIBMRA.RAK  2
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.

APPN config>LIST ALL
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210A
 XID: 2210A
 APPN ENABLED: YES
 MAX SHARED MEMORY: 1792
 MAX CACHED: 200
DLUR:
 DLUR ENABLED: YES  1.
 PRIMARY DLUS NAME: USIBMRA.RAK  2
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 --------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 ------------------------------------------------------
     0      TKRA1   IBMTRNET    YES      YES      YES
     1       FRA1         FR    YES      YES      YES
     2      PPPA2        PPP    YES      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
      RAK    TKRA1    400001240000       YES     YES       0
  WSO5112    TKRA1    10005AAC4296       YES      NO       1
   R2210B     FRA1              16       YES     YES       0
   R2210C    PPPA2    000000000000       YES     YES       0
```

Figure 85 (Part 1 of 2). DLUR Configuration Steps for Router A

```
LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------

APPN Config>exit
*restart
```

Figure 85 (Part 2 of 2). DLUR Configuration Steps for Router A

Notes:

1. Enable the DLUR function.
2. Configure the primary DLUS name.

Chapter 6. APPN Data Link Controls

This chapter lists the different APPN data link controls and provides configuration information and pointers for some of the less straightforward ones.

6.1 Supported DLCs

Table 6 shows the interfaces supported by APPN on the router:

Table 6. Port Types Supported for APPN Routing

Port Type	Standard	HPR	ISR	DLUR [1]
Ethernet	Version 2	Yes	Yes	Yes
Ethernet	IEEE 802.3	Yes	Yes	Yes
Token-Ring	802.5	Yes	Yes	Yes
ATM LANE - Ethernet	Forum-compliant	Yes	Yes	Yes
ATM LANE - Token-Ring	Forum-compliant	Yes	Yes	Yes
Native ATM [2]		(Yes)	(No)	(No)
Serial PPP		Yes	Yes	No
PPP over ISDN		Yes	Yes	No
PPP using V.25bis		Yes	Yes	No
Serial FR (BAN - bridged) [3]		Yes	Yes	Yes
Serial FR (BNN - routed) [3]		Yes	Yes	Yes
FR over ISDN		Yes	Yes	Yes
Serial LAN bridging		NA	NA	NA
SDLC		No	Yes	Yes
X.25 (QLLC) [4]	CCITT X.25	(No)	(Yes)	(Yes)
DLSw (remote only) [5]		No	Yes	Yes
ESCON LCS [6]		No	No	No
ESCON LSA [6]		No	Yes	No
ESCON MPC+ [6]		Yes	No	No

Notes:

1. This column refers to the port providing the connection to the downstream PU (DSPU).
2. IBM has stated that it intends to make this support available for both the 2210 and 2216 in future levels of MRS and MAS. Note that the support is for HPR only.
3. Use bridged format (BAN) when you have two routers connected by frame relay and one of them does not have APPN capability. Otherwise, use routed format for improved performance.
4. At initial availability, neither MRS V1R1.0 nor MAS V1.R1.0 provided X.25 QLLC support for APPN. However, IBM has stated that it intends to make this support available for both the 2210 and 2216.

5 Since APPN can run over DLSw, you can route any APPN ISR traffic across any port supported by DLSw, including X.25 and Classical IP over ATM, among others.

6 The 2210 does not provide ESCON support.

2216 Only

ESCON support on the 2216 requires MAS V1R1.1 or higher. Note that MPC+ is HPR only, and LSA is ISR only.

LCS is for TCP/IP only.

6.2 Configuring DLSw for APPN

The router supports APPN over DLSw for connectivity to nodes through a *remote* DLSw partner. This support allows customers with DLSw configurations to migrate their networks to APPN. It is recommended that you use APPN over direct DLCs when available instead of APPN over DLSw.

APPN configuration restrictions using DLSw to:

- Connectivity through remote DLSw partners only.
- Only one DLSw port per router.
- Use of a locally administered MAC address.
- HPR is not supported on DLSw ports.
- DLSw ports cannot be members of connection networks.
- Parallel TGs are not supported on DLSw ports.

6.2.1 How APPN Uses DLSw Ports to Transport Data

When APPN is configured on the router to use data link switching (DLSw) port, DLSw is used to provide a connection-oriented interface (802.2 LLC type 2) between the APPN component in the router and APPN nodes and LEN end nodes attached to a remote DLSw partner.

When configuring a DLSw port for APPN on the router, you assign the network node a unique MAC and SAP address pair that enables it to communicate with DLSw. The MAC address for the network node is locally administered and must not correspond to any physical MAC address in the DLSw network.

6.2.2 A Sample APPN/DLUR Scenario Using DLSw

This scenario, shown in Figure 86 on page 161, has only one router (2210A) with the APPN and DLUR functions. The partner router (2210B) only has DLSw and TCP/IP configured. This type of setup is applicable in situations where a customer may be migrating from DLSw to APPN or in situations where the remote office router is not APPN-capable.

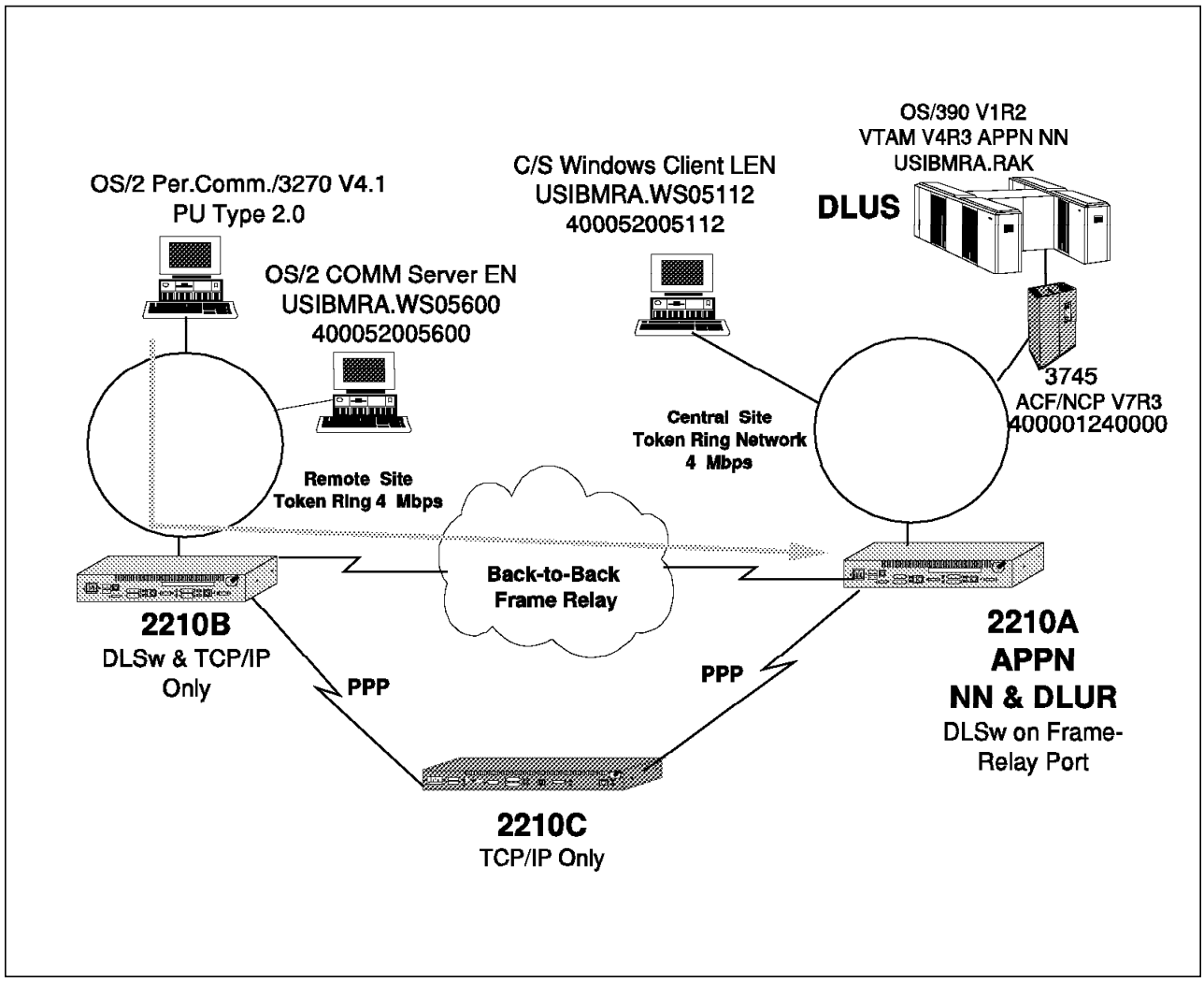


Figure 86. Logical Diagram of APPN Using DLSw

This scenario was used for both APPN network node and DLUR functionality. As an APPN end node, WS05600 (the PC on remote token-ring running Communications Server Client software) was configured with the following:

- Network node as 2210A
- LAN destination address as 40002210Addd, the locally administered DLSw MAC address of the 2210A APPN network node.

To use the DLUR functionality, the PC on the remote token-ring LAN was configured as a PU Type 2.0 node using the Personal Communications/3270 V4.1 software. Again, its LAN destination address is 40002210Addd, the locally administered DLSw MAC address of the 2210A DLUR.

6.2.2.1 Configuration Steps for 2210A

These steps show the configuration of DLSw and APPN. The quick configuration was done to set the following:

- Intf 0 is Token-Ring, speed 4 Mbps, Connector STP.
- Intf 1 is WAN 1 with frame relay encapsulation, V.35 DTE cable.
- Intf 2 is WAN 2 with PPP encapsulation, RS-232 DTE cable.
- Intf 3 is WAN 3 with PPP encapsulation, RS-232 DTE cable.

- Intf 4 is WAN 4 with PPP encapsulation, RS-232 DTE cable.

For this scenario, interfaces 3 and 4 were not used. The TCP/IP addresses were also configured and OSPF was enabled during the quick configuration process.

The steps shown in this configuration are:

1. Interface configuration of the back-to-back frame relay in Figure 87.
2. IP and OSPF configuration in Figure 88 on page 163. TCP/IP configuration is required because we will use DLSw.
3. Bridging and DLSw configuration in Figure 89 on page 164.
4. APPN port configuration in Figure 90 on page 165.
5. APPN link configuration in Figure 91 on page 166.
6. APPN node configuration in Figure 92 on page 166.
7. DLUR configuration in Figure 93 on page 167.

```
Config>n 1
Frame Relay user configuration
FR Config>disable lmi   1
FR Config>add per   1
Circuit number [16]?
Committed Information Rate (CIR) in bps [64000]? 400000
Committed Burst Size (Bc) in bits [64000]? 400000
Excess Burst Size (Be) in bits [0]?
Assign circuit name []? to2210b
Is circuit required for interface operation [N]?
FR Config>exit
```

Figure 87. Back-to-Back Frame Relay Configuration for Router A

```
Config>protocol ip
Internet protocol user configuration
IP config>set internal-ip-address
Internal IP address [0.0.0.0]? 10.24.104.93   2
IP config>set router
Router-ID [0.0.0.0]? 9.24.104.93
IP config>li addresses
IP addresses for each interface:
   intf  0   9.24.104.93      255.255.255.0    Local wire broadcast, fill 1
   intf  1   200.200.200.2    255.255.255.0    Local wire broadcast, fill 1
   intf  2   202.202.202.1    255.255.255.0    Local wire broadcast, fill 1
   intf  3                                     IP disabled on this interface
   intf  4                                     IP disabled on this interface
Router-ID: 9.24.104.93
Internal IP address: 10.24.104.93
IP config>exit

Config>protocol opspf
Protocol name or number [IP]? ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>li all
                        --Global configuration--
                OSPF Protocol:          Enabled
                # AS ext. routes:       1000
                Estimated # routers:    50
                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
9.24.104.93       0.0.0.0              1      5       1     1     10     40
200.200.200.2     0.0.0.0              1      5       1     1     10     40
202.202.202.1     0.0.0.0              1      5       1     1     10     40

OSPF Config>add neighbor
Interface IP address [0.0.0.0]? 200.200.200.2
IP Address of Neighbor [0.0.0.0]? 200.200.200.1
Can that router become Designated Router on this net [Yes]? n
OSPF Config>exit
```

Figure 88. TCP/IP and OSPF Configuration for Router A

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge  3
ASRT config>disable transparent 1
ASRT config>enable source-routing 1 584 e  3
ASRT config>enable dls  3
ASRT config>li bridge
                Source Routing Transparent Bridge Configuration
                ===============================================
Bridge:                 Enabled                 Bridge Behavior: SRB
                  +---------------------------+
------------------] SOURCE ROUTING INFORMATION ]------------------------------
                  +---------------------------+
Bridge Number:          0E                      Segments:          1
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1 N SRB:                Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
                  +-------------------+
------------------] SR-TB INFORMATION ]-----------------------------------------
                  +-------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
                  +-----------------------------------+
------------------] SPANNING TREE PROTOCOL INFORMATION ]----------------------
                  +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IBM-SRB proprietary
                  +-------------------------+
------------------] TRANSLATION INFORMATION ]---------------------------------
                  +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                  +------------------+
------------------] PORT INFORMATION ]-----------------------------------------
                  +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled
ASRT config>exit

Config>protocol dls
DLSw protocol user configuration
DLSw config>enable dls  4
DLSw config>set srb aaa  4
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 10.8.8.1  4
Connectivity Setup Type (a/p) [p]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]? e
Neighbor Priority (H/M/L) [M]?
DLSw config>open  5
Interface # [0]?
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 0
DLSw config>exit
```

Figure 89. ASRT Configuration for Router A

```
Config>P APPN
APPN user configuration

APPN config>ADD PORT
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? T   6
Interface number(Default 0): [0]?
Port name (Max 8 characters) [TR000]? TKRA1
Enable APPN on this port (Y)es (N)o [Y]?   6
Port Definition
 Service any node: (Y)es (N)o [Y]?
 High performance routing: (Y)es (N)o [Y]?
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>ADD PORT
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? D   7
Port name (Max 8 characters) [DLS254]? DLS2210A
Enable APPN on this port (Y)es (N)o [Y]?   7
Port Definition
 Service any node: (Y)es (N)o [Y]?
 Maximum BTU size (768-2063) [2048]?
 Maximum number of link stations (1-976) [512]?
 Percent of link stations reserved for incoming calls (0-100) [0]?
 Percent of link stations reserved for outgoing calls (0-100) [0]?
 Local SAP address (04-EC) [4]?
 Locally administered MAC address (hex) [000000000000]? 40002210ADDD   7
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 90. APPN Port Configuration for Router A

```
APPN config>ADD LINK
APPN Station
Port name for the link station [ ]? TKRA1
Station name (Max 8 characters) [ ]? RAK  8
 Activate link automatically (Y)es (N)o [Y]?
 MAC address of adjacent node [000000000000]? 400001240000  8
 Adjacent node type: 0 = APPN network node,
 1 = APPN end node or Unknown node type
 2 = LEN end node [1]? 0
 High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 91. ASRT Configuration for Router A

```
APPN config>SET NODE  9
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? USIBMRA  9
Control point name (Max 8 characters) [  ]? RA2210A  9
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]? 2210A
Write this record? [Y]?
The record has been written.
```

Figure 92. APPN Node Configuration for Router A

```
APPN config>set dlur
Enable DLUR (Y)es (N)o [N]? y   10
Fully qualified CP name of primary DLUS []? USIBMRA.RAK   10
Fully qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [N]?
Write this record? [Y]?
The record has been written.

APPN config>LI ALL
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210A
 XID: 2210A
 APPN ENABLED: YES
 MAX SHARED MEMORY: 4096
 MAX CACHED: 4000
DLUR:
 DLUR ENABLED: YES   10
 PRIMARY DLUS NAME: USIBMRA.RAK   10
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 --------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 ---------------------------------------------------
     0      TKRA1   IBMTRNET    YES      YES      YES
   254   DLS2210A        DLS     NO      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
      RAK    TKRA1    400001240000       YES     YES       0
LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------

APPN config>
Config>SET PACKET   11
What is the maximum packet size (in bytes) [0]? 2069   11
Packet size updated successfully
Config>
*RESTART
```

Figure 93. DLUR Configuration for Router A

Notes:

1 Configure interface 1 for back-to-back frame relay.

2 Set the internal IP address for use in DLSw.

3 Configure bridging on the token-ring port and enable DLSw.

4 Enable DLSw, set the virtual ring number, and add the TCP/IP address of the DLSw partner.

5 Open the SAPs for SNA.

6 Configure the token-ring port for APPN.

7 Configure the DLSw as an APPN port.

8 Add and initiate a link to the VTAM host.

9 Configure the node level APPN parameters.

10 Enable DLUR and configure the primary DLUS name.

11 For this scenario, which uses DLSw as an APPN port, we found it necessary to set the packet size of router 2210A. The PIU size configured in WS05600′s PerComm/3270 is 2012 bytes.

6.2.2.2 Configuration Steps for 2210B

These steps show the configuration of DLSw for 2210B. The quick configuration was done to set the following:

- Intf 0 is token-ring, speed 4 Mbps, Connector STP, MAC Address=40002210B000.
- Intf 1 is WAN 1 with frame relay encapsulation, V.35 DTE cable.
- Intf 2 is WAN 2 with PPP encapsulation, RS-232 DTE cable.
- Intf 3 is WAN 3 with PPP encapsulation, RS-232 DTE cable.
- Intf 4 is WAN 4 with PPP encapsulation, RS-232 DTE cable.
- Intf 5 is token-ring, speed 4 Mbps, Connector STP.

For this scenario, interfaces 3, 4, and 5 were not used. The TCP/IP addresses were also configured and OSPF was enabled during the quick configuration process.

The steps shown in this configuration are:

1. Interface configuration of the back-to-back frame relay in Figure 94 on page 169.
2. IP and OSPF configuration in Figure 95 on page 170. TCP/IP configuration is required because we use DLSw.
3. Bridging and DLSw configuration in Figure 96 on page 171.

```
Config>n 1
Frame Relay user configuration
FR Config>disable lmi   1
FR Config>add per   1
Circuit number [16]?
Committed Information Rate (CIR) in bps [64000]? 400000
Committed Burst Size (Bc) in bits [64000]? 400000
Excess Burst Size (Be) in bits [0]?
Assign circuit name []? to2210a
Is circuit required for interface operation [N]?
FR Config>ex
```

Figure 94. Back-to-Back Frame Relay Configuration for Router B

```
Config>protocol ip
Internet protocol user configuration
IP config>set internal-ip-address
Internal IP address [0.0.0.0]? 10.8.8.1   2
IP config>set router
Router-ID [0.0.0.0]? 8.8.8.1
IP config>li addresses
IP addresses for each interface:
   intf  0   8.8.8.1          255.255.255.0    Local wire broadcast, fill 1
   intf  1   200.200.200.1    255.255.255.0    Local wire broadcast, fill 1
   intf  2   201.201.201.1    255.255.255.0    Local wire broadcast, fill 1
   intf  3                                     IP disabled on this interface
   intf  4                                     IP disabled on this interface
   intf  5                                     IP disabled on this interface
Router-ID: 8.8.8.1
Internal IP address: 10.8.8.1
IP config>ex

Config>protocol ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>add neighbor
Interface IP address [0.0.0.0]? 200.200.200.2
  IP address is not assigned to an interface
OSPF Config>add neighbor
Interface IP address [0.0.0.0]? 200.200.200.1
IP Address of Neighbor [0.0.0.0]? 200.200.200.2
Can that router become Designated Router on this net [Yes]?
OSPF Config>li all
                        --Global configuration--
                OSPF Protocol:          Enabled
                # AS ext. routes:       1000
                Estimated # routers:    50
                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
8.8.8.1           0.0.0.0              1      5       1     1     10     40
200.200.200.1     0.0.0.0              1      5       1     1     10     40
201.201.201.1     0.0.0.0              1      5       1     1     10     40
                        --Neighbor configuration--
                Neighbor Addr     Interface Address   DR eligible?
                200.200.200.2     200.200.200.1       yes
OSPF Config>ex
```

Figure 95. TCP/IP and OSPF Configuration for Router B

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge  3
ASRT config>disable transparent 1  3
ASRT config>enable source-routing  3
Port Number [1]?
Segment Number for the port in hex(1 - FFF) [  1]? ffb
Bridge number in hex (0 - 9, A - F) [0]? 2
ASRT config>enable dls  3
ASRT config>list bridge
               Source Routing Transparent Bridge Configuration
               ===============================================
Bridge:                 Enabled                 Bridge Behavior: STB and SRB
                  +-----------------------------+
------------------] SOURCE ROUTING INFORMATION ]------------------------------
                  +-----------------------------+
Bridge Number:          02                      Segments:          1
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1 N SRB:                Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
                  +-------------------+
------------------] SR-TB INFORMATION ]---------------------------------------
                  +-------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
                  +-----------------------------------+
------------------] SPANNING TREE PROTOCOL INFORMATION ]----------------------
                  +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IEEE802.1d on TB ports only, IBM-SRB proprietary on SR ports
                  +-------------------------+
------------------] TRANSLATION INFORMATION ]---------------------------------
                  +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                  +------------------+
------------------] PORT INFORMATION ]---------------------------------------
                  +------------------+
Number of ports added: 2
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled
ASRT config>exit
```

Figure 96 (Part 1 of 2). Bridge and DLSw Configuration for Router B

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>enable dls  4
DLSw config>set srb aaa  4
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 10.24.104.93  4
Connectivity Setup Type (a/p) [p]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]? e
Neighbor Priority (H/M/L) [M]?
DLSw config>open-sap  5
Interface # [0]?
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 0
DLSw config>exit
Config>
*restart
```

Figure 96 (Part 2 of 2). Bridge and DLSw Configuration for Router B

Notes:

1 Configure interface 1 for back-to-back frame relay.

2 Set the internal IP address for use in DLSw.

3 Configure bridging on the token-ring port and enable DLSw.

4 Enable DLSw, set the virtual ring number, and add the TCP/IP address of the DLSw partner.

5 Open the SAPs for SNA.

6.3 Configuring Frame Relay for APPN

APPN on the 2210 and 2216 frame-relay ports accepts both the RFC 1490 bridged and routed frame formats. For example, the frame-relay APPN link in the HPR scenario in 3.5, "A Sample High-Performance Routing Configuration Scenario" on page 89 uses the routed frame format.

Support for the RFC 802.5 bridged frame format on APPN frame-relay TGs is useful when the 2210 has a frame-relay connection to a bridge/DLSw BAN/FRAD that is providing frame-relay connectivity for token-ring LAN-attached SNA devices. The use of the bridged frame format over frame-relay PVCs allows multiple LLC2 token-ring LAN connections to be multiplexed over a single frame relay DLCI/SAP. Another advantage of this format is that it allows DLSw and APPN to share the same DLCI/SAP.

6.3.1 A Sample APPN/DLUR Scenario Using FR BAN

This scenario, shown in Figure 97, has only one router (2210A) with the APPN and DLUR functions. 2210A attaches to the host via token-ring. Its frame-relay port is enabled for APPN and is configured to accept RFC 1490 bridged frame format. The partner router (2210B) only has BAN and bridging configured to support the end node and PU 2.0 devices attached to it.

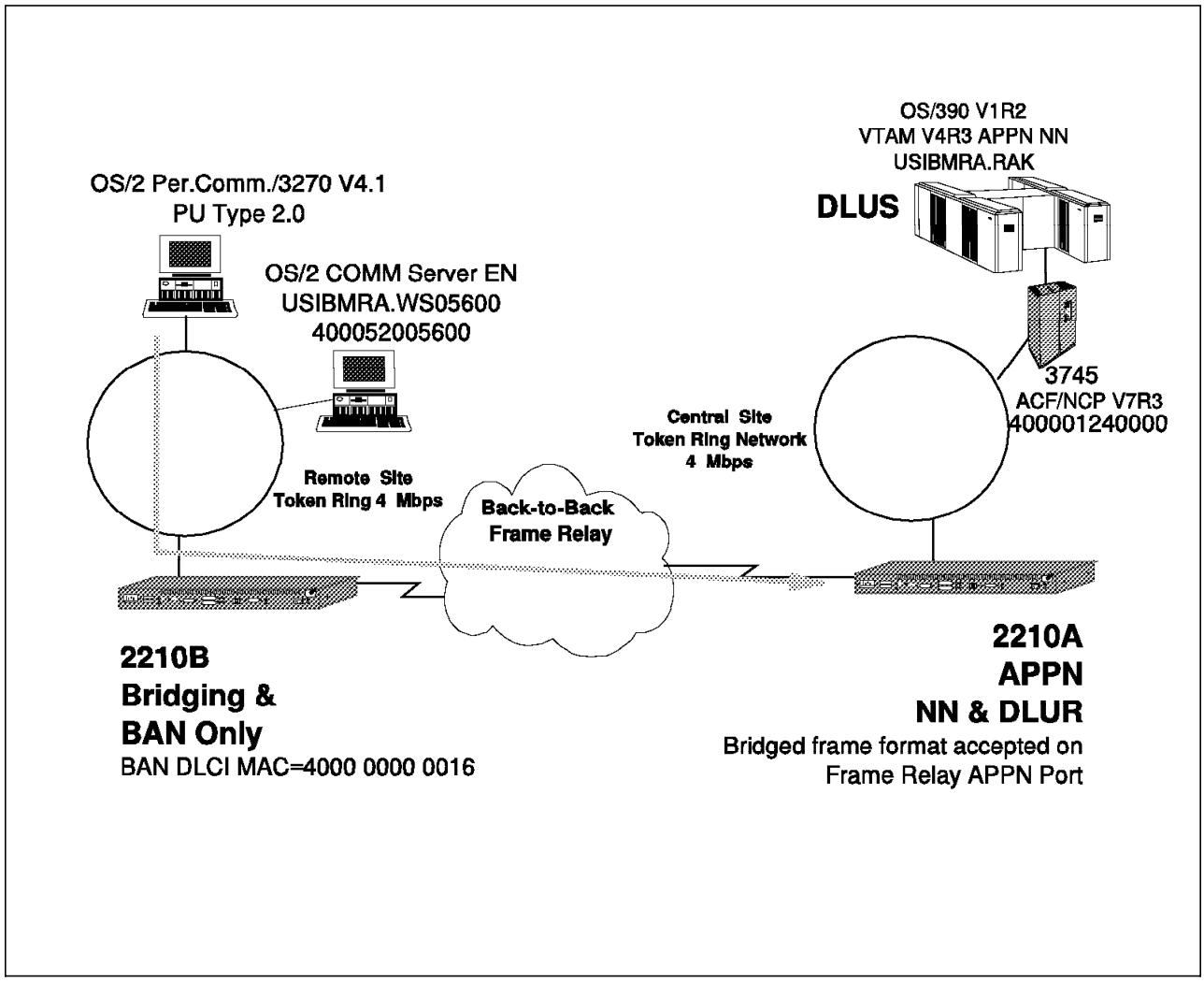


Figure 97. Logical Diagram of APPN Using Frame Relay BAN

This scenario was used for both APPN network node and DLUR functionality. As an APPN end node, WS05600 (the PC on remote token-ring running Communications Server Client software) was configured with the following:

- Network node as 2210A
- LAN destination address as 400000000016, the BAN DLCI MAC address of the 2210B router.

To use the DLUR functionality, the PC on the remote token-ring LAN was configured as a PU Type 2.0 node using the Personal Communications/3270 V4.1 software. Again, its LAN destination address is 400000000016, the BAN DLCI MAC address of the 2210B router.

The 2210 APPN BAN format allows 2210A to support the end node and the PU T2.0 in 2210B′s token-ring LAN. In this configuration:

- To the 2210B, 2210A looks like an NCP.
- 2210A does not really see the 2210B. It only sees the adjacent APPN nodes it is connected to. These nodes appears as regular frame relay-attached nodes.

6.3.1.1 Configuration Steps for 2210A for the BAN Scenario

These steps show the configuration of APPN for 2210A. 2210A is a Model 12T with 8 MB of DRAM. The quick configuration was done to set the following:

- Intf 0 is token-ring, speed 4 Mbps
- Intf 1 is WAN 1 with PPP encapsulation
- Intf 2 is WAN 2 with frame relay encapsulation

For this scenario, interface 1 is not used. The TCP/IP addresses were also configured and OSPF was enabled during the quick configuration process. Interface 2 is configured for back-to-back frame relay with RS-232 DTE and DCE cables.

The steps shown in this configuration are:

1. APPN frame-relay port configuration in Figure 98 on page 175. Only the frame-relay port configuration is shown here. For the other APPN configuration steps, see 3.5, “A Sample High-Performance Routing Configuration Scenario” on page 89. We have preconfigured the other APPN parameters including:
   - Configuration of the token-ring port for APPN
   - Addition and initiation of the link to the VTAM host
   - Configuration of the APPN node-level parameters and the fully qualified network node name
   - Configuration of tuning parameters for an 8 MB router
2. DLUR configuration in Figure 99 on page 176.

```
APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [ ]? f   1
Interface number(Default 0): [0]? 2   1
Port name (Max 8 characters) [FR002]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o [Y]?
High performance routing: (Y)es (N)o [Y]?
Maximum BTU size (768-2048) [2048]?
Maximum number of link stations (1-976) [512]?
Percent of link stations reserved for incoming calls (0-100) [0]?
Percent of link stations reserved for outgoing calls (0-100) [0]?
Local SAP address (04-EC) [4]?
Support bridged formatted frames: (Y)es (N)o [N]? y   1
Boundary node identifier (hex-noncanonical) [4FFF00000000]?   1
Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 98. APPN BAN Scenario: Frame-Relay Port Configuration for Router A

```
APPN config>set dlur
Enable DLUR (Y)es (N)o [N]? y  2
Fully qualified CP name of primary DLUS []? usibmra.rak  2
Fully qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [N]?
Write this record? [Y]?
The record has been written.
APPN config>li all
NODE:
NETWORK ID: USIBMRA  3
CONTROL POINT NAME: WS2210A
XID: 210B0
APPN ENABLED: YES
MAX SHARED MEMORY: 1792  4
MAX CACHED: 200
DLUR:
DLUR ENABLED: YES  2
PRIMARY DLUS NAME: USIBMRA.RAK  2
CONNECTION NETWORK:
      CN NAME       LINK TYPE  PORT INTERFACES
------------------------------------------------------------
COS:
COS NAME
--------
  #BATCH
#BATCHSC
#CONNECT
  #INTER
#INTERSC
 CPSVCMG
SNASVCMG
MODE:
 MODE NAME  COS NAME
--------------------
PORT:
  INTF     PORT      LINK      HPR    SERVICE   PORT
 NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
-------------------------------------------------------
    0      TR000   IBMTRNET    YES      YES      YES  5
    2      FR002         FR    YES      YES      YES
STATION:
 STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
  NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
------------------------------------------------------------
     RAK    TR000    400001240000       YES     YES       0  6
LU NAME:
      LU NAME         STATION NAME           CP NAME
------------------------------------------------------------
APPN config>
*rest
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 99. APPN BAN Scenario: DLUR Configuration for Router A

Notes:

1 Configure the frame-relay port for APPN. Enable the port to accept bridged format frames and configure the boundary node identifier.

2 Enable DLUR and configure the primary DLUS.

3 We preconfigured the APPN node level parameters.

4 We preconfigured the tuning parameters for this 8 MB router.

5 The token-ring APPN functionality was preconfigured.

6 The APPN link to the VTAM host was preconfigured.

6.3.1.2 Configuration Steps for 2210B

These steps show the configuration of BAN for 2210B. 2210B is a Model 127 with 8 MB of DRAM. The quick configuration was done to set the following:

- Intf 0 is token-ring, speed 4 Mbps
- Intf 1 is WAN 1 with frame relay encapsulation
- Intf 2 is WAN 2 with PPP encapsulation

For this scenario, interface 2 was not used. The TCP/IP addresses were also configured and OSPF was enabled during the quick configuration process.

The steps shown in this configuration are:

1. Bridging configuration in Figure 100 on page 178.
2. Boundary Access Node (BAN) configuration in Figure 101 on page 179.

```
Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>enable source    1
Port Number [1]?  1
Segment Number for the port in hex(1 - FFF) [  1]? ffb
Bridge number in hex (0 - 9, A - F) [0]? 2
ASRT config>disable transparent port 1

ASRT config>add port   2
Interface Number [0]? 1   2
Port Number [2]?
Circuit number [16]?   2
ASRT config>disable transparent
Port Number [1]? 2
ASRT config>enable source   2
Port Number [1]? 2
Segment Number for the port in hex(1 - FFF) [  1]? aaa
ASRT config>li br

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

Bridge:                 Enabled                 Bridge Behavior: SRB
                  +----------------------------+
------------------] SOURCE ROUTING INFORMATION ]------------------------------
                  +----------------------------+
Bridge Number:          02                      Segments:          2
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1 N SRB:                Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
                  +------------------+
------------------] SR-TB INFORMATION ]-----------------------------------------
                  +------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
                  +-----------------------------------+
------------------] SPANNING TREE PROTOCOL INFORMATION ]----------------------
                  +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000

STP Participation:      IBM-SRB proprietary
                  +-------------------------+
------------------] TRANSLATION INFORMATION ]---------------------------------
                  +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Disabled
                  +-----------------+
------------------] PORT INFORMATION ]-----------------------------------------
                  +-----------------+
Number of ports added: 2
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled
Port:   2      Interface:       1      Behavior:    SRB Only   STP:  Enabled
 Circuit number: 16
```

Figure 100. APPN BAN Scenario: Bridge Configuration for Router B

```
ASRT config>ban
BAN (Boundary Access Node) configuration
BAN config>add
Port Number [0]? 2   3
Enter the BAN DLCI MAC Address []? 400000000016   3
Enter the Boundary Node Identifier MAC Address [4FFF00000000]?
Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) [b]?
BAN port record added.
Reminder: enable source-routing on the port if you have not already done so.

BAN config>list
bridge  BAN                 Boundary            bridged or
port    DLCI MAC Address    Node Identifier     DLSw terminated
2       40 00 00 00 00 16   4F FF 00 00 00 00   bridged   3

BAN config>ex
ASRT config>ex
Config>
*restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 101. BAN APPN Scenario: BAN Configuration for Router B

Notes:

1 Configure source routing on the token-ring port.

2 Add the frame-relay port to the bridge and enable source routing.

3 Configure BAN for the frame-relay port. Configure the BAN DLCI MAC address, the Boundary Node Identifier MAC, and choose bridged traffic.

6.4 Configuring a Permanent Circuit Using ISDN

This example is a configuration of a permanent circuit using frame relay over ISDN from node 21 to node 1.

Note: You configure a permanent circuit by setting the idle timer value to 0.

```
*************************************************************************
****  Configuring a PERMANENT circuit via ISDN from NN21 to NN1
****  Using Frame Relay over ISDN
*************************************************************************

Config>n 6
Circuit configuration
Od>li all

 Base net                       = 3
 Destination name               = 2216-01
 Circuit priority               = 8
Destination address: subaddress = 99199994301:

 Inbound destination name       = 2216-01
Inbound dst address: subaddress = 99199994301:

 Inbound calls                  = allowed
 Idle timer                     = 0 (fixed circuit)   1
 SelfTest Delay Timer           = 150 ms

Od>

*************************************************************************
**** Verify that a FR PVC is defined to NN1. This is required for APPN
*************************************************************************

Od>en
Frame Relay user configuration
FR Config>li perm

  Maximum PVCs allowable =      64
  Total PVCs configured  =       1

             Circuit              Circuit   Circuit   CIR     Burst  Excess
              Name                Number     Type    in bps   Size   Burst
 ------------------------------- ------- ---------- ------- ------- -------
2216-21-i6           2             16     Permanent 64000    64000     0

FR Config>ex
Od>ex
```

Figure 102. APPN Using Frame Relay over ISDN: ISDN Circuit

```
Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [  ] ? f
Interface number(Default 0): [0 ] ? 6
Port name (Max 8 characters) [FR006 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
 Service any node: (Y)es (N)o [Y ] ?
 Limited resource: (Y)es (N)o [N ] ?
 High performance routing: (Y)es (N)o [Y ] ?
 Maximum BTU size (768-2044) [2044 ] ?
 Maximum number of link stations (1-976) [512 ] ?
 Percent of link stations reserved for incoming calls (0-100) [0 ] ?
 Percent of link stations reserved for outgoing calls (0-100) [0 ] ?
 Local SAP address (04-EC) [4 ] ?
 Support bridged formatted frames: (Y)es (N)o [N ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>
```

Figure 103. APPN Using Frame Relay over ISDN: APPN Port

```
APPN config>add li
APPN Station
Port name for the link station [  ] ? fr006
Station name (Max 8 characters) [  ] ? tonn1isdn
Station name (Max 8 characters) [  ] ? tonn1is
 Limited resource: (Y)es (N)o [N ] ?
 Activate link automatically (Y)es (N)o [Y ] ?
 DLCI number for link (16-1007) [16 ] ?
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0 ] ?
 High performance routing: (Y)es (N)o [Y ] ?
Edit Dependent LU Server: (Y)es (N)o [N ] ?
 Allow CP-CP sessions on this link (Y)es (N)o [Y ] ?
 CP-CP session level security (Y)es (N)o [N ] ?
 Configure CP name of adjacent node: (Y)es (N)o [N ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>ex
```

Figure 104. APPN Using Frame Relay over ISDN: APPN Station

```
APPN config>li all
NODE:
        NETWORK ID: STFNET
        CONTROL POINT NAME: NN21
        XID: 00000
        APPN ENABLED: YES
        MAX SHARED MEMORY: 4096
        MAX CACHED: 4000
DLUR:
        DLUR ENABLED: YES
        PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
             CN NAME       LINK TYPE  PORT INTERFACES
        ------------------------------------------------------------
COS:
        COS NAME
        --------
          #BATCH
        #BATCHSC
        #CONNECT
          #INTER
        #INTERSC
         CPSVCMG
        SNASVCMG
         #USRBAT
         #USRNOT
MODE:
         MODE NAME  COS NAME
        --------------------
         #USRBAT     #USRBAT
         #USRNOT     #USRNOT
PORT:
          INTF     PORT      LINK      HPR    SERVICE   PORT
         NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
        ------------------------------------------------------
            0      TR000   IBMTRNET    YES      YES      YES
            1    SDLC001       SDLC     NO      YES      YES
          254     DLS254        DLS     NO      YES      YES
            6      FR006         FR    YES      YES      YES   3
STATION:
         STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
          NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
        ------------------------------------------------------------
          TONN25    TR000    0004ACA2A407       YES     YES       0
          TONN31    TR000    4FFF00001031       YES      NO       0
           SDLC1  SDLC001              C1        NO      NO       2
         TONN103   DLS254    400000000103        NO      NO       0
         TONN1IS    FR006              16       YES     YES       0  4
LU NAME:
             LU NAME         STATION NAME           CP NAME
        ------------------------------------------------------------
APPN config>
```

Figure 105. APPN Using Frame Relay over ISDN: APPN Configuration Summary

Notes:

1. Idle timer = 0 gives a fixed circuit.
2. Frame relay PVC is defined.
3. This is the ISDN port.
4. This is the link station.

6.5 Configuring APPN over Dial-on-Demand Circuits

APPN is supported over dial-on-demand circuits for the following DLC types:

- APPN/PPP/ISDN
- APPN/FR/ISDN
- APPN/PPP/V.25bis

6.5.1 PU 2.1 Node Considerations

When configuring an APPN link station for PU 2.1 nodes over a dial-on-demand link, you should specify yes for the limited resource link station parameter. This allows APPN to:

- Consider this link as a viable link to be used for route computation, even though the link is not actually active. The link will automatically become active during LU-LU session activation for a session needing to use it.
- Deactivate the link station when there are no active sessions using this link.

You should not configure CP-CP sessions over a dial-on-demand link. CP-CP sessions are persistent sessions. That is, they should remain active as long as the link is active. Since the active session count will not go to zero in this case, the link will remain active.

Note: If you specify yes for the limited resource parameter for a PU 2.1 node, you must specify an adjacent CPNAME and a TG number in the range of 1 to 20.

6.5.2 PU 2.0 Node Considerations

When configuring an APPN link station for PU 2.0 nodes over a dial-on-demand link, you can specify yes for the limited resource link station parameter. This allows APPN to deactivate the link station when there are no active sessions using it.

Note: If limited resource is set to yes, link activation for this link station must be initiated by either the DSPU (the PU 2.0) or by VTAM.

6.5.3 Considerations When Using DLUR for T2.0 or T2.1 Devices

For T2.0 or T2.1 nodes utilizing DLUR for dependent session traffic, an SSCP-PU and an SSCP-LU session must be active in order to establish an LU-LU session. These sessions are included in the session count for the link to the DSPU. Therefore, if limited resource is set to yes, the link will remain active as long as the SSCP-PU session is active or LU-LU sessions are active over this link.

If you specify no for the limited resource parameter, link deactivation is controlled by the node that initiated the connection.

If the link to the DSPU was activated due to the DSPU calling into the DLUR node or the DLUR node calling out to the DSPU (that is the link station to the DSPU

has been configured in the router and activate link automatically is set to yes), when the active session count goes to zero the link is deactivated by APPN DLUR only if the DSPU requested DACTPU. In this case, if the DLUS sends a DACTPU request to DLUR, DLUR will deactivate the SSCP-PU session. However, it will not deactivate the link to the DSPU. DLUR will attempt to re-establish the SSCP-PU session to the DLUS or the backup DLUS until it is successful or until the DSPU no longer needs this session.

If the link to the DSPU was activated by the DLUS and the session count goes to zero, the link is deactivated by APPN DLUR only if the DLUS sends a DACTPU request to DLUR.

6.5.4 A Sample APPN Scenario Using Dial-On-Demand

The following is a configuration example of dial-on-demand. This configuration is similar to the ISDN permanent connection except:

- You may want to configure this link so that CP-CP sessions do not use it. If you allow CP-CP sessions on this link, the link will not disconnect.
- You must specify that the link is a limited resource.
- You must define the adjacent CP name.
- You must specify a TG number.

You configure both sides of the communication link the same way.

```
*t 6
Gateway user configuration
Config>
************************************************************************
****  This is the NN6 configuration for a   NN6----NN15  dial-on-demand link.
****  The NN15 config will look just like this.
****  interface 9 is a Dial On Demand link with destination = NN15

************************************************************************
Config>n 9
Circuit configuration
Od>li all

Base net                        = 6
Destination name                = 2216-15
Circuit priority                = 8

Inbound destination name        = 2216-15

Inbound calls                   = allowed
Idle timer                      = 60 sec  1
SelfTest Delay Timer            = 150 ms

Od>ex
```

Figure 106. APPN over PPP Dial-on-Demand: Circuit Configuration

```
*************************************************************************
**** Configure APPN Port for the Interface
*************************************************************************
Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw [  ] ? p
Interface number(Default 0): [0 ] ? 9
Port name (Max 8 characters) [PPP009 ] ?

Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
 Service any node: (Y)es (N)o [Y ] ?
 Limited resource: (Y)es (N)o [Y ] ?  2
 ****  note that limited resource = YES
 High performance routing: (Y)es (N)o [Y ] ?
 Maximum BTU size (768-2044) [2044 ] ?
 Local SAP address (04-EC) [4 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>
```

Figure 107. APPN over PPP Dial-on-Demand: APPN Port

```
*************************************************************************
**** Configure the linkstation for the DOD link to NN15
*************************************************************************
APPN config>add li
APPN Station
Port name for the link station [  ] ? ppp009
Station name (Max 8 characters) [  ] ? to15dod
 Limited resource: (Y)es (N)o [Y ] ?  2
**** < note limited resource= YES
 TG Number (1-20) [1 ] ?    3
**** < note TG number is required input for limited resource
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node [0 ] ?
 High performance routing: (Y)es (N)o [Y ] ?
 Allow CP-CP sessions on this link (Y)es (N)o [Y ] ? N  4
**** < Be sure to NOT allow CP-CP sessions, or link won't hang up
Fully qualified CP name of adjacent node (netID.CPname) [ ] ? stfnet.NN15
**** < Adjacent node name required for limited resource links 5
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>
```

Figure 108. APPN over PPP Dial-on-Demand: APPN Station

```
APPN config>li all
NODE:
 NETWORK ID: STFNET
 CONTROL POINT NAME: NN6
 XID: 00000
 APPN ENABLED: YES
 MAX SHARED MEMORY: 4096
 MAX CACHED: 4000
DLUR:
 DLUR ENABLED: YES
 PRIMARY DLUS NAME: NETB.MVSC
 CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
 COS:
 COS NAME
 --------
BATCH
BATCHSC
CONNECT
INTER
INTERSC
CPSVCMG
SNASVCMG
USRBAT
USRNOT
MODE:
  MODE NAME  COS NAME
 ---------------------
   USRBAT      USRBAT
   USRNOT      USRNOT
 PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 -------------------------------------------------------
     0      TR000   IBMTRNET    YES      YES      YES
     1     PPP001        PPP    YES      YES      YES
     2         SS       SDLC     NO      YES      YES
     3                  SDLC     NO      YES       NO
     4                   PPP    YES      YES       NO
     5      TR005   IBMTRNET    YES      YES      YES
   254                   DLS     NO      YES       NO
    17     PPP017        PPP    YES      YES      YES
     9     PPP009        PPP    YES      YES      YES   6
```

Figure 109 (Part 1 of 2). APPN over PPP Dial-on-Demand: APPN Configuration Summary

```
STATION:
 STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
  NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
-------------------------------------------------------------
   TONN1    TR000    0004AC4E7505       YES     YES       1
   TONN2    TR000    550020004020       YES     YES       1
   TONN9    TR000    0004AC4E951D       YES     YES       1
   TOPC4    TR000    0004AC9416B4       YES     YES       1
 TOVTAM1    TR000    400000003888       YES     YES       1
  TONN35   PPP001    000000000000       YES     YES       0
 TO15DOD   PPP009    000000000000       YES      NO       0   7
LU NAME:
      LU NAME         STATION NAME           CP NAME
-------------------------------------------------------------
```

Figure 109 (Part 2 of 2). APPN over PPP Dial-on-Demand: APPN Configuration Summary

Notes:

1 Idle timer > 0 means dial-on-demand.

2 This is a limited resource.

3 TG number is required for a limited resource.

4 Do not allow CP-CP sessions on this link.

5 Provide a fully-qualified CP name.

6 This is the port.

7 This is the link station.

6.6 Configuring V.25bis

The following is a sample V.25bis configuration that could be used when APPN traffic uses PPP over V.25bis:

```
Config>list device
Ifc 0 Token Ring                      Slot: 100663296  Port: 0
Ifc 1 WAN PPP                         Slot: 529952  Port: 527616
Ifc 2 WAN X.25                        Slot: 529984  Port: 527872
Config>set data v25 2
Config>list device
Ifc 0 Token Ring                      Slot: 100663296  Port: 0
Ifc 1 WAN PPP                         Slot: 529952  Port: 527616
Ifc 2 WAN V.25bis                     Slot: 529984  Port: 527872
Config>add v25
Assign address name (1-23) chars []? brown
Assign network dial address (1-30 digits) []? 555-1211.
Config>add v25
Assign address name (1-23) chars []? gray
Assign network dial address (1-30 digits) []? 555-1212

Config>list v25

Address assigned name             Network Address
----------------------            ---------------
brown                             555-1211
gray                              555-1212

Config>
```

Figure 110. APPN using PPP over V.25bis: V.25bis Interface

```
Config>add device dial
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use net 3 command to configure circuit parameters

Config>net 3
Circuit configuration
Circuit config:   3>list all

Base net                       = 0
Destination name               =
Circuit priority               = 8

Outbound calls                 = allowed
Inbound calls                  = allowed
Idle timer                     = 60 sec   1
SelfTest Delay Timer           = 150 ms

Circuit config:   3>set net
Base net for this circuit [0]? 2
Circuit config:   3>set idle 0           2
Circuit config:   3>set dest
Assign destination address name []? brown
Circuit config:   3>list all

 Base net                       = 2
 Destination name               = brown
 Circuit priority               = 8
Destination address: subaddress = 555-1211

 Outbound calls                 = allowed
 Inbound calls                  = allowed
 Idle timer                     = 0 (fixed circuit)
 SelfTest Delay Timer           = 150 ms


Circuit config:   3>ex
```

Figure 111. APPN using PPP over V.25bis: Configure Circuit to Remote Node

```
Config>net 2
V.25bis Data Link Configuration
V25bis Config>list all
         V.25bis Configuration
Local Network Address Name    = Unassigned
No local addresses configured

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Cable type                    = V.35 DTE

Speed (bps)                   = 2048000
V25bis Config>set local
Local network address name   []? gray
V25bis Config>list all
         V.25bis Configuration
Local Network Address Name    = gray
Local Network Address         = 555-1212

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds
Cable type                    = V.35 DTE
Speed (bps)                   = 2048000

V25bis Config>
```

Figure 112. APPN using PPP over V.25bis: Configure Local V.25 Interface

Notes:

1 A non-zero value for Idle Timer results in a dial-on-demand link.

2 A zero value results in a leased link.

6.7 Configuring APPN Use of SDLC

APPN supports the following SDLC stations:

- Primary point-to-point
- Secondary point-to-point
- Negotiable point-to-point
- Primary multipoint

Using the talk 5 command interface for SDLC, you can:

- Enable/disable a SDLC link

- Update SDLC station parameters.

In order to activate an APPN connection to the remote SDLC link station, you must configure and activate the APPN SDLC link station in the router. This enables the APPN link station in the router to receive an activation XID from the remote SDLC link station. This is different from other DLC types, such as token-ring or Ethernet, whose APPN link stations do not need to be explicitly defined for APPN in the router since APPN has the capability to dynamically define these types of link stations.

6.8 Configuring ESCON for APPN

2216 Only

ESCON is available for the 2216, but not for the 2210. MAS V1R1.1 is required for ESCON support.

Note: We did not have an ESCON adapter to test, and the level of MAS we used did not support ESCON. The information included in this section is based on preliminary information, and the detail is *subject to change* by the availability date.

6.8.1 An Overview of ESCON and APPN

There are three basic steps when configuring APPN use of ESCON:

1. Define the slot used by the ESCON adapter.
2. Configure the ESCON logical resources that are to use the adapter.
3. Configure APPN use of one or more of these logical resources.

6.8.1.1 ESCON Physical Interface

The basic characteristics of the ESCON support are:

- A maximum of four ESCON adapters per 2216.
- Each adapter provides one physical ESCON connection.
- Each adapter supports up to 32 subchannels.
- If EMIF and/or ESCON directors are used, each adapter is capable of connecting to up to 32 host images (though, in many cases, the practical limit is usually 16, because most of the protocols that use ESCON require at least two subchannels, one for each direction).

At the adapter level, the only configuration action required is to add an ESCON device, and specify the adapter slot number. Most of the configuration effort is applied to the logical definitions that apply on top of the physical definition.

An example of adding a physical ESCON adapter is shown in Figure 113 on page 192.

```
*talk 6
Gateway user configuration
Config>add device escon
Device Slot #(1-8) [1]?                          1
Adding Nways ESCON Channel device in slot 1  port 1 as interface #4
Use "net 4" to configure Nways ESCON Channel parameters
Config>
```

Figure 113. Adding an ESCON Adapter

Note:

1 This is the slot in which the adapter is installed.

6.8.1.2 ESCON Virtual Interfaces

You need to define one or more logical entities (sometimes referred to as virtual network handlers, or just virtual interfaces) for each ESCON adapter.

Most of these virtual interfaces are related directly to a particular ESCON adapter:

- Up to 16 of these adapter-related virtual interfaces can be defined for each adapter.
- There are four types of adapter-related virtual interfaces:
  - LAN Channel Station (LCS)
  - Link Services Architecture (LSA)
  - Link Services Architecture Loopback
  - Multi-Path Channel Plus (MPC+)
- LSA and LCS instances may be mixed on one adapter.
- MPC+ instances cannot be mixed with either LSA or LCS instances on one adapter.

An ESCON adapter identifies the particular host system and a subchannel used by the virtual interface from information contained in the ESCON message headers. This information consists of:

Link address	The ESCON director port number of the host channel
LPAR number	The partition number of the host image if EMIF is used
CU image number	The logical control unit number used within the ESCON adapter
Device address	The address within the logical control unit used for the subchannel

APPN loopback is an additional type of virtual interface that is not specific to any particular ESCON adapter, and is only used for APPN LSA support.

The various virtual interfaces are used for different purposes and have their own particular configuration characteristics.

LAN Channel Station (LCS): LCS provides the following support:

- Used for access to mainframe TCP/IP.
- Supports the protocol used by the 3172 Interconnect Control Program (ICP) for TCP/IP.

- All TCP/IP traffic goes via the IP router function in the 2216.
- Each LCS instance must be in a different IP subnet.
- Each LCS instance is dedicated to a single host TCP/IP instance.
- Each LCS instance requires two subchannels, one for read and one for write.
- Multiple LCS instances on the same adapter may share the same host subchannels, by using a different relative LAN adapter number and/or LAN type.
- In addition to the ESCON address, a host TCP/IP subsystem selects an LCS instance by specifying a LAN type and relative LAN adapter number.
- An LCS instance cannot be shared across different adapters.
- Each LCS instance is configured to have either a token-ring or an Ethernet appearance.
- Each LCS instance is configured with a specified MAC address.

Link Services Architecture (LSA): LSA provides the following support:

- Used by the SNA Gateway function (non-APPN, from a 2216 perspective) to access VTAM.
- Supports the protocol used by the IBM 3172 Interconnect Control Program (ICP) for SNA.
- Requires VTAM V3R4 or higher.
- An LSA instance supports a single direct LAN interface (real, or emulated over ATM using FC LANE).
- An LSA instance uses the MAC address of the associated direct LAN interface.
- An LSA instance uses the SAP addresses it is instructed to open by VTAM. (Note that different SAPs are used for APPN and an LSA instance if a direct LAN interface is shared.)
- An LSA instance supports up to 255 LLC connections per opened SAP. (Note that there is a 2216-wide limit of 1500 LLC connections.)
- Each LSA instance requires a single host subchannel, which is used for both reading and writing, per VTAM.
- Multiple LSA instances on the same adapter may share the same host subchannel, by using a different relative LAN adapter number and/or LAN type.
- In addition to the ESCON address, VTAM selects an LSA instance by specifying a LAN type and relative LAN adapter number.
- An LSA instance cannot be shared across different adapters.
- An LSA instance may be shared by multiple VTAMs, but each must use different SAPs.

Link Services Architecture Loopback (LSA Loopback): LSA loopback provides the following support:

- Used for SNA (non-APPN, from a 2216 perspective) access to VTAM from DLSw attached resources.
- Used for 2216 APPN (ISR) access to VTAM.

- Uses the protocol used by the IBM 3172 Interconnect Control Program (ICP) for SNA.
- An LSA loopback instance may be shared by both 2216 APPN and SNA over DLSw.
- Requires VTAM V3R4 or higher for non-APPN.
- Requires VTAM V4R2 or higher for APPN.
- An LSA loopback instance uses a specified MAC address.
- An LSA loopback instance uses the SAP addresses it is instructed to open by VTAM.
- An LSA loopback instance supports up to 255 LLC connections per opened SAP. (Note that there is a 2216-wide limit of 1500 LLC connections. Also note that a connection that uses remote DLSw requires two LLC control blocks; one at the LSA instance and one for the DLSw connection to the remote DLSw partner.)
- Each LSA loopback instance requires a single host subchannel, which is used for both reading and writing, per VTAM.
- Multiple LSA loopback instances on the same adapter may share the same host subchannel, by using a different relative LAN adapter number and/or LAN type.
- In addition to the ESCON address, VTAM selects an LSA loopback instance by specifying a LAN type and relative LAN adapter number.
- An LSA loopback instance cannot be shared across different adapters.
- An LSA loopback instance may be shared by multiple VTAMs, but each must use different SAPs.

An example of defining an LSA loopback instance is shown in Figure 114 on page 195.

```
Config>network 4                                          1
ESCON Config>add lsa                                      2
ESCON Add Virtual>enable loopback                         3
Enabling loopback through network 5.
Please set the MAC address using the "MAC" command
ESCON Add Virtual>mac address 40:00:22:16:00:05           4
ESCON Add Virtual>subchannel add
ESCON Add LSA Subchannel>device 0                         5
ESCON Add LSA Subchannel>exit
ESCON Add Virtual>subchannel list
          Sub  0   Device address   :  0   LPAR number        : 0
                   Link address     :  1   CU Image number    : 0
ESCON Add Virtual>lantype
Please select one of the following LAN types:
    E  Ethernet
    T  Token Ring
LSA LAN Type: [E]? t                                      6
ESCON Add Virtual>exit
ESCON Config>list all                                     7
Net:  5   Protocol: LSA    LAN type: Token Ring           LAN number:  0
          Maxdata: 2052
          Loopback is enabled.
          MAC address: 400022160005
          Sub  0   Dev addr:  0  LPAR: 0  Link addr:  1  CU num: 0

ESCON Config>
```

Figure 114. Defining an LSA Loopback Instance

Notes:

1. This is the logical interface number assigned to the physical ESCON adapter.
2. Add an LSA instance to the ESCON adapter.
3. Make it an LSA loopback instance rather than one used by the SNA Gateway function.
4. Assign a MAC address to the LSA loopback instance.
5. Assign a device address to the subchannel. Although not shown, it is also possible to specify the:
   - Host ESCON Director port (Link address)
   - Host LPAR number
   - Control unit logical number (CU number)
6. Set the LAN type to token-ring.
7. List all the virtual instances defined on the physical adapter.

Although not shown, it is possible to specify a different MAXDATA value.

APPN Loopback: APPN loopback provides the following support:

- APPN loopback instances are only used if APPN is to use one or more LSA loopback instances.
- One or two APPN loopback interfaces can be configured.

- An APPN loopback instance can be shared across multiple ESCON adapters (rather than being dedicated to a specific adapter).
- Each APPN loopback instance is configured either as a token-ring or an Ethernet interface.
- Each APPN loopback instance is allocated a unique MAC address.
- Each APPN loopback instance can be used to connect to any LSA loopback instance, regardless of with which ESCON adapter it is associated.

An example of configuring an APPN loopback interface is shown in Figure 115.

```
ESCON Config>add appn loopback                                    1
ESCON Add Virtual>lantype                                         2
Please select one of the following LAN types:
    E  Ethernet
    T  Token Ring
APPN LAN Type: [T]?                                               2
ESCON Add Virtual>mac address                                     3
MAC address in 00:00:00:00:00:00 form [000000000000]? 40:00:22:16:00:09
ESCON Add Virtual>exit
ESCON Config>list all                                             4
Net:  9   Protocol: APPN Loopback   LAN type: Token-Ring/802.5
          APPN loopback MAC address: 400022160009

Net:  5   Protocol: LSA    LAN type: Token Ring           LAN number:  0
          Maxdata: 2052
          Loopback is enabled.
          MAC address: 400022160005
          Sub  0   Dev addr:  0  LPAR: 0  Link addr:  1  CU num: 0

ESCON Config>
```

Figure 115. Defining an APPN Loopback Interface

Notes:

1. Define an APPN loopback instance.
2. Specify the type of emulated LAN.
3. Specify the MAC address that APPN will use for this port.
4. This shows an LSA loopback instance and an APPN loopback instance.

Multi-Path Channel Plus (MPC+): MPC+ provides the following support:

- Each MPC+ group requires at least one read and one write subchannel, but multiple read and write subchannels may be included in the group if performance or availability requires it.
- Used for APPN HPR traffic *only*.
- All traffic passes through the APPN routing function in the 2216.
- Requires VTAM V4R4 or higher.
- An MPC+ group cannot be shared across different adapters.

An example of defining an MPC+ group is shown in Figure 116 on page 197.

```
Config>network 6                                              1
ESCON Config>add mpc                                          2
ESCON Add Virtual>subchannel addread                          3
ESCON Add MPC+ Read Subchannel>device 8                       4
ESCON Add MPC+ Read Subchannel>exit
ESCON Add Virtual>subchannel addwrite                         5
ESCON Add MPC+ Write Subchannel>device 10                     6
ESCON Add MPC+ Write Subchannel>exit
ESCON Add Virtual>subchannel list
          Read Subchannels:
          Sub  0   Device address   :  8   LPAR number        : 0
                   Link address     :  1   CU Image number    : 0
          Write Subchannels:
          Sub  1   Device address   : 10   LPAR number        : 0
                   Link address     :  1   CU Image number    : 0
ESCON Add Virtual>subchannel addread                                7
ESCON Add MPC+ Read Subchannel>device 9
ESCON Add MPC+ Read Subchannel>exit
ESCON Add Virtual>subchannel addwrite                               8
ESCON Add MPC+ Write Subchannel>device 11
ESCON Add MPC+ Write Subchannel>exit
ESCON Add Virtual>sub lis
          Read Subchannels:
          Sub  0   Device address   :  8   LPAR number        : 0
                   Link address     :  1   CU Image number    : 0
          Sub  1   Device address   :  9   LPAR number        : 0
                   Link address     :  1   CU Image number    : 0
          Write Subchannels:
          Sub  2   Device address   : 10   LPAR number        : 0
                   Link address     :  1   CU Image number    : 0
          Sub  3   Device address   : 11   LPAR number        : 0
                   Link address     :  1   CU Image number    : 0
ESCON Add Virtual>exit
ESCON Config>list all
Net:  8   Protocol: MPC+   LAN type: MPC+                 LAN number:  0
          Maxdata: 2048
          Reply TO: 45000   Sequencing Interval Timer: 3000
          Read Subchannels:
          Sub  0   Dev addr:  8  LPAR: 0  Link addr:  1  CU num: 0
          Sub  1   Dev addr:  9  LPAR: 0  Link addr:  1  CU num: 0
          Write Subchannels:
          Sub  2   Dev addr: 10  LPAR: 0  Link addr:  1  CU num: 0
          Sub  3   Dev addr: 11  LPAR: 0  Link addr:  1  CU num: 0

ESCON Config>exit
Config>exit
ESCON configuration changes has been changed.
Do you wish to keep the changes? [Yes]:
Config>write
Config Save: Using bank A and config number 2
Config>
```

Figure 116. Defining an MPC+ Group

Notes:

1. This is the logical interface number assigned to the physical ESCON adapter.

2. Add an MPC+ group.
3. Add a read subchannel to the group.
4. Assign a device address to the subchannel. Although not shown, it is also possible to specify the:
   - Host ESCON Director port (Link address)
   - Host LPAR number
   - Control unit logical number (CU number)
5. Add a write subchannel to the group.
6. Assign a device address to the subchannel.
7. Add a second read subchannel.
8. Add a second write subchannel.

Although not shown, it is also possible to specify non-default values for:

- MAXDATA
- Reply timeout
- Sequencing interval timer

6.8.2 Configuring APPN Using ESCON LSA

The APPN loopback interfaces are used to connect APPN to LSA loopback instances. These are not real LAN interfaces in the normal manner, but internal interfaces that appear to be LAN ports to APPN and are defined as part of the ESCON configuration of LSA loopback instances. Typically, one is used for LSA instances that have a token-ring appearance, and the other for those with an Ethernet appearance. If only one type of LAN appearance is used for LSA loopback instances, there is no need to define more than one of these APPN loopback interfaces.

As far as APPN configuration is concerned, a port is defined for each of the defined APPN loopback interfaces. The port appears to be a LAN interface, and takes the MAC address defined for the particular APPN loopback interface. Stations can be defined for each LSA loopback instance with which that APPN port is to communicate. The MAC address of a station is the MAC address assigned to the particular LSA loopback instance. From a VTAM perspective, the address of the APPN node in the 2216 is the MAC address of an APPN loopback interface.

The LSA loopback instances are not dedicated to APPN, but may also be used for SNA-to-host traffic that is presented by DLSw. (In this case, the SNA traffic from DLSw does not go via the APPN function in the 2216, though an alternative approach is to connect the SNA traffic from DLSw into APPN.)

6.8.3 Configuring APPN Using ESCON MPC+

The MPC+ groups are defined as part of the ESCON interface configuration, and an interface number is allocated to each group. To APPN, an MPC+ group is just an interface on which a port is defined.

Chapter 7. APPN Monitoring and Problem Investigation

This chapter describes the facilities that are available on the router to monitor and trouble-shoot APPN.

7.1 Monitoring APPN

The command line interface provides a number of functions that provide information about the active APPN configuration.

7.1.1 Accessing the APPN Console

To access the APPN console, use the sequence shown in Figure 117, starting from the base command line prompt.

```
*talk 5                                    1
+protocol appn                             2
APPN GWCON
APPN >                                     3
```

Figure 117. Accessing the APPN Console

Notes:

1. '*' is the base command line. talk 5 is used to enter console operation mode. The result is the + prompt.
2. '+' is the base console prompt. You can access the APPN console from this prompt.
3. This is the APPN console prompt. To leave this mode, type exit to return to base console mode.

7.1.2 APPN Console Commands

Table 7 summarizes the APPN console commands for monitoring APPN. For more detailed information on these commands and their parameters, see the *Protocol Configuration and Monitoring Reference, Volume 2*.

Table 7 (Page 1 of 2). APPN Console Command Summary

Command	Function
? (Help)	Lists all of the APPN configuration commands, or lists the options associated with specific commands.
Dump	Creates an APPN dump. • Saved on the hard disk (2216 only). • Transmitted to a remote dump server (2210 only).
Stop	Stops APPN.
Restart	Restarts APPN.

Table 7 (Page 2 of 2). APPN Console Command Summary

Command	Function
List	Lists: • Config - Displays all the APPN configuration parameters. • CP-CP_sessions - Displays information on active CP-CP sessions. • Dumps - Displays information on any APPN dumps stored on the hard disk (2216 only). • ISR_sessions - Displays information on active ISR sessions. • Link_information - Displays information on all links unless a particular station is requested. • Port_information - Displays information on all ports unless a particular port is requested. • RTP_sessions - Displays information on active RTP sessions. • Session_information - if Save RSCV information for intermediate nodes is set to Yes, displays origin CP name, primary LU name, and secondary LU name.
Memory	Obtains and displays APPN memory usage information.
Transmit	Transmits an APPN dump from the hard file to a workstation in the network using TFTP (2216 only).
Exit	Exits the APPN Monitoring process and returns to the + prompt.

7.1.3 Sample Display Command Output

Examples of the output from some of the list commands are shown in the following sections.

7.1.3.1 Ports

A sample list of ports is shown in Figure 118.

```
APPN >list port_information
Intf          Name       DLC Type        HPR          State
============================================================
  0          TR000       IBMTRNET       TRUE       ACT_PORT
  5          TR005       IBMTRNET       TRUE       ACT_PORT
APPN >
```

Figure 118. List of Ports

7.1.3.2 Link Stations

A sample list of link stations is shown in Figure 119 on page 201.

```
APPN >list link_information
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=========================================================================
     @@0       TKRB0    0    USIBMRA.WS0560O    EN    ACTIVE     ACT_LS
 R2210CS      SDLCB3    3    USIBMRA.RA2210D    NN  INACTIVE     ACT_LS
 R2210AD       DLSB4  254    USIBMRA.RA2210A    NN  INACTIVE     ACT_LS
APPN >
```

Figure 119. List of Link Information

7.1.3.3 CP-CP Sessions

A sample list of CP-CP sessions is shown in Figure 120.

```
APPN >list cp-cp_sessions
           CP Name      Type    Status  Connwiner ID    Conloser ID
=========================================================================
   USIBMRA.WS0560O       EN     Active    B6A235D7        B6A235D3
   USIBMRA.RA2210C       NN     Active    B6A23567        B6A23566
   USIBMRA.RA2210A       NN     Active    B6A23585        B6A23584
APPN >
```

Figure 120. List of CP-CP Sessions

7.1.3.4 ISR Sessions

A sample list of ISR sessions is shown in Figure 121.

```
APPN >list isr_sessions
  Adjacent CP Name  TG Number   ISR Sessions
=============================================
   USIBMRA.RA2210C      19             0
   USIBMRA.RA2210A      15             1
   USIBMRA.WS0560O      15             0
APPN >
```

Figure 121. List of ISR Sessions

If Save RSCV information for intermediate nodes is enabled during APPN configuration (an APPN management option), the list session_information command displays information about the session endpoints. See 4.3.6, “Collecting ISR Session Data” on page 136 for more information.

7.1.3.5 RTP Connections

A sample list of CP-CP sessions is shown in Figure 122 on page 202.
ISR-to-HPR boundary function is being performed for a session from WS05600.

```
APPN >list rtp_sessions
RTP PARTNER TABLE:
 Remote Partner Name  Remote Boundary Name  TG Number
======================================================
     USIBMRA.WSO5600         FFFFFFFF
RTP CONNECTION TABLE:
  TCID             CP Name  ISR  APPC  Pathswitch    Alive    COS TPF   TG Number
================================================================================
317740B0   USIBMRA.WSO5600    1    0    00000708  00000262     #INTER      15
3176CC08   USIBMRA.RA2210C    0    2    00000708  00000708    CPSVCMG      16
3176B0D8   USIBMRA.RA2210B    0    0    00000000  00000708     RSETUP      15
316AAB88   USIBMRA.RA2210B    0    2    00000708  00000708    CPSVCMG      15
APPN >
```

Figure 122. List of RTP Connections

7.1.3.6 Configuration

This command provides a display of the settings of all the APPN parameters. The output for a complete (but simple) configuration is shown in Figure 123.

```
APPN >list config
def_appn:
   def_node:
     netid:  USIBMRA
     cpname:  RA2216A
     id_number:  00000
     max_shared_mem:  5108
     max_dir_cache:  4000
     route_addition_resistance:  128
     hpr_max_sessions_per_connection:  100
     hpr_rtp_liveness_timer_low:  3
     hpr_rtp_liveness_timer_med:  3
     hpr_rtp_liveness_timer_high:  3
     hpr_rtp_liveness_timer_net:  3
     hpr_max_rtp_retries_low:  6
     hpr_max_rtp_retries_med:  6
     hpr_max_rtp_retries_high:  6
     hpr_max_rtp_retries_net:  6
     hpr_path_switch_timer_low:  180
     hpr_path_switch_timer_med:  180
     hpr_path_switch_timer_high:  180
     hpr_path_switch_timer_net:  180
     topo_safestore_interval:  100
     topo_safestore:  DISABLED
   edef_node:
```

Figure 123 (Part 1 of 5). Configuration List

```
def_dlur:
  dlur_enable:  DISABLED
edef_dlur:
def_collection:
  isr_information:  DISABLED
  isr_save_rscv:  DISABLED
edef_collection:
def_accounting:
  create_is_records:  DISABLED
  def_accounting_type:
    accounting_threshold:  0
    def_accounting_media:
      media_type:  MEMORY
      media_state:  DISABLED
      media_max_buffers:  1
      media_records_per_buffer:  100
      media_full_action:  STOP RECORDING
      media_record_format:  ASCII
    edef_accounting_media:
    def_accounting_media:
      media_type:  DASD
      media_state:  DISABLED
      media_max_buffers:  3
      media_records_per_buffer:  500
      media_full_action:  STOP RECORDING
      media_record_format:  ASCII
    edef_accounting_media:
  edef_accounting_type:
edef_accounting:
def_port:
  port_name:  TR000
  dlc_name:  IBMTRNET
  total_lim:  512
  percent_inbound_lim:  0
  percent_outbound_lim:  0
  max_btu_size:  2048
  service_any:  ENABLED
  hpr_supported:  ENABLED
  port_number:  0
  sap_value:  4
  local_hpr_sap:  C8
```

Figure 123 (Part 2 of 5). Configuration List

```
     connect_cost:  0
     byte_cost:  0
     security:  NONSECURE
     propagation_delay:  NEGLIGIBLE
     capacity:  75
     user_defined_1:  128
     user_defined_2:  128
     user_defined_3:  128
     timer_t1:  2
     timer_ti:  30
     timer_t2:  1
     max_retry_count:  8
     maxout_incr:  1
     maxout:  26
     maxin:  26
     limited_resource_timer:  180
     hpr_timer_t1_override:  2
     hpr_timer_ti_override:  2
     hpr_max_retry_override:  3
   edef_port:
```

Figure 123 (Part 3 of 5). Configuration List

```
def_ls:
  ls_name:  RAK
  port_name:  TR000
  adjacent_cpname:
  adjacent_node_type:  APPN END NODE
  auto_act_supported:  ENABLED
  activate_cp_cp_sessions:  ENABLED
  session_security_supported:  DISABLED
  hpr_supported:  ENABLED
  fq_cpname_pri_dlus:
  fq_cpname_backup_dlus:
  node_id:  00000000
  dest_mac:  400001240000
  hpr_remote_sap:  C8
  dest_sap:  4
  connect_cost:  0
  byte_cost:  0
  security:  NONSECURE
  propagation_delay:  NEGLIGIBLE
  capacity:  75
  user_defined_1:  128
  user_defined_2:  128
  user_defined_3:  128
  timer_t1:  2
  timer_ti:  30
  timer_t2:  1
  max_retry_count:  8
  maxout_incr:  1
  maxout:  26
  maxin:  26
  limited_resource_timer:  180
  hpr_timer_t1_override:  2
  hpr_timer_ti_override:  2
  hpr_max_retry_override:  3
  tg_num: 0
edef_ls:
```

Figure 123 (Part 4 of 5). Configuration List

```
   def_trace:
     process_mgmt:  DISABLED
     proc_proc_comm:  DISABLED
     locking:  DISABLED
     misc_tower_act:  DISABLED
     io_to_from_sys:  DISABLED
     store_mgmt:  DISABLED
     q_data_type_mgmt:  DISABLED
     t_data_type_mgmt:  DISABLED
     buf_mgmt:  DISABLED
     cfg_ctrl:  DISABLED
     timer_service:  DISABLED
     service_prov_mgmt:  DISABLED
     interprocess_mess_seg:  DISABLED
     cntl_proc_outside_scp:  DISABLED
     monitor_proc_svc_twr:  DISABLED
     dist_env_ctrl:  DISABLED
     proc_srv_dial:  DISABLED
     avl_tree_sprt:
APPN >
```

Figure 123 (Part 5 of 5). Configuration List

7.1.3.7 Memory Use

Figure 124 is an example display of the current shared memory use by APPN. In this case, the maximum shared memory value is set to 5108. The percent buffer memory is set to 11 percent, and the maximum cached directory entries is set to 4000. See 4.2.6, “Adjusting the APPN Memory for Network Size” on page 124 for an explanation of these parameters.

There is a memory command in talk 5 that you can use to display the overall memory usage in the router.

```
APPN >memory
APPN total shared memory size= 5230592, special use= 552
APPN main part: size = 4654685 crit_thresh= 3956410 cons_thresh= 3258220
APPN main part: inuse= 1108184
APPN bufr part: size = 575355 crit= 460240 cons= 373945 slow= 230120
APPN bufr part: inuse= 640 reserved (< slow)= 19192
APPN >
```

Figure 124. Displaying APPN Memory Use

7.2 APPN Traces

The APPN implementation on the router has extensive tracing capabilities. These are mainly intended for software debugging purposes, but some of the options may be of use to you. See 7.3.2, “APPN DLC Trace Events” on page 210 and 7.3.3, “APPN Configuration Events at Restart” on page 213 for two examples of this.

7.2.1 Enabling Traces

Figure 125 shows how to selectively enable tracing via the command line interface. All the options are listed.

```
APPN config>set traces
Edit Node-Level Traces (Y)es (N)o [N]? y
  Process management (Y)es (N)o [N]?
  Process to process communication (Y)es (N)o [N]?
  Locking (Y)es (N)o [N]?
  Miscellaneous tower activities (Y)es (N)o [N]?
  I/O to and from the system (Y)es (N)o [N]?
  Storage management (Y)es (N)o [N]?
  Queue data type management (Y)es (N)o [N]?
  Table data type management (Y)es (N)o [N]?
  Buffer management (Y)es (N)o [N]?
  Configuration control (Y)es (N)o [N]?
  Timer service (Y)es (N)o [N]?
  Service provider management (Y)es (N)o [N]?
  Interprocess message segmenting (Y)es (N)o [N]?
  Control of processes outside scope of this tower (Y)es (N)o [N]?
  Monitoring existence of processes, services, towers (Y)es (N)o [N]?
  Distributed environment control (Y)es (N)o [N]?
  Process to service dialogs (Y)es (N)o [N]?
  AVL tree support (Y)es (N)o [N]?
Component-level Traces
Edit Interprocess Signals (Y)es (N)o [N]? y
  Address space manager (Y)es (N)o [N]?
  Attach manager (Y)es (N)o [N]?
  Configuration services (Y)es (N)o [N]?
  Dependent LU requester (Y)es (N)o [N]?
  Directory services (Y)es (N)o [N]?
  Half session (Y)es (N)o [N]?
  HPR path control (Y)es (N)o [N]?
  Management services (Y)es (N)o [N]?
  Node operator facility (Y)es (N)o [N]?
  Path control (Y)es (N)o [N]?
  Presentation services (Y)es (N)o [N]?
  Resource manager (Y)es (N)o [N]?
  Session connector manager (Y)es (N)o [N]?
  Session connector (Y)es (N)o [N]?
  Session manager (Y)es (N)o [N]?
  Session services (Y)es (N)o [N]?
  Topology and routing services (Y)es (N)o [N]?
```

Figure 125 (Part 1 of 2). Enabling APPN Traces

```
Edit Module Entry and Exit (Y)es (N)o [N]? y
  Attach manager (Y)es (N)o [N]?
  Half session (Y)es (N)o [N]?
  Node operator facility (Y)es (N)o [N]?
  Presentation services (Y)es (N)o [N]?
  Rapid transport protocol (Y)es (N)o [N]?
  Resource manager (Y)es (N)o [N]?
  Session manager (Y)es (N)o [N]?
Edit General (Y)es (N)o [N]? y
  Accounting services (Y)es (N)o [N]?
  Address space manager (Y)es (N)o [N]?
  Architected transaction programs (Y)es (N)o [N]?
  Configuration services (Y)es (N)o [N]?
  Dependent LU requester (Y)es (N)o [N]?
  Directory services (Y)es (N)o [N]?
  HPR path control (Y)es (N)o [N]?
  Management services (Y)es (N)o [N]?
  Node operator facility (Y)es (N)o [N]?
  Path control (Y)es (N)o [N]?
  Problem determination services (Y)es (N)o [N]?
  Rapid transport protocol (Y)es (N)o [N]?
  Session connector manager (Y)es (N)o [N]?
  Session connector (Y)es (N)o [N]?
  Session services (Y)es (N)o [N]?
  SNMP subagent (Y)es (N)o [N]?
  Topology and routing services (Y)es (N)o [N]?
Miscellaneous traces
  Data link control transmissions and receptions (Y)es (N)o [N]? y
Write this record? [Y]?
APPN config>
```

Figure 125 (Part 2 of 2). Enabling APPN Traces

7.3 APPN Use of Event Logging System

The event logging system (ELS) can be used to monitor activity for the many different interfaces and protocols that the router supports. APPN events may be logged; two examples are shown later.

ELS allows event messages to be:

- Displayed interactively at a local or remote console, or at a Telnet terminal.
- Sent within traps to an SNMP manager.
- Collected in memory in a trace buffer. The trace buffer may be saved to hard disk (2216 only), viewed, or sent from the router using TFTP.

Note that APPN is just a protocol that uses the underlying interfaces, and as such, you may need to log events for the underlying interfaces (for example, SDLC, token-ring, or LLC) as well as APPN when investigating problems.

The event messages issued by all users of ELS are listed in the *Event Logging System Messages Guide*. Refer to this manual if you want a better understanding of specific messages, or if you want to get a feel for the event messages created by a component (subsystem). The latter can allow you to take a more informed view as to whether ELS might provide you with useful information in a particular circumstance.

7.3.1 Using ELS for APPN

Figure 126 shows a command line sequence that:

- Disables all ELS message displays.
- Lists all the APPN ELS event message templates.
- Enables the interactive display of the specific APPN event that is used for the DLC trace.
- Displays the active APPN events, which lists the count of each event type that ELS has received and the processing that is being applied to each one.
- Disables all ELS event message displays.

```
*talk 5
CGW Operator Console
+event                                                    1
Event Logging System user console
ELS>nodisplay subsystem all all                           2
ELS>list subsystem appn                                   3

Event      Level      Message

APPN.001   C-INFO     Rcvd netup for intf %d
APPN.002   C-INFO     Rcvd netdn for intf %d
APPN.

APPN.
APPN.027   C-INFO     APPN %S
APPN.028   ALWAYS     APPN %S

ELS>display event appn.014                                4
Complete
ELS>list active appn                                      5

Event      Active  Count

APPN.001           1
APPN.011           2
APPN.014   D       636                                    6
APPN.015           333
APPN.023           58
APPN.024           37
APPN.026           2
D=Display on   T=Trap on   P=Packet Trace on

ELS>nodisplay subsystem all all                           7
```

Figure 126. Using ELS for APPN

Notes:

1. This initiates ELS console mode.
2. This ensures any existing display of ELS events is terminated, for all subsystems.
3. This lists all the ELS event messages for the APPN subsystem. See Figure 127 on page 210 for the full output.

4 This starts the display of a specific APPN subsystem event.

5 This lists the APPN subsystem events that have been received, along with the number of each received.

6 The D shows that this particular event is in display status. T and P are used for trap and (packet) trace respectively.

7 This stops all ELS event displays.

```
ELS>list subsystem appn

Event      Level      Message

APPN.001   C-INFO     Rcvd netup for intf %d
APPN.002   C-INFO     Rcvd netdn for intf %d
APPN.003   C-INFO     Discarding APPN HPR pkt rcvd on dn intf.
APPN.004   C-INFO     Unkwn Dialog Msge rcvd
APPN.005   C-INFO     APPN rtry cnt exhstd.
APPN.006   C-INFO     APPN cannot be restarted
APPN.007   C-INFO     %dth attempt to restart APPN
APPN.008   C-INFO     APPN dumped to file
APPN.009   C-INFO     Stop APPN node
APPN.010   C-INFO     APPN node not running
APPN.011   UE-ERROR   APPN LOG: %S
APPN.012   UE-ERROR   APPN LOG: Part: %d Text: %S
APPN.013   C-INFO     APPN Msg: Comp: %S PrID: %X Op: %S Text: %S
APPN.014   P-TRACE    %S
APPN.015   P-TRACE    %S
APPN.016   P-TRACE    %S
APPN.017   C-INFO     %x
APPN.018   C-INFO     %x
APPN.019   C-INFO     %x
APPN.020   C-INFO     reserved
APPN.021   C-INFO     %x
APPN.022   C-INFO     reserved
APPN.023   C-INFO     DX %x %x %x %x
APPN.024   C-INFO     ***%S***
APPN.025   UE-ERROR   ***%S***
APPN.026   UE-ERROR   %S
APPN.027   C-INFO     APPN %S
APPN.028   ALWAYS     APPN %S

ELS>
```

Figure 127. APPN Subsystem ELS Event Messages

7.3.2 APPN DLC Trace Events

One APPN use of ELS that you may find helpful is the DLC level trace. An example of enabling the DLC trace is shown in Figure 128 on page 211. Once activated, trace entries will be passed to ELS by APPN, and then, depending on the monitoring parameters in use, ELS can display the events or log them.

```
APPN config>set trace
Edit Node-Level Traces (Y)es (N)o [N]?
Component-level Traces
 Edit Interprocess Signals (Y)es (N)o [N]?
Edit Module Entry and Exit (Y)es (N)o [N]?
Edit General (Y)es (N)o [N]?
Miscellaneous traces
  Data link control transmissions and receptions (Y)es (N)o [N]? y
Write this record? [Y]?
APPN config>
```

Figure 128. Enabling the DLC Level Trace

The sequence shown in Figure 126 on page 209 was used to enable the display of this event, and some sample output is shown in Figure 129. You can use such a sequence to see that there is in fact some communication activity, though note that there is no selective tracing by port at the APPN DLC level.

No DLC trace formatting is provided, but, if you are very keen, you can decode the data flow. There are 11 PIUs in the sample. If you look carefully after the Data Input: and Data Output: labels, the first two bytes give the length, in binary, of the SNA PIU, and this is followed by the SNA PIU itself. In this case, the PIUs start with a FID2 transmission header, and the rest of the data can be decoded if you persevere.

```
*talk 2                                    1
APPN.014: PSNA F1 2051F21B 331D700A B 1E2 Data Input:
00EF2C00010100660B90810E0502FF0003D000000422F0F0F3004312C481000020240380FF1660F
21B1969DEEBC63F0BC4C5C4C1D2F0F0F14BD4F207810000020240078200010000001384800101
APPN.014: F1.01
0E0EF6E4E2C9C2D4D9C14BD9C1D2003512CA05808044C00F3D00F6E4E2C9C2D4D9C14BD9C1D2093E078080FFFFFFF
F148200F3E4E2C9C2D4D9C14BD9C1F0F0C3C9C3F0006012C500040150000008404040404040404000002919O5C000
08E4E2C9
APPN.014: F1.02
C2D4D9C14008D9C1F0F0C3C9C3F008C4C5C4C1D2F0F0F108D9C1F0F0C3C9C3F01619002003D9C1D207E4E2C9C2D4D
9C103D9C1D200000C2C07087BC3D6D5D5C5C3E3
APPN.014: PSNA F2 2052E0EB 331D700A C EC Data Output:
00742E00000200140B9081310502FF0003D000000422F0F0F300180FE4E2C9C2D4D9C14BD9C1F2F
2F1F6C1331D6F5B0000000108367279783316D6FBA003A12C440000020241660F21B1969DEEBC6
APPN.014: F2.01 3F0BC4C5C4C1D2F0F0F14BD4F21B3508400007900212C40FE4E2C9C2D4D9C14BD9C1F2F2F1F6C100
```

Figure 129 (Part 1 of 3). Monitor Console - APPN DLC Trace (APPN.014)

```
APPN.014: PSNA F3 2051F21B 331D7010 B 1C2 Data Input:
00DF2C00010100670B90810E0502FF0003D000000422F0F0F3003412C481000020240380FF1A60C
B333B03F11653CB0FC1E3C2D4E6D5F0F14BE2E2C3D7F0F1078100000202400782000100000000
APPN.014: F3.01
3412CA05808044C00F3D00F6E4E2C9C2D4D9C14BD9C1D2093E078080FFFFFFFF138200F3E4E2C9C2D4D9C14BD9C1E
3E4C2C5E2006012C5000401500000084040404040404040000291904C00008E4E2C9C2D4D9C14008D9C1E3E4C2C5
E24008C1
APPN.014: F3.02 E3C2D4E6D5F0F108D9C1E3E4C2C5E2401619002003D9C1D207E4E2C9C2D4D9C103D9C1D200000
C2C07087BC3D6D5D5C5C3E3
APPN.014: PSNA F4 2052E0EB 331D7010 C F4 Data Output:
00782E00000200150B9081310502FF0003D000000422F0F0F300180FE4E2C9C2D4D9C14BD9C1F2F
2F1F6C1331D6F5B0000000108367287D0331D6FBC003E12C440000020241A60CB333B03F11653
APPN.014: F4.01 CB0FC1E3C2D4E6D5F0F14BE2E2C3D7F0F11B3508400007900212C40FE4E2C9C2D4D9C14BD9C1F
2F2F1F6C100
APPN.014: PSNA F5 2051F21B 331D701B B 1C2 Data Input:
00DF2C00010100680B90810E0502FF0003D000000422F0F0F3003412C481000020240380FF1A60C
B333B03F11653CB0FC1E3C2D4E6D5F0F14BE2E2C3D7F0F1078100000202400782000100000000
APPN.014: F5.01
3412CA05808044C00F3D00F6E4E2C9C2D4D9C14BD9C1D2093E078080FFFFFFFF138200F3E4E2C9C2D4D9C14BD9C1E
3E4C2C5E2006012C5000401500000084040404040404040000291905C00008E4E2C9C2D4D9C14008D9C1E3E4C2C5
E24008C1
APPN.014: F5.02 E3C2D4E6D5F0F108D9C1E3E4C2C5E2401619002003D9C1D207E4E2C9C2D4D9C103D9C1D200000
C2C07087BC3D6D5D5C5C3E3
APPN.014: PSNA F6 2052E0EB 331D701B C F4 Data Output:
00782E00000200160B9181310502FF0003D000000422F0F0F300180FE4E2C9C2D4D9C14BD9C1F2F
2F1F6C1331D6F5B0000000108367279783 31D6FBE003E12C440000020241A60CB333B03F11653
APPN.014: F6.01 CB0FC1E3C2D4E6D5F0F14BE2E2C3D7F0F11B3508400007900212C40FE4E2C9C2D4D9C14BD9C1F
2F2F1F6C100
APPN.014: PSNA F7 2051F21B 331D701B B 1C Data Input: 000C2F000200000008301000000008   2
APPN.014: PSNA F8 2051F21B 331D702B B 1E0 Data Input:
00EE2C00010100690B90810E0502FF0003D000000422F0F0F3004312C481000020250380FF1660F
6FF4164100F63CD0BE4E2C9C2D4D9C14BD9C1F3078100000202500782000100000001384800101
APPN.014: F8.01
0E0EF6E4E2C9C2D4D9C14BD9C1D2003412CA05808044800F3D00F6E4E2C9C2D4D9C14BD9C1D2093E078080FFFFFFF
F138200F3E4E2C9C2D4E2C34BE2C3F5F5C3E3D3006012C5000401500000084040404040404040000291909C40008
E4E2C9C2
APPN.014: F8.02
D4E2C34008E2C3F5F5C3E3D34008E4E2C9C2D4D9C14008E2C3F5F5C3E3D3401619002003D9C1D207E4E2C9C2D4D9C
103D9C1D200000C2C07087BC3D6D5D5C5C3E3
APPN.014: PSNA F9 2052E0EB 331D702B C EC Data Output:
00742E00000200170B9081310502FF0003D000000422F0F0F300180FE4E2C9C2D4D9C14BD9C1F2F
2F1F6C1331D6F5B0000000108367287D0331D6FC0003A12C440000020251660F6FF4164100F63
APPN.014: F9.01 CD0BE4E2C9C2D4D9C14BD9C1F31B3508400007900212C40FE4E2C9C2D4D9C14BD9C1F2F2F1F6C
100
```

Figure 129 (Part 2 of 3). Monitor Console - APPN DLC Trace (APPN.014)

```
APPN.014: PSNA FA 2051F21B 331D7030 B 1C0 Data Input:
00DE2C000101006A0B90810E0502FF0003D000000422F0F0F3003412C48100002024038OFF1A60C
B333B03F11653CD0FC1E3C2D4E6D5F0F14BE2E2C3D7F0F1078100000202400782000100000000
APPN.014: FA.01
3312CA05808044C00F3D00F6E4E2C9C2D4D9C14BD9C1D2093E078080FFFFFFFF128200F3E4E2C9C2D4D9C14BD9C1C
3C9C3E2006012C500040150000008404040404040404000002919O3C00008E4E2C9C2D4D9C14008D9C1C3C9C3E240
4008C1E3
APPN.014: FA.02 C2D4E6D5F0F108D9C1C3C9C3E240401619002003D9C1D207E4E2C9C2D4D9C103D9C1D200000C2
C07087BC3D6D5D5C5C3E3
APPN.014: PSNA FB 2052E0EB 331D7030 C F4 Data Output:
00782E00000200180B9081310502FF0003D000000422F0F0F300180FE4E2C9C2D4D9C14BD9C1F2F
2F1F6C1331D6F5B0000000108367279783316D6FC2003E12C440000020241A60CB333B03F11653
APPN.014: FB.01 CD0FC1E3C2D4E6D5F0F14BE2E2C3D7F0F11B3508400007900212C40FE4E2C9C2D4D9C14BD9C1F
2F2F1F6C100
```

Figure 129 (Part 3 of 3). Monitor Console - APPN DLC Trace (APPN.014)

Notes:

1. The monitor console is accessed by using talk 2 at the base command line prompt.
2. If you look carefully, you will see that this is an isolated pacing message.

7.3.3 APPN Configuration Events at Restart

Figure 130 is another ELS event message sample, this time of the APPN.024 messages issued during an APPN restart. This particular event is created by APPN configuration services.

Note that these are not the only events issued at APPN restart; we have just displayed that particular event.

```
*talk 2                          1
APPN.024: ***appnrst - Entering appn_restart with retries = 1***
APPN.024: ***appnrst - Calling AppnInit***
APPN.024: ***xxxcfg01 - CFG01 is here***
APPN.024: ***xxxcfg01 - About to read_sram***
APPN.024: ***xxxcfsrm - Entering read_sram***
APPN.024: ***xxxcfg01 - Starting appn node***
APPN.024: ***xxxcfstn - Creating NOF...***
APPN.024: ***xxxcfstn - enqueue DEF_LOCAL_CP verb***
APPN.024: ***xxxcfstn -  enqueue of ENABLE_TRACE verb***
APPN.024: ***xxxcfstn -  enqueue of DEF_ACS verb***
```

Figure 130 (Part 1 of 2). Monitor Console - Event APPN.024 - APPN Restart

```
APPN.024: ***xxxcfstn -  enqueue of DEF_COS verb for #BATCH***
APPN.024: ***xxxcfstn -  enqueue of DEF_COS verb for #BATCHSC***
APPN.024: ***xxxcfstn -  enqueue of DEF_COS verb for #CONNECT***
APPN.024: ***xxxcfstn -  enqueue of DEF_COS verb for #INTER***
APPN.024: ***xxxcfstn -  enqueue of DEF_COS verb for #INTERSC***
APPN.024: ***xxxcfstn -  enqueue of DEF_COS verb for #CPSVCMG***
APPN.024: ***xxxcfstn -  enqueue of DEF_COS verb for #SNASVCMG***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #BATCH***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #BATCHSC***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #CONNECT***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #INTER***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #INTERSC***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #BLANK***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #CPSVCMG***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #CPSVRMRG***
APPN.024: ***xxxcfstn -  enqueue of DEF_MODE verb for #SNASVCMG***
APPN.024: ***xxxcfstn - enqueue of DEF_DLC verb for IBMTRNET***
APPN.024: ***xxxcfstn - enqueue of DEF_PORT verb for TROOO***
APPN.024: ***xxxcfstn - enqueue of DEF_LINK verb for RAK***
APPN.024: ***xxxcfstn - enqueue of DEF_DFLTS verb***
APPN.024: ***xxxcfstn - enqueue of DEF_PERFORMANCE verb***
APPN.024: ***xxxcfstn - enqueue of START_AM verb***
APPN.024: ***xxxcfstn - enqueue of ACT_PORT verb for TROOO***
APPN.024: ***xxxcfstn - enqueue of ACT_LINK verb for all links***
APPN.024: ***xxxcfg01 - PE_SERVICE_ENABLED msg recvd***
APPN.024: ***xxxcfg01 - handle_netups***
```

Figure 130 (Part 2 of 2). Monitor Console - Event APPN.024 - APPN Restart

Note:

1 The monitor console is accessed by using talk 2 at the base command line prompt.

7.4 Other Useful Console Facilities

We found the following facilities useful.

7.4.1 APPN Configuration Display

In APPN configuration mode, the list command can be most useful. In particular, the summary configuration display that it provides gives a most useful overall view of the APPN configuration. An example is shown in Figure 131 on page 215.

```
APPN config>list all
NODE:
 NETWORK ID: USIBMRA
 CONTROL POINT NAME: RA2210B
 XID: 2210B
 APPN ENABLED: YES
 MAX SHARED MEMORY: 4096
 MAX CACHED: 4000
DLUR:
 DLUR ENABLED: NO
 PRIMARY DLUS NAME:
CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
COS:
 COS NAME
 --------
   #BATCH
 #BATCHSC
 #CONNECT
   #INTER
 #INTERSC
  CPSVCMG
 SNASVCMG
MODE:
  MODE NAME  COS NAME
 --------------------
PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 -----------------------------------------------------
     0      TKRB0   IBMTRNET    YES      YES      YES
   254      DLSB4       DLS     NO      YES      YES
     3     SDLCB3      SDLC     NO      YES      YES
STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
  R2210AD    DLSB4    40002210ADDD        NO     YES       0
  R2210CS   SDLCB3              D2        NO     YES       0
LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------
APPN config>
```

Figure 131. APPN Node Configuration Summary

7.5 Managing APPN from an External Manager

APPN on the router provides functions that enable it to be managed from network management platforms that use either SNA or SNMP protocols. This is discussed more fully in 2.2.4, “APPN Management” on page 22, which includes a list of the MIBs provided with the APPN implementation.

For unsolicited error information to be sent to such a management platform:

- For an SNMP-based platform, you must specify the destination of SNMP traps on the router as part of the configuration of SNMP.
- For an SNA-based platform, you must ensure that LU 6.2 management sessions are started to the router, so that alerts may be sent to, for example, host NetView.

For the SNMP-based platform to have full APPN management capability, set access must be configured as part of the SNMP configuration on the router.

For SNA-based topology management via the Integrator, appropriate entries must be made in the VTAM CMIP directory file, and the SNMP parameters (IP address and SNMP community name) of the router must be configured in the Integrator. Again, set access must be configured in SNMP to enable control commands to be issued from host NetView.

Part 2. Data Link Switching

Chapter 8. Data Link Switching for SNA

This chapter provides a brief overview of data link switching (DLSw), discusses configuration of data link switching on the 2210, and provides some configuration scenarios with the 2210.

8.1 Data Link Switching Overview

DLSw is designed to facilitate integration of SNA traffic into a multiprotocol network. DLSw functions include:

- Transporting of SNA in a multiprotocol routed backbone
- Dynamic re-routing in the wide area network
- Reliable delivery of SNA traffic
- Termination of LLC acknowledgments on the LAN segments
- Broadcast traffic control through the WAN
- LAN and WAN control for congestion and data flow

DLSw uses IP encapsulation of SNA as its transport vehicle across the internetwork. To supply the reliability SNA requires in the internetwork, DLSw uses Transmission Control Protocol (TCP) flows between edge-node routers (those routers joining the LAN segments to the IP portion of the network).

DLSw routers establish TCP connections to other DLSw routers using ports 2065 and 2067. Port 2065 is a read port on which all DLSw information is received, and port 2067 is a write port from which all DLSw information is sent.

DLSw also uses a technique known as DLC termination, or spoofing, to minimize T1 timer expirations and to keep acknowledgments isolated to the local LAN segment.

Spoofing is the process that acknowledges receipt of the frame on the local LAN segment by masquerading as the destination endstation. Spoofing keeps the receiver ready and/or supervisory poll frames from leaving their subnet media. Therefore it ensures local media response speeds to acknowledge layer 2 timers (T1 timers for example) and lessens the bandwidth overhead requirements in the WAN.

The DLSw technique is more easily understood if you consider circuit establishment between two endstations.

8.1.1 DLSw Circuit Establishment

Figure 132 on page 220 shows the configuration used in this explanation of DLSw circuit establishment.

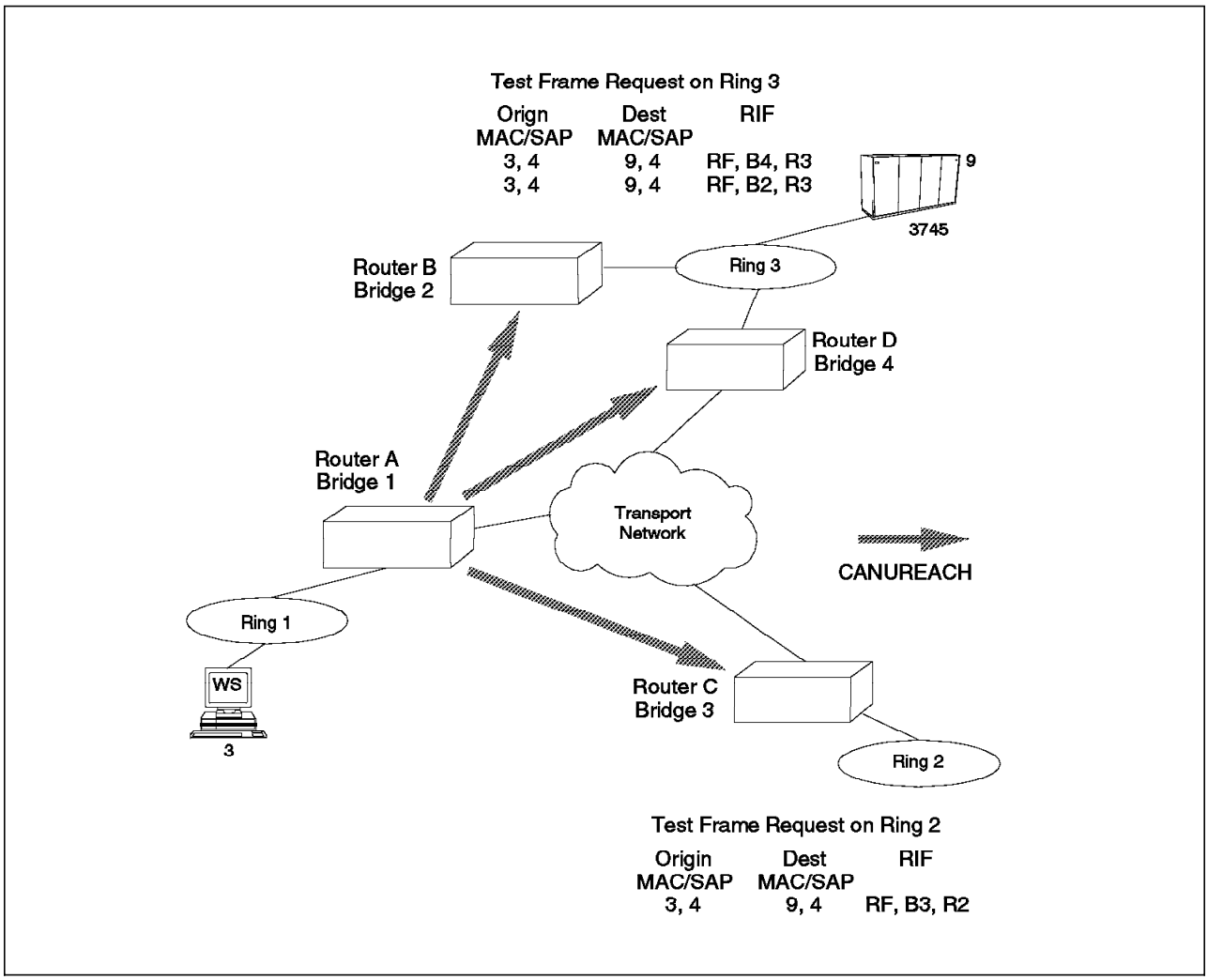


Figure 132. Circuit Establishment

An endstation (workstation 3) requests SNA connectivity to another end station (3745) by sending out an explorer frame. This frame contains the source MAC and SAP addresses of workstation 3 and the destination MAC and SAP addresses of the 3745. When router A sees the broadcast explorer frame, the DLSw function in router A sends a CANUREACH request over the TCP/IP connections to each of the DLSw participating routers in its list. These partner routers broadcast the explorer frame on the LAN subnetworks to which they are connected. Since router B and D in this example are connected to the same LAN subnet, two explorer frames are sent to the 3745. The 3745 views the data as coming from a phantom ring segment one hop beyond router B and D. This is because the RI field of the explorer frames coming from router B and D shows that workstation 3 is on a phantom ring segment (RF) immediately on the other side of routers B and D. In effect, a 2210 with DLSw actually uses source route bridging on its LAN ports to bridge the frames into the router. However, once in the router, the DLSw code encapsulates the SNA packet in TCP packets to be routed through the IP internetwork.

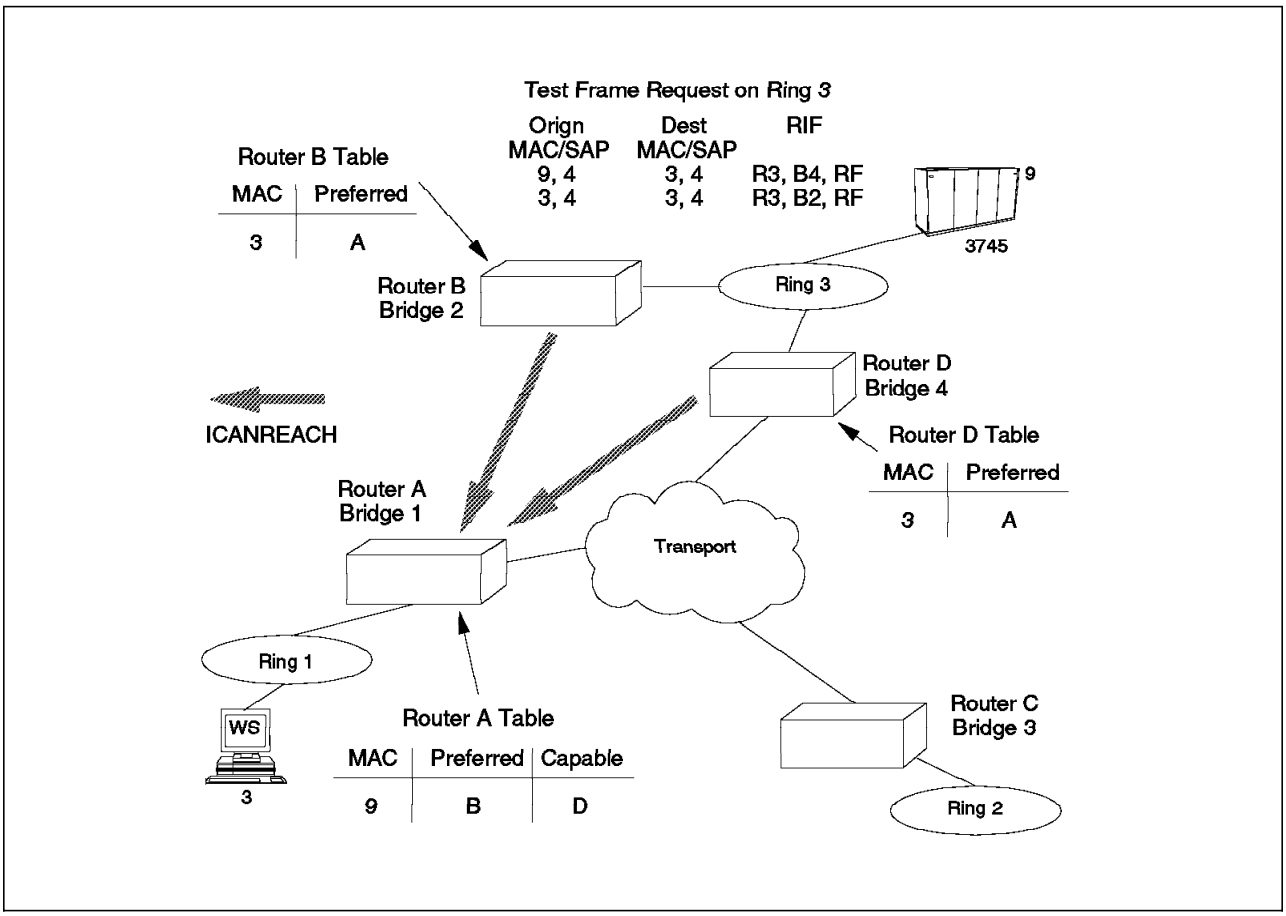


Figure 133. Circuit Establishment Completion

In Figure 133, the 3745 responds to the explorer frames. These responses are sent to routers B and D. Therefore, routers B and D both send back ICANREACH responses to router A. Routers B and D cache this information so that any future requests from workstations on their LAN ports to reach workstation 3 can be satisfied by sending a specific CANUREACH frame to router A rather than querying each of the participating router partners on the network. When router A receives the two responses to the workstation's 3 explorer frame from router B and D, router A caches the first received response as the preferred router (in this case router B). Any subsequent responses from other routers (router D in this example) are cached as capable routes to use to reach the 3745. Router A now sends the explorer frame response back to the workstation, and the session setup continues.

8.2 DLSw on the 2210

The DLSw function of the 2210 supports the interconnection of SNA devices attached to either a LAN (token-ring or Ethernet), or an SDLC non-switched line.

As a prerequisite for DLSw, if the 2210 supports LAN-attached SNA devices, it must be configured to support source route bridging on the token-ring interface, or transparent bridging on the Ethernet interface.

A DLSw virtual segment number also needs to be configured for 2210s implementing DLSw. This virtual segment must be the same for all 2210s

participating in the DLSw function. This is to ensure that the endstations both see the TCP/IP network as one token-ring.

SNA devices attached to a 2210 via SDLC are each assigned a source and destination locally administered MAC address (LAA), a source and destination service access point (SAP) and SNA ID block and ID number. These will be used by the 2210 to represent such devices to other SNA devices that are using the DLSw function as if they are attached to a token-ring LAN. SDLC-attached devices can have SNA connections with token-ring and/or Ethernet-attached devices connected to the same 2210.

SNA devices attached to a 2210 establish connections with SNA devices attached to other 2210s as if they are on the virtual segment.

SNA devices attached to a 2210 via LAN segments establish connections with SNA devices attached to the same 2210 via SDLC as if they were on the virtual segment.

With MRS V1R1, the 2210′s SLDC now supports attachments to PU Type 4.0, PU Type 2.0, or PU Type 2.1. The 2210 can be a primary, secondary, or negotiable on the SDLC link.

There are two types of data link switching:

- Local data link switching
- Remote data link switching

In local DLSw, the data link switching function is performed within a single 2210. In remote DLSw, stations attached to two or more 2210s communicate across an IP network using DLSw.

8.2.1 Local Data Link Switching

Local DLSw allows communication between a token-ring or Ethernet-attached SNA device and an SDLC secondary or primary station that is link attached to the 2210.

Local DLSw converts SDLC frames to LLC2 frames. The encapsulated SDLC frames are passed to the DLSw function which will in turn use source route or transparent bridging function to deliver them to the LAN-attached device. It is also possible now to do local DLSw between two SDLC ports.

8.2.2 Remote Data Link Switching

SNA stations attached to an IBM 2210 via a token-ring, Ethernet or SDLC connection can establish sessions with other SNA stations that are attached to a remote 2210, 2216 or 6611 via a token-ring or an Ethernet connection. The connection between the two 2210s or between the 2210 and the 2216 is over an IP network that can include OEM routers that support compatible IP functions such as RIP or OSPF. Note that only the two routers connected to the endstations must be enabled for DLSw. DLSw function is not required in the routers that might exist between the two edge-node routers.

The DLSw in the 2210 encapsulates the SNA frames in a TCP/IP datagram and delivers the encapsulated frames to its partner over the IP network.

Remote DLSw supports:

- SDLC (secondary or primary) to LAN over WAN

  SDLC frames are converted into LLC2 frames. This allows a link-attached SDLC device to communicate with a LAN-attached (token-ring and Ethernet) device.

- LAN-to-LAN over WAN

  Remote DLSw allows communication between SNA devices attached to token-ring or Ethernet networks. Remote DLSw can convert frames between the token-ring and Ethernet allowing token-ring and Ethernet-attached devices to communicate with each other using DLSw.

- SDLC (secondary or primary) to LAN on the same 2210.

  This is local DLSw which converts SDLC to LAN protocols.

- SDLC-to-SLDC on the same 2210.

  This is local DLSw on SDLC.

- SDLC-to-SLDC over WAN

  Remote DLSw for SDLC links that can be used as a better alternative to SLDC relay. This technique can be used, for example, for INN traffic.

8.2.3 DLSw Using MOSPF

The 2210 supports use of the DLSw Group Membership function to allow it to dynamically discover its DLSw partners, instead of having to manually configure the partner addresses. This feature utilizes the Multicast OSPF (MOSPF) function.

The DLSw Group Membership defines two types of group:

- Client/server
- Peer-to-peer

Client/server groups have members that are designated either a client or a server. Server routers only form DLSw connections with client routers. This group type is used for subarea SNA connections. Peer-to-peer groups have members that are all designated peers. All members of a peer-to-peer group will form DLSw connections with all other members of the group. This group type could be used for APPC connections.

DLSw group membership will only work between routers that support it, so a combination of group membership and pre-configured DLSw partner definitions may be required in your network.

8.3 DLSw Configuration on the 2210

The 2210 supports remote DLSw over PPP, frame relay and X.25.

To configure DLSw on the 2210 you can use either the Nways MRNS Configuration Program or the Config process of Nways MRS.

8.3.1 DLSw Configuration Commands

This section summarizes the DLSw configuration commands available within the Config process of Nways MRS. To access the commands, you need to issue the following command:

```
Config>protocol dls
```

Table 8 shows the commands available. The *Nways MRS Protocol Configuration and Monitoring Reference* covers these commands in detail.

Table 8. DLSw Configuration Commands

Command	Function
? (Help)	Lists all the DLSw configuration commands, or lists the options associated with specific commands.
Add	Adds an SDLC link station, a TCP neighbor IP address, or a QLLC station or destination.
Ban	Allows access to the boundary access node (BAN) configuration prompt so that BAN configuration commands can be entered.
Close-Sap	Close a currently opened service access point (SAP). DLSw uses SAPs for communication on interfaces that support LLC.
Delete	Deletes an SDLC link station, a TCP neighbor IP address, or a QLLC station or destination.
Disable	Disables DLSw, SDLC link stations, LLC disconnect functionality, dynamic neighbors, or a QLLC station of interface.
Enable	Enables DLSw, SDLC link stations, LLC disconnect functionality, dynamic neighbors, or a QLLC station of interface.
Join-Group	Adds the router to a DLSw group, allows DLSw neighbors to dynamically find each other.
Leave-Group	Removes the router from specified DLSw group.
List	Displays information for SDLC link stations, SAPs, circuit priority, DLSw groups, DLSw global information, and QLLC destinations, stations, and interfaces. The command also provides detailed information on TCP connections.
Open-Sap	Allows DLSw to transmit data over the specified SAP. DLSw uses SAPs fo communication on interfaces that support LLC.
Set	Sets LLC attributes, TCP buffer size, the maximum number of DLSw sessions supported, the memory allocated to DLSw, the DLSw virtual SRB segment number, protocol timers, circuit priority, parameters for dynamic neighbors, and parameters for QLLC operations.
Exit	Exits the DLSw configuration environment and returns to the Config environment.

8.3.2 DLSw Configuration Overview

In addition to the DLSw-specific configuration, you will also need to configure IP and bridging. If you intend to use the DLSw group functionality, you will also have to configure OSPF.

IP is configured via the IP Config> prompt on Nways MRS, or via the Protocols/IP panels of the Nways MRNS Configuration Program. If you wish to use RIP, this is configured via the IP Config> prompt on Nways MRS, or via the Protocols/IP/RIP panels of the Nways MRNS Configuration Program.

If you wish to use OSPF, this is configured via the OSPF Config> prompt on Nways MRS, or via the Protocols/IP/OSPF panels of the Nways MRNS Configuration Program.

Bridging is configured via the ASRT Config> prompt of Nways MRS, or via the Protocols/Bridging panels of the Nways MRNS Configuration Program.

Configuration of DLSw requires you to:

- Enable DLSw.
- Set the DLSw SRB virtual segment number. (This value must be set on Ethernet models as well, and it should be the same value on all participating DLSw routers.)
- Add the TCP neighbor IP addresses, or join a DLSw group.
- Open the SAPs you wish to be DLSw switched.
- Set the default MAC address for SDLC link stations if required.
- Add an SDLC link station if required.

8.3.2.1 Enabling DLSw

To enable DLSw, you need to:

- Enter DLSw Config>**enable dls**, or
- Enable DLSw on the Protocols/DLSw/General panel of the Nways MRNS Configuration Program.

8.3.2.2 Setting the SRB Virtual Segment Number

To set the SRB virtual segment number:

- Enter DLSw Config>**set srb**, or
- Complete the SRB Segment field on the Protocols/DLSw/General panel of the Nways MRNS Configuration Program.

8.3.2.3 Adding TCP Neighbors

To add TCP neighbors:

- Enter DLSw Config>**add tcp**, or
- Complete the information on the Protocols/DLSw/TCP Connections panel of the Nways MRNS Configuration Program.

8.3.2.4 Joining a DLSw Group

To join a DLSw group:

- Enter DLSw Config>**join-group**, or
- Complete the information on the Protocols/DLSw/Multicast Groups panel of the Nways MRNS Configuration Program.

8.3.2.5 Opening SAPs for DLSw Switching

To open SAPs for DLSw switching:

- Enter DLSw Config>**open-sap**, or
- Select **Configure** for interface 0 on the Protocols/DLSw/Interfaces panel of the Nways MRNS Configuration Program, and add the required SAPs.

Note: The Nways MRNS Configuration Program opens SAPs 00 and 04 for the LAN interface by default.

8.3.2.6 Adding an SDLC Link Station to DLSw

To add an SDLC link station to DLSw:

- Enter DLSw Config>**add sdlc**, or
- Select **Configure** for the SDLC interface on the Protocols/DLSw/Interfaces panel of the Nways MRNS Configuration Program, and complete the fields.

8.3.3 Further DLSw Configuration Considerations

The DLSw configuration process allows you to set the memory allocation for DLSw, which will probably be required if you intend to have a large number of concurrent DLSw sessions. To set the memory allocation you need to:

- Issue the DLSw Config>**set memory** command, or
- Complete the memory allotment fields on the Protocols/DLSw/General panel of the Nways MRNS Configuration Program.

To calculate the memory required for DLSw, you should take into consideration the estimated number of DLSw sessions and TCP neighbors, and the amount of memory available in the IBM 2210.

The memory required can be calculated using the following formula:

```
(session allocation * number of sessions * 75%) +
(number of TCP neighbors * 512)
```

For example, if you have 8192 bytes allocated per LLC session, and 4096 bytes per SDLC session, and you estimate that there will be 40 LLC DLSw sessions and 20 SDLC sessions, using two TCP neighbors, then the calculation would be:

```
(8192 * 40 * 75%) + (4096 * 20 * 75%) + (512 * 2) = 308224 bytes.
```

If many small packets are anticipated on the DLSw sessions, then the 75% value should be increased to 85%.

You are also able to limit the maximum number of DLSw sessions permitted. You do this by:

- Issuing the DLSw Config>**set maximum** command, or
- Complete the maximum DLSw sessions field on the Protocols/DLSw/General panel of the Nways MRNS Configuration Program.

8.4 DLSw Enhancements with V1R2 of Nways MRNS Software

Some new capabilities for this release of the Nways MRNS software are as follows:

- SDLC X.21 support

  SDLC is now supported over X.21 links.

- PU2.0 and PU2.1 multi-drop

  Support for the IBM 2210 routers for coexistence of SNA T2.0 and T2.1 link stations on SDLC multipoint lines.

Note: To mix roles among the link stations on a single SDLC link, you must configure the IBM 2210 to support whichever remote nodes do not match the default.

- On-demand vs static TCP sessions

  DLSw now has the capability to automatically re-establish TCP connections after they break and upon power-up. Previously, TCP sessions were established only when they were needed for this first time (for a CANUREACH, for example) or if the DLSw Group functionality found a neighbor.

  The following new commands have been added to the DLSw configurator and console in order to implement this:

  - **Enable Auto-TCP-Connection:** Allows pre-configured TCP sessions to be automatically established, and causes broken sessions to be re-established. This is the default.
  - **Disable Auto-TCP-Connection:** TCP sessions are not established until DLSw needs them. TCP connections caused by DLSw groups are still created automatically. Broken TCP group connections will be re-established after the user-specified group join timer interval expires. This timer is set with the Set Timers command from the DLSw configuration or console command.

- Large frame support for SDLC relay

  SDLC relay now supports frame sizes larger than 2048 bytes, up to the maximum allowed by the device that SDLC relay runs over.

  Although the router now supports the larger frame size, care should be taken to ensure that IP fragmentation does not occur in the IP cloud. If fragmentation does occur, performance will suffer between two routers that have reachability via multiple paths.

  Note: Keep in mind that the time required to transmit larger frames over slower WAN links will lengthen the round-trip times; this should be accounted for by lengthening the data link's response timeout values at the connected endstations.

- User-settable TCP receive buffer

  The ability to set the receive buffer size is useful when communicating over networks that have a high bandwidth delay, such as a frame relay network running over a T1 line.

  Note: Unless you have a reason to increase the buffer size, you should accept the default value of 4096. Setting the buffer too high will use up memory on the router.

- Configurable MAC address cache size

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

  Note: Setting this option too high will cause a reduction in router memory and in the number of DLSw sessions that can be handled by the router.

- MIB extensions

Two additional objects have been added to the ibmdlsRouterTable. They are ibmdlsRouterInFrames, which is a count of the number of frames received from the partner router, and ibmdlsRouterOutFrames, which is a count of the number of frames sent to the partner router.

One additional object has been added to the ibmdlsCirTable. The ibmdlsCirKicakAddress object indicates which of the source or destination MAC addresses for the circuit is local to this router.

8.5 DLSw Enhancements with V1R1 of Nways MRS Software

Recent enhancements to the DLSw function of MRS include the following:

- Multicast exploration and frame forwarding (multicast DLSw)

  This is the initial implementation of enhancements to improve the salability of DLSw to large networks. Rather than bring up static TCP connections to configured neighbor routers, the code uses both multicast and directed UDP packets to propagate address and name resolution messages, and NetBIOS UI-frame traffic. Transport connections between multicast-capable DLSw nodes are established only on demand, and are taken down after they are no longer needed. These salability enhancements are compatible with back-level DLSw nodes that have no multicast IP support, and with MRNS releases that provided for MOPF-based discovery of DLSw partners.

- NetBIOS name list support

  This allows a user with a structured naming convention to have more control over the broadcasting of NetBIOS datagrams. DLSw builds and sends a list of local NetBIOS names (with wildcard characters), and uses the information in received lists to minimize the number of destinations to which is sends NetBIOS SSP messages.

- APPN remote device attachment The introduction of APPN had implications for DLSw. DLSw had an internal interface to APPN that connects APPN and endstations attached to remote routers. It does not support DLSw between locally attached APPN devices. No DLSw configuration is required to support the interface but APPN must be configured to use a specific DLS virtual interface to reach a given endstation.

- SDLC improvements:

  – DLSw act as secondary for multiple PU types It is now possible for the 2210 to be configured as a secondary SDLC endstation, rather than just as a primary. This means that it is no longer necessary to configure the 2210 for SDLC relay (SDLC frames encapsulated in IP packets).

    DLSw can support SDLC endstations that are PU types 2.0, 2.1, 4 (for NCP-NCP traffic) or 4/5 (a host or NCP performing the SNA boundary function).

    For DLSw to support an SDLC interface, the configuration is done in two phases. First, the SDLC interface parameters are configured. Most of the default values can be used, but it is advisable to configure the link station name and SDLC address. Secondly, each SDLC link station must be defined from the DLSw perspective. During this process, the PU type of the link station must be defined. The options are 2, 4 or 5. If the station is either PU type 2.0 or 2.1, enter 2. These PU types are differentiated between by the next two options, which ask for SID0 block number and XID0 ID number. If the station is PU 2.1, these fields should be left as

zero. If the station is PU 2.0, these fields must match the definitions in the link station′s configuration.

- Poll PU 2.0 via SNRM. This allows the user to have PU 2.0 SDLC devices polled with SNRM rather than TEST frames.
- PU4 INN support. This allows PU4s on point-to-point SDLC to connect through DLSw to other PU4s on LANs, SDLC and frame relay.
- Local SDLC to SDLC support

  DLSw sessions between two SDLC devices attached to the same DLSw box are now supported.

- IETF DLSw MIB Support

  This DLSw implementation supports the recently approved IETF Proposed Standard MIB for DLSw. At this time, the MIB has not received an RFC number but is available on Internet Draft directories under the name (draft-ietf-dlswmib-mib-09.txt).

- LNM support

  DLSw has been enhanced so that it can be used to transport LAN network manage packets. LNM had the SAP c′F4′. While this was initially introduced in V1R3 with enhancements, further improvements have been introduced, For example, with first implementation it was only possible to link remote 8230s, but not to manage them. With this release, the 8230 management function has been added.

- No-cache-aging option

  The no-cache-aging option will drastically reduce the amount of DLSw-search traffic. This option is only advantageous over ISDN links where the location of the endstations is fixed. It is configured using the set timers command, and setting the first option, database age timeout, to zero. This is not generally recommended as it disables a number of other DlSw functions.

8.6 DLSw Configuration Scenarios

The data link switching (DLSw) scenarios in this particular section focus on the newer SDLC capabilities of the 2210. With the exception of some additional DLSw parameter options and a change in the syntax of one of the SDLC parameters, the setup and traditional DLSw support for LAN-attached workstations and remote secondary SDLC stations remain the same. These changes are noted in the configuration examples that follow.

The DLSw scenarios previously documented in the *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios*, SG24-4046 using the Nways MRNS Program remain applicable under the Nways MRS Program when taken in the context of these parameter changes.

This section provides configuration examples for the following DLSw scenarios:

1. Remote DLSw between two routers, where:
   - A remote router (2210B) is providing traditional SNA support for LAN-attached workstations and a remote secondary SDLC device.

     In this configuration, router 2210B is emulating an SDLC primary link station to provide polling for the remotely attached workstation or

secondary SDLC device on one link, and traditional DLSw TCP connections over the other link.

- A central site router (2210A) is providing local secondary SDLC attachment to a 3745 Communications Controller.

  In this configuration, router 2210A is emulating an SDLC secondary link station and is the recipient of the polling from the 3745 on one link, and is providing traditional DLSw support for its remote DLSw partner, router 2210B, on the other link.

2. Local DLSw, where a single router provides:
   - SNA Gateway support for LAN-attached workstations
   - SDLC-to-SDLC support

     In this configuration, 2210B emulates a primary SDLC link station on one link to provide polling for remotely attached SDLC devices, and a secondary SDLC link station on another link to receive polling from the 3745.
3. Remote DLSw support for INN traffic between two 3745s or PU Type 4.0 devices over SDLC links

   In this configuration, both the routers were configured for negotiable link roles on their SDLC interfaces. Either router could have emulated the primary or the secondary link station role. The final configuration would depend on which 3745 initiated the contact and the NCP GEN parameters for the SDLCST macros. If the link station roles are coded, the GEN parameters can identify which 3745 should be primary, and which should be secondary. If the link station roles are not coded, the decision is made after the XID exchange and a comparison of the subarea numbers.

8.6.1 Scenario X1 - Remote DLSw Using SDLC for Host Access

Figure 134 on page 232 is a pictorial representation of this scenario.

8.6.1.1 Environment

In this scenario, there were two 2210s connected across the wide area network by a PPP link, and running data link switching between them.

- The local or central site router, 2210A, was SDLC attached to a 3745 running ACF/NCP V7R4 on Serial Port 2, and to router 2210B across the PPP interface on Serial Port 1.

  Figure 136 on page 241 shows the configuration process for 2210A using the command line interface.

  Figure 138 on page 257 shows the configuration process for 2210A using the Nways MRS Configuration program.
- The remote router, 2210B, was supporting SNA sessions over its token-ring interface and over Serial Port 2, which was configured for SDLC support. Serial Port 1 was connected remotely to 2210A across the PPP link.

  Figure 135 on page 233 shows the configuration process for 2210B using the command line interface.

  Figure 137 on page 251 shows the configuration process for 2210B using the Nways MRS Configuration program.

- Both remote workstations were configured as PU Type 2.0 devices in the initial configuration, to match the NCP GEN parameters (XID = NO) on an existing and available NCP line on the 3745.
- The LAN-attached workstation was running OS/2 and using Communications Manager/2 Version 2.11 for 3270 emulation.
- The SDLC-attached workstation was running Communications Server for OS/2 Version 4.1 and using the Personal Communications Workstation Program for OS/2 Version 4.1 for 3270 emulation.

8.6.1.2 Objective

The objective of this scenario was to demonstrate part of the secondary SDLC link station support capabilities of the 2210 by establishing 3270 emulation sessions with the mainframe through the NCP's SDLC connection.

The combination of remote data link switching and local secondary SDLC support in the 2210s presented the appearance to VTAM that both workstations, whether LAN or SDLC-attached, were multidropped PUs on an NCP line.

8.6.1.3 Benefit

The potential benefit of this 2210 functionality is to allow you to take advantage of various local and wide area network technologies without the requirement for necessarily installing LAN gateways to your mainframes.

This same functionality also presents you with opportunities to provide some remote SNA concentration support in areas where a remote 3745 might not be appropriate or cost justifiable.

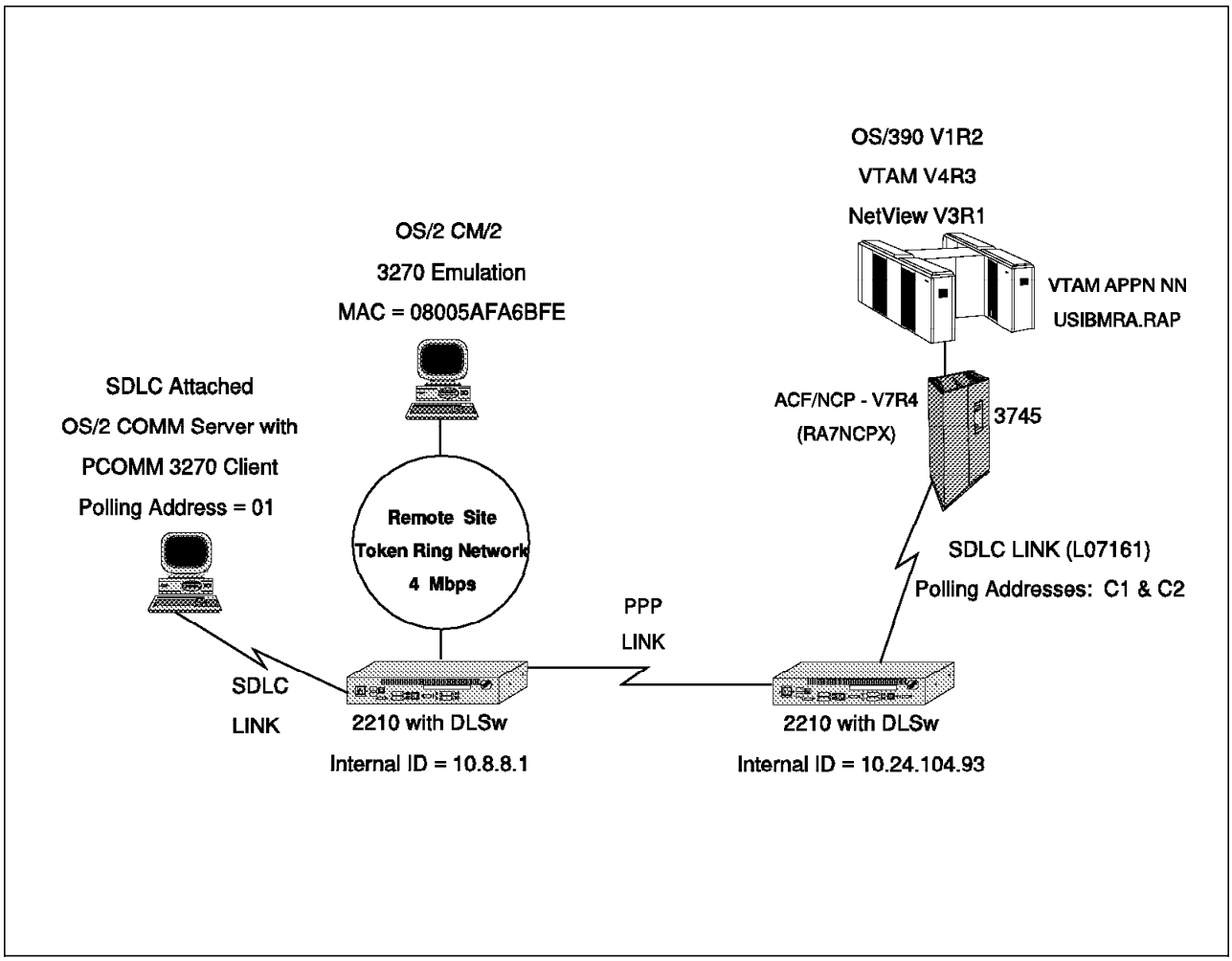


Figure 134. Remote DLSw and Local SDLC Access to the Host

Note: The QCONFIG (quick configuration) procedure was used to configure the basic parameters of router 2210B for this scenario. The following parameters were the basic settings selected during the QCONFIG procedure:

Token-Ring Speed	4 Mbps
Token-Ring Connector Type	STP
Encapsulation for WAN 1	PPP
Cable Type for WAN 1	RS-232 DCE
Internal Clock Speed for WAN 1	56000 decimal
IP address of Interface 0	8.8.8.1 (subnet mask 255.255.255.0)
IP address of Interface 1	200.200.200.2 (subnet mask 255.255.255.0)
Dynamic Routing	Enabled
OSPF	Enabled

The remaining configuration parameters follow on subsequent pages.

Next, we show you the configuration setup for Router 2210B:

```
*TALK 6     1
Config>SET DATA-LINK SDLC      2
Interface Number [1]?2
Config>NETWORK 2     3
SDLC user configuration
Creating a default configuration for this link
SDLC 2 Config>LIST LINK     4
Link configuration for: LINK_2   (ENABLED)

Role:         PRIMARY          Type:         POINT-TO-POINT
Duplex:       FULL             Modulo:       8
Idle state:   FLAG             Encoding:     NRZ
Clocking:     EXTERNAL         Frame Size:   2048
Speed:        0                Group Poll:   00
Cable:        RS-232 DTE

Timers:     XID/TEST response:  2.0 sec
            SNRM response:      2.0 sec
            Poll response:      0.5 sec
            Inter-poll delay:   0.2 sec
            RTS hold delay:     DISABLED
            Inter-frame delay:  DISABLED
            Inactivity timeout: 30.0 sec

Counters:   XID/TEST retry:  8
            SNRM retry:      6
            Poll retry:      10

SDLC 2 Config>ADD STATION     5
Enter station address (in hex) [01]?
Enter station name [SDLC_01]? SDLC_01
Include station in group poll list (Yes or No): NO
Enter max packet size [2048]? 521
Enter receive window [7]?
Enter transmit window [7]?
SDLC 2 Config>LIST STATION ALL     6

Address    Name      Status    Max BTU  Rx Window  Tx Window
-------  --------  ----------  -------  ---------  ---------
  01     SDLC_01     ENABLED       521        7          7

SDLC 2 Config>exit
```

Figure 135 (Part 1 of 6). Scenario X1 - Remote DLSw and SDLC Host Access - 2210B Configuration

```
Config>PROTOCOL IP     7
Internet protocol user configuration
IP config>SET INTERNAL-IP-ADDRESS 10.8.8.1      8
IP config>DISABLE RIP     9

IP config>LIST ALL     10
Interface addresses
IP addresses for each interface:
   intf  0   8.8.8.1          255.255.255.0    Local wire broadcast, fill 1
   intf  1   200.200.200.2    255.255.255.0    Local wire broadcast, fill 1
   intf  2                                     IP disabled on this interface
   intf  3                                     IP disabled on this interface
   intf  4                                     IP disabled on this interface
   intf  5                                     IP disabled on this interface
Internal IP address: 10.8.8.1

Routing
Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: enabled
BGP: disabled
RIP: disabled

IP config>EXIT
```

Figure 135 (Part 2 of 6). Scenario X1 - Remote DLSw and SDLC Host Access - 2210B Configuration

```
Config>PROTOCOL OSPF
Open SPF-Based Routing Protocol configuration console
OSPF Config>ENABLE MULTICAST
Inter-area multicasting enabled? [No]?NO
OSPF Config>LIST ALL     11


                      --Global configuration--
                OSPF Protocol:          Enabled
                # AS ext. routes:       1000
                Estimated # routers:    50
                External comparison:    Type 2
                AS boundary capability: Disabled
                Multicast forwarding:   Enabled
                Inter-area multicast:   Disabled

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

                       --Interface configuration--
IP address        Area              Cost  Rtrns  TrnsDly  Pri  Hello   Dead
8.8.8.1           0.0.0.0              1      5       1     1     10     40
200.200.200.2     0.0.0.0              1      5       1     1     10     40

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

OSPF Config>EXIT
```

Figure 135 (Part 3 of 6). Scenario X1 - Remote DLSw and SDLC Host Access - 2210B Configuration

```
Config>PROTOCOL ASRT     12
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>ENABLE BRIDGE    12
ASRT config>DISABLE TRANSPARENT   14
Port Number [1]?
ASRT config>ENABLE SOURCE-ROUTING 1 FFB 2   14
ASRT config>ENABLE DLS     15
ASRT config>LIST BRIDGE      16

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

Bridge:                 Enabled                 Bridge Behavior: SRB
                  +----------------------------+
------------------] SOURCE ROUTING INFORMATION ]------------------------------
                  +----------------------------+
Bridge Number:          02                      Segments:          1
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1:  SRB:                Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
                  +------------------+
------------------] SR-TB INFORMATION ]---------------------------------------
                  +------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0

                  +-----------------------------------+
------------------] SPANNING TREE PROTOCOL INFORMATION ]----------------------
                  +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IBM-SRB proprietary
                  +-------------------------+
------------------] TRANSLATION INFORMATION ]---------------------------------
                  +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                  +------------------+
------------------] PORT INFORMATION ]---------------------------------------
                  +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled

ASRT config>EXIT
```

Figure 135 (Part 4 of 6). Scenario X1 - Remote DLSw and SDLC Host Access - 2210B Configuration

```
Config>PROTOCOL DLS     17
DLSw protocol user configuration
DLSw config>ENABLE DLS     18
DLSw config>SET SRB FAB     19
DLSw config>JOIN-GROUP     20
Group ID (1-64 Decimal) [1]?
Client/Server or Peer Group Member(C/S/P)- [P]?
Connectivity Setup Type (a/p) [p]?A
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?E
Neighbor Priority (H/M/L) [M]?
DLSw config>OPEN-SAP
Interface #  [0]?
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? SNA
SAPs 0 4 8 C opened on interface 0
DLSw config>ADD SDLC     21
Interface # [0]?2
SDLC Address [C1]? 01
Source MAC address [400BDC4B02C1]?40002210B2C1
Source SAP in hex [4]? 04
Destination MAC address [000000000000]?402210374501
Destination SAP in hex [0]?4
PU type (2/4/5) [2]? 2
XID0 block num in hex (0-0xfff) [0]? 05D
XID0 id num in hex (0-0xfffff) [0]?5183
Poll with TEST (T) or SNRM (S) [T]?SNRM
DLSw config>LIST SDLC    22
Interface #, or 'ALL' [0]?ALL
Net Addr  Status    Source SAP/MAC   Dest SAP/MAC      PU  Blk/IdNum  PollFrame
 2   01   Enabled   04 40002210B2C1  04 402210374501   2   05D/05183  SNRM
```

Figure 135 (Part 5 of 6). Scenario X1 - Remote DLSw and SDLC Host Access - 2210B Configuration

```
DLSw config>LIST DLS     23
DLSw is                              ENABLED
LLC2 send Disconnect is              ENABLED
Dynamic Neighbors is                 ENABLED

SRB Segment number                   FAB
MAC <-> IP mapping cache size        128
Max DLSw sessions                    1000
DLSw global memory allotment         141312
LLC per-session memory allotment     8192
SDLC per-session memory allotment    4096
NetBIOS UI-frame memory allotment    40960

Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor Priority              MEDIUM
DLSw config>exit
Config>
*RESTART
Are you sure you want to restart the gateway? (Yes or [no]YES

*TALK 5     24

CGW Operator Console

+PROTOCOL DLS     25
Data Link Switching Console

DLSw>LIST TCP SESSIONS     26

   Group   IP Address      Conn State     CST  Version  Active Sess Sess Creates
   ------- --------------- -------------- ---  -------- ----------- ------------
1  Peer 1  10.24.104.93    ESTABLISHED     a   AIW V1R0      2          49

DLSw>LIST DLS SESSIONS ALL     27

         Source          Destination      State     Flags    Dest IP Addr    Id
     --------------  --------------  ---------  -------  --------------  ----
   1 08005AFA6BFE 04  402210374502 04  CONNECTED           10.24.104.93       3
   2 SDLC 02-01   04  402210374501 04  CONNECTED           10.24.104.93      48

DLSw>LIST SDLC SESSIONS ALL     28

      Net   Address  Source SAP/MAC    Dest SAP/MAC     PU  OutQ   State
   1.  2    01       04 40002210B2C1   04 402210374501  2    0     CONTACTED
```

Figure 135 (Part 6 of 6). Scenario X1 - Remote DLSw and SDLC Host Access - 2210B Configuration

Notes:

1 Talk to the Configuration process.

2 Set the data link type for interface 2 to SDLC.

3 Start configuration of the SDLC interface.

4 List the SDLC link parameters to ensure that everything is correct. We took the default link configuration.

5 Add the SDLC station which in this case is the PComm/3270 PC with an SDLC adapter.

6 List all of the stations' information.

7 Start the IP configuration process.

8 The Internal IP Address is used for data link switching. The primary reason for defining an internal IP address is to provide an address for a TCP connection that will not become inactive when an interface becomes inactive.

9 We chose to run OSPF instead of RIP for greater DLSw functionality and reduced routing table update overhead.

10 List the IP configuration to make sure everything is correct.

11 List the OSPF configuration to make sure everything is correct.

12 Start the Bridge configuration process.

14 Disable transparent bridging, and enable source route bridging on the token-ring interface.

14 Enable DLSw on the bridge.

15 List the bridge to ensure that everything is correct.

16 Start customization of DLSw.

17 Enable DLSw.

18 Set the DLSw virtual segment number.

19 Join the group as a peer.

20 Open SAPs 04 for DLSw switching on interface 0.

21 Add a DLSw SDLC station.

22 List DLSw SDLC sessions.

23 List the DLSw configuration to ensure that everything is correct.

24 Talk to the GWCON process.

25 Enter the DLSw monitoring console.

26 List the DLSw TCP sessions.

27 List the DLSw sessions. In this scenario we have two DLSw sessions.

28 List the DLSw SDLC sessions. In this scenario there are two DLSw SDLC sessions, and the status is contacted, one for SDLC and one for token-ring.

8.6.1.4 Configuration Setup for Router 2210A

The QCONFIG (quick configuration) procedure was used to configure the basic parameters of router 2210A for this scenario. The following parameters were the basic settings selected during the QCONFIG procedure:

Encapsulation for WAN 1	PPP
Cable type for WAN 1	RS-232 DTE
IP address of Interface 0	9.24.104.93 (subnet mask 255.255.255.0)
IP address of Interface 1	200.200.200.1 (subnet mask 255.255.255.0)
Internal-IP-Address	10.24.104.93 (subnet mask 255.255.255.0)
Dynamic Routing	ENABLED
OSPF	ENABLED

The remaining configuration parameters used in this scenario follow.

```
*TALK 6     1
Config>SET DATA-LINK SDLC     3
Interface Number [0?]1

Config>LIST DEVICES     2
Ifc 0   Ethernet                      CSR  81600, CSR2  80C00, vector 94
Ifc 1   WAN SDLC                      CSR  81620, CSR2  80D00, vector 93
Ifc 2   WAN PPP                       CSR  81640, CSR2  80E00, vector 92
Ifc 3   ISDN Basic                    CSR      0, vector 0

Config>NETWORK 1     4
SDLC user configuration
Creating a default configuration for this link
SDLC 1 Config>SET LINK ROLE SECONDARY     5
SDLC 1 Config>SET LINK ENCODING NRZI    6
SDLC 1 Config>ADD STATION     7
Enter station address (in hex) [C1]? C1
Enter station name [SDLC_C1]? SDLC_C1
Include station in group poll list ([Yes.]or No)NO
Enter max packet size [2048]?521
Enter receive window [7]? 7
Enter transmit window [7]? 7
SDLC 1 Config>ADD STATION     8
Enter station address (in hex) [C2]? C2
Enter station name [SDLC_C2]? SDLC_C2
Include station in group poll list ([Yes] or No)NO
Enter max packet size [2048]? 521
Enter receive window [7]? 7
Enter transmit window [7]? 7
```

Figure 136 (Part 1 of 8). Scenario X1 - Remote DLSw and SDLC Host Access - 2210A Configuration

```
SDLC 1 Config>LIST LINK     9
Link configuration for: LINK_1   (ENABLED)

Role:         SECONDARY        Type:         POINT-TO-POINT
Duplex:       FULL             Modulo:       8
Idle state:   FLAG             Encoding:     NRZI
Clocking:     EXTERNAL         Frame Size:   2048
Speed:        0                Group Poll:   00
Cable:        RS-232 DTE

Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
           RTS hold delay:     DISABLED
           Inter-frame delay:  DISABLED
           Inactivity timeout: 30.0 sec

Counters:  XID/TEST retry:  8
           SNRM retry:      6
           Poll retry:      10

SDLC 1 Config>LIST STATION ALL     10

Address    Name      Status    Max BTU  Rx Window  Tx Window
-------  --------  ----------  -------  ---------  ---------
  C1     SDLC_C1     ENABLED       521        7          7
  C2     SDLC_C2     ENABLED       521        7          7

SDLC 1 Config>EXIT     11
```

Figure 136 (Part 2 of 8). Scenario X1 - Remote DLSw and SDLC Host Access - 2210A Configuration

```
Config>PROTOCOL IP
Internet protocol user configuration

IP config>DISABLE RIP     12
IP config>SET INTERNAL-IP-ADDRESS 10.24.104.93     12

IP config>LIST ALL     12
Interface addresses
IP addresses for each interface:
   intf  0   9.24.104.93      255.255.255.0    Local wire broadcast, fill 1
   intf  1                                     IP disabled on this interface
   intf  2   200.200.200.1    255.255.255.0    Local wire broadcast, fill 1
   intf  3                                     IP disabled on this interface
Internal IP address: 10.24.104.93

Routing
protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: enabled
BGP: disabled
RIP: disabled

IP config>EXIT
```

Figure 136 (Part 3 of 8). Scenario X1 - Remote DLSw and SDLC Host Access - 2210A Configuration

```
Config>PROTOCOL OSPF     13
Open SPF-Based Routing Protocol configuration console
OSPF Config>ENABLE MULTICAST    14
Inter-area multicasting enabled? [No]? NO

OSPF Config>LIST ALL     15

                      --Global configuration--
               OSPF Protocol:          Enabled
               # AS ext. routes:       1000
               Estimated # routers:    50
               External comparison:    Type 2
               AS boundary capability: Disabled
               Multicast forwarding:   Enabled
               Inter-area multicast:   Disabled

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

                      --Interface configuration--
IP address       Area             Cost  Rtrns  TrnsDly  Pri  Hello   Dead
9.24.104.93      0.0.0.0             1      5       1     1     10     40
200.200.200.1    0.0.0.0             1      5       1     1     10     40

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

OSPF Config>EXIT
```

Figure 136 (Part 4 of 8). Scenario X1 - Remote DLSw and SDLC Host Access - 2210A Configuration

```
Config>PROTOCOL ASRT     16
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>ENABLE BRIDGE      17
ASRT config>ENABLE DLS     18
ASRT config>DISABLE TRANSPARENT 1
ASRT config>ENABLE SOURCE-ROUTING 1 584 A     18

ASRT config>LIST BRIDGE      19

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

Bridge:                 Enabled                 Bridge Behavior: SRB
                   +----------------------------+
------------------] SOURCE ROUTING INFORMATION ]------------------------------
                   +----------------------------+
Bridge Number:          N/A                     Segments:          0
Max ARE Hop Cnt:        00                      Max STE Hop cnt:   00
1:  SRB:                Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
                   +-------------------+
------------------] SR-TB INFORMATION ]---------------------------------------
                   +-------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
                   +-----------------------------------+
------------------] SPANNING TREE PROTOCOL INFORMATION ]----------------------
                   +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IEEE802.1d
                   +-------------------------+
------------------] TRANSLATION INFORMATION ]---------------------------------
                   +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                   +------------------+
------------------] PORT INFORMATION ]-----------------------------------------
                   +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled

ASRT config>EXIT
```

Figure 136 (Part 5 of 8). Scenario X1 - Remote DLSw and SDLC Host Access - 2210A Configuration

```
Config>PROTOCOL DLS      20
DLSw protocol user configuration
DLSw config>ENABLE DLS       21
DLSw config>SET SRB FAB      22
DLSw config>OPEN-SAP      23
Interface # [0]? 0
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]?SNA
SAPs 0 4 8 C opened on interface 0
DLSw config>JOIN-GROUP      24
Group ID (1-64 Decimal) [1]? 1
Client/Server or Peer Group Member(C/S/P)- [P]?
Connectivity Setup Type (a/p) [p]?A
Transmit Buffer Size (Decimal) [5120]? 5120
Receive Buffer Size (Decimal) [5120]? 5120
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?E
Neighbor Priority (H/M/L) [M]? M DLSw config>ADD SDLC      25
Interface # [0]?1
SDLC Address [C1]? C1 Source MAC address [4000A7E501C1]?402210374501
Source SAP in hex [4]? 04
Destination MAC address [000000000000]?40002210B201
Destination SAP in hex [0]?4
PU type (2/4/5) [2]?5
DLSw config>ADD SDLC
Interface # [0]?1
SDLC Address [C1]?C2
Source MAC address [4022103701C2]?402210374502
Source SAP in hex [4]? 04 Destination MAC address [000000000000]?08005AFA6BFE
Destination SAP in hex [0]?04
PU type (2/4/5) [2]?5
DLSw config>LIST SDLC     26
Interface #, or 'ALL' [0]?ALL

Net Addr  Status    Source SAP/MAC   Dest SAP/MAC      PU  Blk/IdNum  PollFrame
 1   C1   Enabled   04 402210374501  04 40002210B201   5
 1   C2   Enabled   04 402210374502  04 08005AFA6BFE   5
```

Figure 136 (Part 6 of 8). Scenario X1 - Remote DLSw and SDLC Host Access - 2210A Configuration

```
DLSw config>LIST DLS      27
DLSw is                              ENABLED
LLC2 send Disconnect is              ENABLED
Dynamic Neighbors is                 ENABLED

SRB Segment number                   FAB
MAC <-> IP mapping cache size        128
Max DLSw sessions                    1000
DLSw global memory allotment         141312
LLC per-session memory allotment     8192
SDLC per-session memory allotment    4096
NetBIOS UI-frame memory allotment    40960

Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor Priority              MEDIUM

DLSw config>LIST OPEN     28
Interface  SAP
0            0
0            4
0            8
0            C

DLSw config>EXIT
Config>
*RESTART
Are you sure you want to restart the gateway? (Yes or [No])YES
```

Figure 136 (Part 7 of 8). Scenario X1 - Remote DLSw and SDLC Host Access - 2210A Configuration

```
*Talk 5     29

CGW Operator Console

+PROTOCOL DLSw     30

DLSw>LIST TCP SESSIONS     31

   Group   IP Address      Conn State     CST  Version  Active Sess Sess Creates
   ------- --------------- -------------- ---  -------- ----------- ------------
1  Peer 1  10.8.8.1        ESTABLISHED     a   AIW V1R0      2          49

DLSw>LIST DLS SESSIONS ALL     32

         Source         Destination      State     Flags    Dest IP Addr    Id
     --------------  --------------  ---------  -------  --------------  ----
   1 SDLC 01-C1   04  40002210B2C1 04  CONNECTED           10.8.8.1          48
   2 SDLC 01-C2   04  08005AFA6BFE 04  CONNECTED           10.8.8.1          52

DLSw>LIST SDLC SESSIONS     33

      Net   Address  Source SAP/MAC    Dest SAP/MAC     PU  OutQ   State
   1.  1    C1       04 402210374501   04 40002210B2C1  5    0     CONTACTED
   2.  1    C2       04 402210374502   04 08005AFA6BFE  5    0     CONTACTED
```

Figure 136 (Part 8 of 8). Scenario X1 - Remote DLSw and SDLC Host Access - 2210A Configuration

Notes:

1. Talk to the Configuration process.
2. List all the devices.
3. Set the data link type for Interface 1 to SDLC.
4. Start the configuration of the SDLC interface.
5. Set the link role type to Secondary.
6. Set the SDLC transmission encoding scheme as NRZI (Non-Return to Zero Inverted).
7. Add an SDLC station, which will represent the attachment of the remote SDLC-attached workstation to the 3745.
8. Add an SDLC station, which will represent the attachment of the remote LAN-attached workstation to the 3745.
9. List the SDLC link to ensure that everything is correct.
10. List all of the stations' information.
11. Start the IP configuration process.
12. List the IP configuration to make sure everything is correct.
13. Start the OSPF configuration process.
14. Enable MOSPF for use with the DLSw groups.
15. List the OSPF configuration to make sure all are correct.
16. Begin the bridge configuration.
17. Enable bridging.
18. Enable DLSw on the bridge.
19. List the bridge to ensure that everything is correct.
20. Begin the DLSw configuration process.
21. Enable DLSw.
22. Set the DLSw Virtual Segment number.
23. Open SAPs 04 for DLSw switching on interface 0.
24. Join the DLSw Group as a Peer.
25. Add a DLSw SDLC station.
26. Check the SDLC Station definitions for accuracy.
27. List the DLSw configuration to ensure that everything is correct.

28 List all open SAPs and their associated interfaces.

29 Talk to the GWCON process for monitoring 2210/2216 activity.

30 Access the DLSw monitoring console.

31 List the DLSw TCP sessions.

32 List the DLSw SDLC session information to determine the state of the SDLC connection. CONTACTED indicates that a UA or Unnumbered Acknowledgment was sent in response to a SABME or Set Asynchronous Balanced Mode Extended command. This is the state you would like to see devices in and indicates that the device polling or session initiation sequence completed successfully.

33 List the DLSw sessions. In this scenario, there are also two DLSw sessions on router 2210A.

```
On the 2210 Navigation Window:
    Select CONFIGURE from the menu bar
        Select NEW CONFIGURATION      1
            Select 2210-24T(TR/WWW/WWW/WWW/WWW/TR)
                Select Empty slot

On the 2210 Navigation Window:
Select INTERFACES on the DEVICES directory
       Select CONFIGURE of interface 0      2
           ENABLE INTERFACE
           MAC ADDRESS = 40002210B001
           Select SPEED
               Select 4
           Select PACKET SIZE
               Select 2052
           Select CABLE TYPE
               Select STP
           RIF TIMER = 120
           DISABLE END NODE SOURCE ROUTING

       Select the data-link protocol of Serial 1 (PPP by default)
          Select PPP

       Select CONFIGURATION of Serial 1      3
          On GENERAL subpanel :
         On GENERAL subpanel :
             ENABLE INTERFACE
             MAXIMUM TRANSMISSION UNIT = 2048
             Select ENCODING
                 Select NRZ
             Select IDLE
                 Select FLAG
          Select CLOCKING
              Select INTERNAL
          CLOCK SPEED = 0
          TRANSMIT DELAY = 0
          Select CABLE TYPE
              Select RS-232 DCE
      Select subpanel LCP
          RETRY TIMER = 3000
          CONFIG TRIES = 20
          NAK TRIES = 10
          TERMINATE TRIES = 10
          MAXIMUM RECEIVE UNIT = 2048
```

Figure 137 (Part 1 of 5). Remote DLSw Scenario - 2210B Configuration Using Configuration Program

```
   Select subpanel BNCP
       ENABLE MAGIC NUMBER
       DISABLE TINYGRAM COMPRESSION
   Select subpanel IPCP
       DISABLE IP Compression
       Number of Slots = 16
       DISABLE SEND IP ADDRESS
       DISABLE REQUEST IP ADDRESS

Select the data-link protocol of Serial 2 (PPP by default)
    Select SDLC      4

Select CONFIGURE of Serial 2      5
   On GENERAL subpanel :
       ENABLE INTERFACE
       MAXIMUM TRANSMISSION UNIT = 2048
       Select ENCODING
            Select NRZ
        Select IDLE
            Select FLAG
        Select CLOCKING
            Select EXTERNAL
        CLOCK SPEED = 0
        TRANSMIT DELAY = 0
        Select CABLE TYPE
            Select RS-232 DTE

    On DETAIL subpanel :
        ENABLE LINK
        LINK NAME = LINK_2
        Select ROLE
            Select PRIMARY
        Select TYPE
            Select : Point to Point
        Select DUPLEX
            Select FULL
        Select MODULO
            Select 8
        XID TIMEOUT = 2000
        XID RETRY = 4
        SNRM TIMEOUT = 2000
        SNRM RETRY = 6
        RTS HOLD = 0
    On Station subpanel :      6
         ENABLE STATION
         ADDRESS = 01
```

Figure 137 (Part 2 of 5). Remote DLSw Scenario - 2210B Configuration Using Configuration Program

```
            RECEIVE WINDOW SIZE = 7
            TRANSMIT WINDOW SIZE = 7
            NAME = SDLC_01
            PACKET SIZE = 1024
            Select ADD
On the 2210 Navigation Window:
Select GENERAL on the IP directory

On the IP GENERAL Window:        7
    DISABLE ACCESS CONTROL
    ENABLE DIRECTED-BROADCAST
    DISABLE PER-PACKET-MULTIPATH
    DISABLE ARP SUBNET ROUTING
    DISABLE ARP NETWORK ROUTING
    INTERNAL ADDRESS = 10.8.8.1
    ROUTING TABLE SIZE = 768
    CACHE SIZE = 64
    ROUTER ID = 2210B
    REASSEMBLY ORIGINATED IP PACKETTIME TO LIVE =64
    ENABLE REPLY TO ICMP ECHO REQUESTS(PING)
    ENABLE FORWARD SOURCE-ROUTED PACKETS

On the 2210 Navigation Window:
Select INTERFACES on the IP directory

On the IP INTERFACES Window:
    Select IP ADDRESSES for interface 0      8
       IP ADDRESS = 8.8.8.1
       SUBNET MASK = 255.255.255.0
       select ADD
    Select IP ADDRESSES for interface 1
       IP ADDRESS = 200.200.200.2
       SUBNET MASK = 255.255.255.0
       select ADD
On the 2210 Navigation Window:
Select GENERAL on the OSPF directory

On the OSPF GENERAL window:
    ENABLE OSPF      9
    NUMBER OF EXTERNAL ROUTES = 20
    NUMBER OF OSPF ROUTERS = 20

On the 2210 Navigation Window:
Select IP MULTICAST FORWARDING on the OSPF directory
```

Figure 137 (Part 3 of 5). Remote DLSw Scenario - 2210B Configuration Using Configuration Program

```
 On the OSPF MULTICAST FORWARDING Window:
     ENABLE MULTICAST FORWARDING     10
     DISABLE INTER AREA MULTICASTING

 On the 2210 Navigation Window:
 Select AREA CONFIGURATION on the OSPF directory
 On the OSPF AREA CONFIGURATION Window:
     On the GENERAL subpanel:
           AREA = 0.0.0.0      11
           AUTHENTICATION TYPE = 00
           SELECT ADD

On the 2210 Navigation Window:
Select INTERFACES on the OSPF directory

On the OSPF INTERFACES GENERAL Window:
    Select CONFIGURE of interface 0      12
         ENABLE OSPF
    Select CONFIGURE of interface 1
         ENABLE OSPF

On 2210 Navigation Window :
Select GENERAL on the DLSw directory

On 2210 DLSw General Window :
    ENABLE DLSw      13
    SRB SEGMENT = fab
    MAXIMUM DLSW SESSION=100
    MAC CACHE SIZE=128
    ENABLE LLC DISCONNECT

On 2210 Navigation Window :
Select MULTICAST GROUPS on the DLSw directory

On 2210 DLSw Multicast Groups Window :
    GROUP ID = 1      14
    ROLE = PEER
    TRANSMIT BUFFER SIZE = 5120
    MAXIMUM SEGMENT SIZE = 1024
    RECEIVE BUFFER SIZE =5120
    NEIGHBOR PRIORITY = MEDIUM
    CONNECTIVITY SETUP TYPE = ACTIVE
    ENABLE KEEPALIVE
    SELECT ADD
```

Figure 137 (Part 4 of 5). Remote DLSw Scenario - 2210B Configuration Using Configuration Program

```
On 2210 Navigation Window :
Select INTERFACES on the DLSw directory

On the DLSw INTERFACES Window:
    Select CONFIGURE of Interface 2      15
       SOURCE MAC ADDRESS = 40002210B201
       LINK ADDRESS = 01
       PU TYPE = 2
       DESTINATION MAC ADDRESS = 402210374501
       ID BLOCK = 05D
       POLL TYPE = SNRM
       SOURCE SAP = 4
       ID NUMBER = 05183
       DESTINATION SAP = 4
       ENABLE SDLC ADDRESS
       Select ADD

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory
 On BRIDGING - GENERAL Window :
     ENABLE BRIDGING      16
     ENABLE DLSw

 On 2210 Navigation Window :
 Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

 On BRIDGING - INTERFACES Window :
     ENABLE TOKEN-RING      17

     Select CONFIGURE of INTERFACE 0
         Select INTERFACE SUPPORTS
             Select SRB      18

 On 2210 Navigation Window :
     Select CONFIGURE from the menu bar
        Select CREATE ROUTER CONFIGURATION      19


 On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
     Enter dlspppb
     Select OK
```

Figure 137 (Part 5 of 5). Remote DLSw Scenario - 2210B Configuration Using Configuration Program

Notes:

1. Start a new configuration and use Token-ring Model 24T.
2. Configure the token-ring interface.
3. Configure the PPP interface.
4. Set the data link for interface 2 to SDLC.
5. Configure the SDLC interface.

6 Configure the SDLC link.

7 Set the internal IP address.

8 Add IP address to interface 0 and interface 1.

9 Enable OSPF.

10 Enable MOSPF.

11 Add area 0.0.0.0 to the OSPF configuration.

12 Configure OSPF on interface 0 and 1.

13 Enable DLSw and set the virtual segment number.

14 Add this router to DLSw group number 1 as a peer.

15 Add the SDLC device configuration to DLSw.

16 Enable bridging and DLSw on the bridge.

17 Enable bridging on the token-ring.

18 Set the bridging method to SRB.

19 Create a router configuration file.

```
On the 2210 Navigation Window:
    Select CONFIGURE from the menu bar
        Select NEW CONFIGURATION      1
            Select 2210-126/8(ET/WWW/WWW/ISDN)

On the 2210 Navigation Window:
Select INTERFACES on the DEVICES directory
       Select CONFIGURE of interface 0      2
           ENABLE INTERFACE
           CONNECTOR TYPE = AUTO CONFIG
           IP ENCAPSULATION = ETHERNET


   Select the data-link protocol of Serial 1 (PPP by default)
       Select SDLC      3

   Select CONFIGURE of Serial 1      4
      On GENERAL subpanel :
          ENABLE INTERFACE
          MAXIMUM TRANSMISSION UNIT = 2048
          Select ENCODING
              Select NRZI
           Select IDLE
              Select FLAG
           Select CLOCKING
              Select EXTERNAL
           CLOCK SPEED = 0
           TRANSMIT DELAY = 0
           Select CABLE TYPE
              Select RS-232 DTE

       On DETAIL subpanel :       5
           ENABLE LINK
           LINK NAME = LINK_2
           Select ROLE
              Select SECONDARY
           Select TYPE
              Select : Point to Point
           Select DUPLEX
              Select FULL
           Select MODULO
              Select 8
           XID TIMEOUT = 2000
           XID RETRY = 4
           SNRM TIMEOUT = 2000
           SNRM RETRY = 6
           RTS HOLD = 0
```

Figure 138 (Part 1 of 5). Remote DLSw Scenario - 2210C Configuration

```
      On Station subpanel :      6
           ENABLE STATION
           ADDRESS = C1
           RECEIVE WINDOW SIZE = 7
           TRANSMIT WINDOW SIZE = 7
           NAME = SDLC_C1
           PACKET SIZE = 1024
           Select ADD
      Select the data-link protocol of Serial 2 (PPP by default)
         Select PPP

      Select CONFIGURATION of Serial 2      7
         On GENERAL subpanel :
        On GENERAL subpanel :
            ENABLE INTERFACE
            MAXIMUM TRANSMISSION UNIT = 2048
            Select ENCODING
                Select NRZ
            Select IDLE
                Select FLAG
         Select CLOCKING
             Select EXTERNAL
         CLOCK SPEED = 0
         TRANSMIT DELAY = 0
         Select CABLE TYPE
             Select :RS-232 DTE
     Select subpanel LCP
         RETRY TIMER = 3000
         CONFIG TRIES = 20
         NAK TRIES = 10
         TERMINATE TRIES = 10
         MAXIMUM RECEIVE UNIT = 2048
     Select subpanel BNCP
         ENABLE MAGIC NUMBER
         DISABLE TINYGRAM COMPRESSION

     Select subpanel IPCP
         DISABLE IP Compression
         Number of Slots = 16
         DISABLE SEND IP ADDRESS
         DISABLE REQUEST IP ADDRESS

On the 2210 Navigation Window:
Select GENERAL on the IP directory
```

Figure 138 (Part 2 of 5). Remote DLSw Scenario - 2210C Configuration

```
On the IP GENERAL Window:
    DISABLE ACCESS CONTROL      8
    ENABLE DIRECTED-BROADCAST
    DISABLE PER-PACKET-MULTIPATH
    DISABLE ARP SUBNET ROUTING
    DISABLE ARP NETWORK ROUTING
    INTERNAL ADDRESS = 10.24.104.93
    ROUTING TABLE SIZE = 768
    CACHE SIZE = 64
    ROUTER ID = 2210B
    REASSEMBLY ORIGINATED IP PACKETTIME TO LIVE =64
    ENABLE REPLY TO ICMP ECHO REQUESTS(PING)
    ENABLE FORWARD SOURCE-ROUTED PACKETS

On the 2210 Navigation Window:
Select INTERFACES on the IP directory

On the IP INTERFACES Window:
    Select IP ADDRESSES for interface 0      9
       IP ADDRESS = 9.24.104.93
       SUBNET MASK = 255.255.255.0
       select ADD
    Select IP ADDRESSES for interface 2
       IP ADDRESS = 200.200.200.1
       SUBNET MASK = 255.255.255.0
       select ADD

On the 2210 Navigation Window:
Select GENERAL on the OSPF directory

On the OSPF GENERAL window:
    ENABLE OSPF      10
    NUMBER OF EXTERNAL ROUTES = 20
    NUMBER OF OSPF ROUTERS = 20

On the 2210 Navigation Window:
Select IP MULTICAST FORWARDING on the OSPF directory

On the OSPF MULTICAST FORWARDING Window:
    ENABLE MULTICAST FORWARDING     11
    DISABLE INTER AREA MULTICASTING
On the 2210 Navigation Window:
Select AREA CONFIGURATION on the OSPF directory
```

Figure 138 (Part 3 of 5). Remote DLSw Scenario - 2210C Configuration

```
 On the OSPF AREA CONFIGURATION Window:
     On the GENERAL subpanel:
           AREA = 0.0.0.0      12
           AUTHENTICATION TYPE = 00
           SELECT ADD

On the 2210 Navigation Window:
Select INTERFACES on the OSPF directory

On the OSPF INTERFACES GENERAL Window:
    Select CONFIGURE of interface 0      13
         ENABLE OSPF
    Select CONFIGURE of interface 2
         ENABLE OSPF

On 2210 Navigation Window :
Select GENERAL on the DLSw directory

On 2210 DLSw General Window :
    ENABLE DLSw      14
    SRB SEGMENT = fab
    MAXIMUM DLSW SESSION=100
    MAC CACHE SIZE=128
    ENABLE LLC DISCONNECT

On 2210 Navigation Window :
Select MULTICAST GROUPS on the DLSw directory

On 2210 DLSw Multicast Groups Window :
    GROUP ID = 1      15
    ROLE = PEER
    TRANSMIT BUFFER SIZE = 5120
    MAXIMUM SEGMENT SIZE = 1024
    RECEIVE BUFFER SIZE =5120
    NEIGHBOR PRIORITY = MEDIUM
    CONNECTIVITY SETUP TYPE = ACTIVE
    ENABLE KEEPALIVE
    SELECT ADD

On 2210 Navigation Window :
Select INTERFACES on the DLSw directory

On the DLSw INTERFACES Window:
    Select CONFIGURE of Interface 1      16
       SOURCE MAC ADDRESS =  402210374501
       LINK ADDRESS = C1
```

Figure 138 (Part 4 of 5). Remote DLSw Scenario - 2210C Configuration

```
       PU TYPE = 5
       DESTINATION MAC ADDRESS = 40002210B2C1
       SOURCE SAP = 4
       DESTINATION SAP = 4
       ENABLE SDLC ADDRESS
       Select ADD

       SOURCE MAC ADDRESS =  402210374502
       LINK ADDRESS = C1
       PU TYPE = 5
       DESTINATION MAC ADDRESS = 08005AFA6BFE
       SOURCE SAP = 4
       DESTINATION SAP = 4
       ENABLE SDLC ADDRESS
       Select ADD

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory
 On BRIDGING - GENERAL Window :                    save
     ENABLE BRIDGING      17
     ENABLE DLSw

 On 2210 Navigation Window :
 Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

 On BRIDGING - INTERFACES Window :
     ENABLE ETHERNET      18

     Select CONFIGURE of INTERFACE 0
         Select INTERFACE SUPPORTS
             Select STB      19
             Select STE&TSF

 On 2210 Navigation Window :
     Select CONFIGURE from the menu bar
        Select CREATE ROUTER CONFIGURATION      20

 On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
     Enter dlspppc
     Select OK
```

Figure 138 (Part 5 of 5). Remote DLSw Scenario - 2210C Configuration

Notes:

1 Start a new configuration and use Ethernet Model 128.

2 Configure the Ethernet interface.

4 Configure the SDLC interface and set the SDLC transmission encoding scheme as NRZI.

5 Set the SDLC link roll as secondary.

6 Configure the SDLC link.

7 Set the data link for interface 1 to SDLC.

8 Set the internal IP address.

8 Add IP address to interface 0 and interface 2.

9 Enable OSPF.

10 Enable MOSPF.

11 Add area 0.0.0.0 to the OSPF configuration.

12 Configure OSPF on interface 0 and 2.

13 Enable DLSw, set the virtual segment number.

14 Add this router to DLSw group number 1 as a peer.

15 Add the SDLC device configuration to DLSw.

16 Enable bridging and DLSw on the bridge.

17 Enable bridging on the Ethernet.

18 Set the bridging method to STB.

19 Create a router configuration file.

8.6.2 Scenario X2 - Local DLSw Using SDLC-to-SDLC for Host Access

In this scenario, we used the same 2210B router of the previous setup in 8.6.1, “Scenario X1 - Remote DLSw Using SDLC for Host Access” on page 230 to show a local DLSw implementation. There is already the CM/2 PU Type 2.0 on the token-ring and PCOMM/3270 PU2.0 on the SDLC attached to 2210B. To complete the local DLSw scenario, we configured a secondary SDLC link to attach to the 3745 and host.

8.6.2.1 Environment

Most of the configuration in 2210B was done in the last scenario so we do not repeat it here. For more details about this procedure, please refer to the last scenario. We show the procedure to add a secondary SDLC and to enable local DLSW in router B.

Figure 139 on page 263 is a pictorial representation of this scenario.

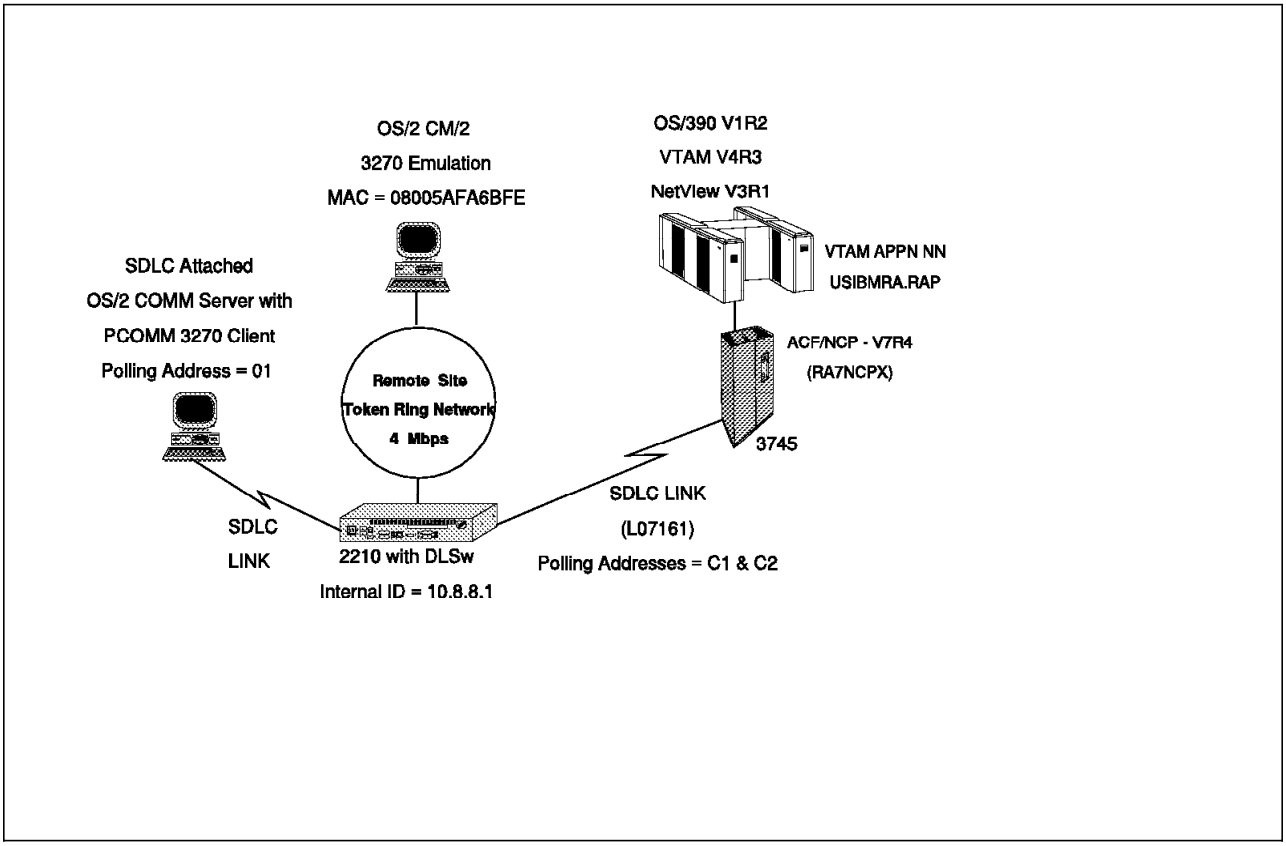


Figure 139. Scenario of Local DLSw

Figure 140 on page 264 shows the configuration process for 2210B using the Nways MRS Configure process.

Figure 141 on page 267 shows the configuration process for 2210c using the Nways MRS Configuration program.

```
*talk 6     1

Config>set data-link sdlc      2
Interface Number [1]?3

Config>network 3     3
SDLC user configuration
Creating a default configuration for this link
SDLC 3 Config>list link     4
Link configuration for: LINK_3   (ENABLED)

Role:         PRIMARY          Type:         POINT-TO-POINT
Duplex:       FULL             Modulo:       8
Idle state:   FLAG             Encoding:     NRZ
Clocking:     EXTERNAL         Frame Size:   2048
Speed:        0                Group Poll:   00
Cable:        RS-232 DTE

Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
           RTS hold delay:     DISABLED
           Inter-frame delay:  DISABLED
           Inactivity timeout: 30.0 sec

Counters:  XID/TEST retry:  8
           SNRM retry:      6
           Poll retry:      10
SDLC 3 Config>set link role secondary     5
SDLC 3 Config>set link encoding nrzi     6
SDLC 3 Config>add station      7
Enter station address (in hex) [C1]?
Enter station name [SDLC_C1]?
Include station in group poll list ([Yes] or No)n
Enter max packet size [2048]?521
Enter receive window :[7]?
Enter transmit window [7]?
SDLC 3 Config>add station      8
Enter station address (in hex) [C2]?
Enter station name [SDLC_C2]?
Include station in group poll list ([Yes] or No)no
Enter max packet size [2048]?521
Enter receive window [7]?
Enter transmit window [7]?
SDLC 3 Config>exit

Config>protocol dls      9
DLSw protocol user configuration
DLSw config>open-sap     10
Interface # [0]3
```

Figure 140 (Part 1 of 2). Local DLSw Scenario - 2210B Configuration

```
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]?sna
SAPs 0 4 8 C opened on interface 3
DLSw config>add sdlc     11
Interface # [0]?3
SDLC Address [C1]?
Source MAC address [4022103703C1]?402210374501
Source SAP in hex [4]?
Destination MAC address [000000000000]?40002210b2c1
Destination SAP in hex [0]?4
PU type (2/4/5) [2]?5
DLSw config>add sdlc      12
Interface # [0]?3
SDLC Address [C1]?c2
Source MAC address [4022103703C2]?402210374502
Source SAP in hex [4]?
Destination MAC address [000000000000]?08005afa6bfe
Destination SAP in hex [0]?4
PU type (2/4/5) [2]?5
DLSw config>add tcp      13
Enter the DLSw neighbor IP Address [0.0.0.0]? 10.8.8.1
Adding local transport connection
Neighbor Priority (H/M/L) [M]?
DLSw config>
*restart     14
Are you sure you want to restart the gateway? (Yes or [No])yes


*talk 5     15

CGW Operator Console

+protocol dlsw    16

DLSw>list tcp session all     17
   Group   IP Address      Conn State     CST  Version  Active Sess Sess Creates
   ------- --------------- -------------- ---  -------- ----------- ------------
1          10.8.8.1        ESTABLISHED     a   AIW V1R0      6          14
2          10.24.104.93    ESTABLISHED     D   AIW V1R0      0           0

DLSw>list dls session all     18
         Source          Destination      State     Flags    Dest IP Addr    Id
     --------------  --------------  ---------  -------  --------------  ----
   1 SDLC 02-C1   04  402210374501 04  CONNECTED           LOCAL              4
   2 SDLC 03-C1   04  40002210B2C1 04  CONNECTED           LOCAL              5
   3 SDLC 03-C1   04  40002210B2C1 04  CONNECTED           LOCAL              2
   4 SDLC 02-C1   04  402210374501 04  CONNECTED           LOCAL              3
   5 SDLC 03-C2   04  08005AFA6BFE 04  CONNECTED           LOCAL             12
   6 08005AFA6BFE 04  402210374502 04  CONNECTED           LOCAL             13
DLSw>list sdlc session     19
      Net   Address  Source SAP/MAC    Dest SAP/MAC     PU  OutQ   State
   1.  2    C1       04 40002210B2C1   04 402210374501  2    0     CONTACTED
   2.  3    C1       04 402210374501   04 40002210B2C1  5    0     CONTACTED
   3.  3    C2       04 402210374502   04 08005AFA6BFE  5    0     CONTACTED
```

Figure 140 (Part 2 of 2). Local DLSw Scenario - 2210B Configuration

Notes:

1 Talk to the Config process.

2 Set the data link for interface 2 to SDLC.

3 Start configuration of the SDLC interface.

4 List the SDLC link to ensure that everything is correct.

5 Send the link role as secondary. The 3745 is the primary.

6 Set the SDLC transmission encoding scheme as NRZI (Non-Return to Zero Inverted). This is the encoding configured in NCP.

7 Add an SDLC station which will be used later by this router to attach to the 3745 the PComm/3270 PC client connected to its other SDLC port.

8 Add an SDLC station which will be used later by this router to attach to the 3745 the CM/2 PC client connected to its token-ring.

9 Start customization of DLSw.

10 Open SNA SAPs for DLSw switching in interface 3.

11 Add a DLSw SDLC station. We configured the locally administered source MAC address for the first SDLC address from the 3745/NCP. The locally administered destination MAC address refers to the SDLC address of our 2210 port which is connected to the SDLC-attached PComm/3270 PC client.

12 Add a DLSw SDLC station. We configured the locally administered source MAC address for the second SDLC address from the 3745/NCP. The destination MAC address refers to the real MAC address of the token-ring attached CM/2 PC client.

13 Add a DLSW neighbor which in this case is this router's own internal IP address. This will enable the local DLSw functionality.

14 Talk to the GWCON process.

15 Enter the DLSw monitoring console.

16 List the DLSw TCP sessions.

17 List the DLSw sessions. In this scenario we have two DLSw sessions:

18 List the DLSw SDLC sessions.

```
On the 2210 Navigation Window:
    Select CONFIGURE from the menu bar
        Select NEW CONFIGURATION      1
            Select 2210-24T(TR/WWW/WWW/WWW/WWW/TR)
                Select Empty slot


   Select the data-link protocol of Serial 3 (PPP by default)
       Select SDLC      4

   Select CONFIGURE of Serial 3      5
      On GENERAL subpanel :
          ENABLE INTERFACE
          MAXIMUM TRANSMISSION UNIT = 2048
          Select ENCODING
              Select NRZ
           Select IDLE
              Select FLAG
           Select CLOCKING
              Select EXTERNAL
           CLOCK SPEED = 0
           TRANSMIT DELAY = 0
           Select CABLE TYPE
              Select RS-232 DTE

       On DETAIL subpanel :
           ENABLE LINK
           LINK NAME = LINK_3
           Select ROLE
              Select PRIMARY
           Select TYPE
              Select : Point to Point
           Select DUPLEX
              Select FULL
           Select MODULO
              Select 8
           XID TIMEOUT = 2000
           XID RETRY = 4
           SNRM TIMEOUT = 2000
           SNRM RETRY = 6
           RTS HOLD = 0
       On Station subpanel :      6
            ENABLE STATION
            ADDRESS = C1
```

Figure 141 (Part 1 of 2). 2210B Configuration

```
            RECEIVE WINDOW SIZE = 7
            TRANSMIT WINDOW SIZE = 7
            NAME = SDLC_C1
            PACKET SIZE = 1024
            Select ADD
 On the 2210 Navigation Window:
 Select GENERAL on the IP directory


On 2210 Navigation Window :
Select INTERFACES on the DLSw directory

On the DLSw INTERFACES Window:
    Select CONFIGURE of Interface 3
       SOURCE MAC ADDRESS = 402210374501
       LINK ADDRESS = C1
       PU TYPE = 5
       DESTINATION MAC ADDRESS = 40002210b2c1
       SOURCE SAP = 4
       DESTINATION SAP = 4
       ENABLE SDLC ADDRESS
       Select ADD
       SOURCE MAC ADDRESS = 402210374502
       LINK ADDRESS = C1
       PU TYPE = 2
       DESTINATION MAC ADDRESS = 08005afa6bfe
       SOURCE SAP = 4
       DESTINATION SAP = 4
       ENABLE SDLC ADDRESS
       Select ADD


 On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
     Enter dlspppb
     Select OK
```

Figure 141 (Part 2 of 2). 2210B Configuration

Notes:

1. Start a new configuration and use Token-ring Model 24T.
2. Configure the token-ring interface.
3. Configure the PPP interface.
4. Set the data link for interface 2 to SDLC.
5. Configure the SDLC interface.
6. Configure the SDLC link.
7. Set the internal IP address.
8. Add IP address to interface 0 and interface 1.

9 Enable OSPF.

10 Enable MOSPF.

11 Add area 0.0.0.0 to the OSPF configuration.

12 Configure OSPF on interface 0 and 1.

13 Enable DLSw and set the virtual segment number.

14 Add this router to DLSw group number 1 as a peer.

15 Add the SDLC device configuration to DLSw.

16 Enable bridging and DLSw on the bridge.

17 Enable bridging on the token-ring.

18 Set the bridging method to SRB.

19 Create a router configuration file.

Part 3. ATM

Chapter 9. Introduction

Part III of this redbook provides the information you need to understand and work with Asynchronous Transfer Mode (ATM) on the IBM 2216 Nways Multiaccess Connector and the IBM 2210 Nways Multiprotocol Router. We start in this chapter by introducing the ATM support provided with these products.

Chapter 10, “ATM and Cell Relay” on page 275 provides an overview of ATM as a transport mechanism and how devices use a cell relay network to communicate.

Chapter 11, “ATM Forum LAN Emulation” on page 285 provides an overview of the ATM Forum’s LAN Emulation specifications and detailed information about using LAN emulation on the 2210 and 2216.

Chapter 12, “Classical IP” on page 313 provides an overview of the IETF’s Classical IP and detailed information about using Classical IP on the 2210 and 2216. This chapter also provides information on the RFC 1483 support provided by the 2210 and 2216 for using IPX over ATM.

9.1 Positioning the 2210 and 2216 in ATM Networks

As can be seen in Figure 142, the 2210 and 2216 play an important role in tying together ATM and legacy networks. They provide access to the ATM network for both wide area traffic and LAN-attached devices.

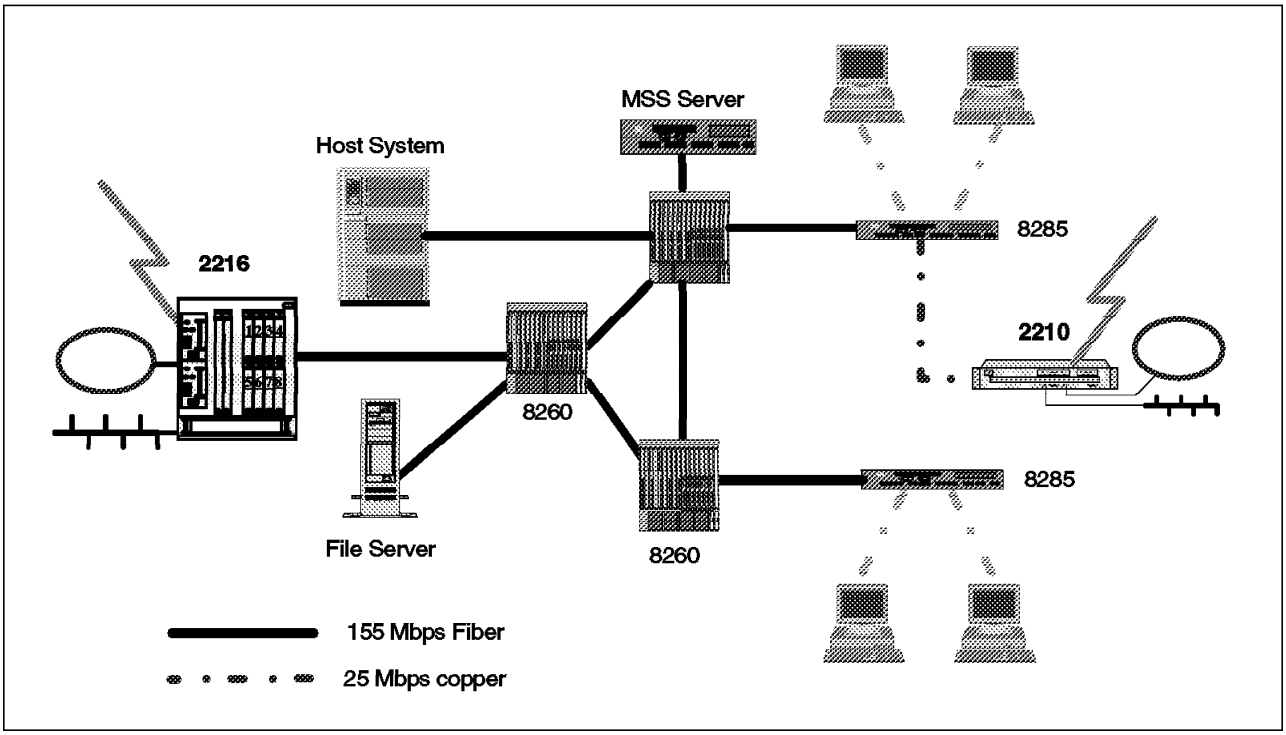


Figure 142. The 2210 and 2216 in ATM Networks

In a pure ATM network, a traditional router operating at the network layer has no good role to play. This is because ATM switches operate well below the network layer (layer 3).

The LAN emulation and classical IP support provided in the 2210 and the 2216 allow these machines to participate in the ATM network to provide connectivity to non-ATM networks.

9.2 2210 and 2216 ATM Support at a Glance

The IBM 2210 Nways Multiprotocol Router and IBM 2216 Nways Multiaccess Connector provide a multiprotocol connection to ATM networks from legacy LANs and WANs by providing:

- Connection to an ATM switch using a 155 Mbps multimode or single-mode fiber ATM adapter (2216) or a 25 Mbps copper UTP ATM adapter (2210)
- UNI 3.0, 3.1 and auto-configuration support
- ATM Forum-compliant LAN emulation, including support for Ethernet emulated LANs and token-ring emulated LANs (supports LAN emulation clients only)
- Standards-based IP routing support on ATM, including support for Classical IP LIS clients and ARP servers. Supports routing between:
  - LANs/WANs and emulated LANs
  - LANs/WANs and Classical IP subnets
  - Emulated LANs and Classical IP subnets
- Standards-based bridging over LAN Emulation including:
  - Transparent bridging
  - Source-route bridging
  - Source-route to transparent bridging
  - Source-route and transparent bridging
  - Source-route transparent bridging
  - Adaptive source-route bridging

    The 2210 and 2216 dynamically decide bridge behavior based on the configuration. This is referred to as adaptive source route bridging (ASRT).
- Standards-based Novell IPX routing support on ATM between LANs/WANs and emulated LANs
- Support for IPX connections to other routers across ATM using RFC 1483 via either PVCs or static SVCs
- A user-friendly environment with:
  - A graphical configuration tool with integrated contextual help information
  - Remote access port for command line configuration and monitoring
  - Service port access for command line local configuration and monitoring

All of these functions are discussed in more detail in the succeeding chapters.

Chapter 10. ATM and Cell Relay

This chapter discusses how ATM networks operate. It will give you a better understanding of how the 2210 and 2216 interface to the switch and communicate with other ATM-attached devices over the cell relay network.

Figure 143 shows the ATM layers in relation to the OSI model. Technically, Asynchronous Transfer Mode (ATM) is merely a transport mechanism: a way to move cells between nodes, hence the other name for ATM of cell relay. It defines nothing about protocols that applications could use to productively communicate. The ATM Forum LAN Emulation Specifications and the IETF′s Classical IP were both invented as a means for applications to use existing protocols to access the ATM transport.

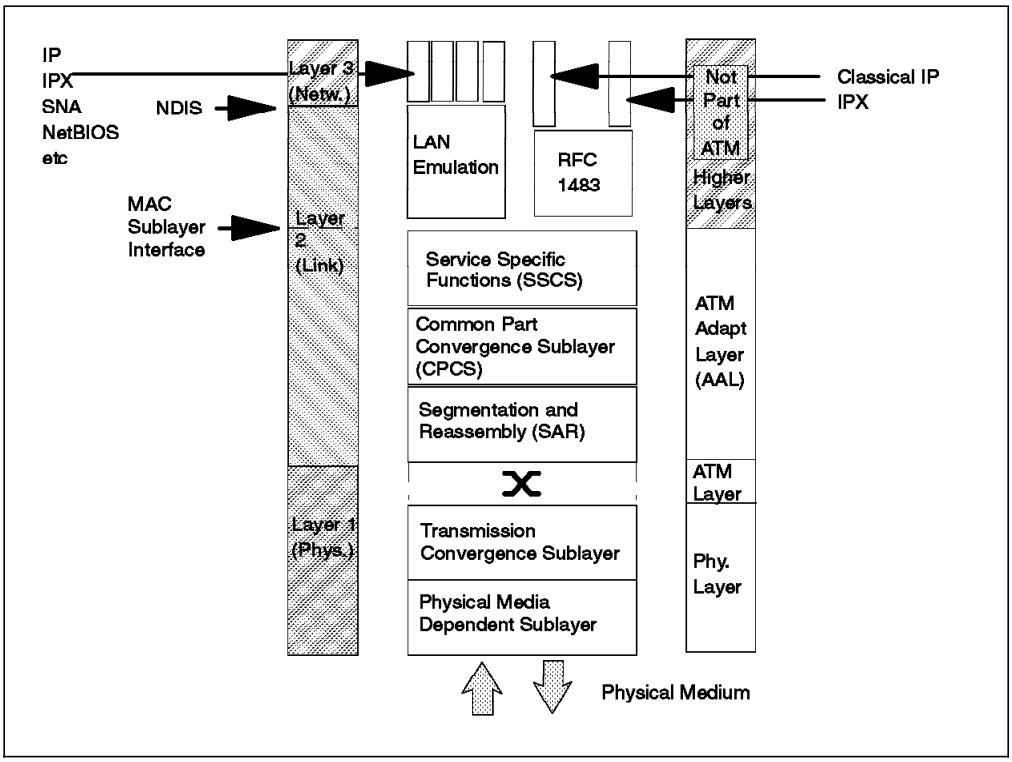


Figure 143. ATM versus the OSI Model

As a practical matter, the term ATM has taken on a much broader meaning that includes the transport layers as well as the LAN emulation and Classical IP specifications. In our discussion, we first examine ATM as a cell relay network and then move on to discuss LAN Emulation and Classical IP in succeeding chapters.

Note: It should be noted that much of the terminology used in describing ATM cell relay networks is derived from the public switched telephone network (PSTN). This is because of the fact that the telecommunications industry has helped define the ATM standards and they are using ATM as the basis of their Broadband ISDN networks.

10.1 ATM Overview

In this section, we introduce the concepts of virtual paths, virtual circuits, and the routing of ATM cells through the network. We also discuss the User/Network Interface (UNI) and ATM addressing formats.

10.1.1 Virtual Paths and Virtual Circuits

As can be seen in Figure 144, links are physical connections between two nodes, for example an OC3 link at 155 Mbps or a 25 Mbps copper link. A virtual channel (VC) is a unidirectional connection between end users. A virtual path (VP) is a route through the network representing a group of virtual channels.

The number of virtual paths and virtual channels on a link says nothing about the capacity of the link. Just one virtual channel could saturate a link or you could use all the available virtual paths and channels and still have remaining link capacity.

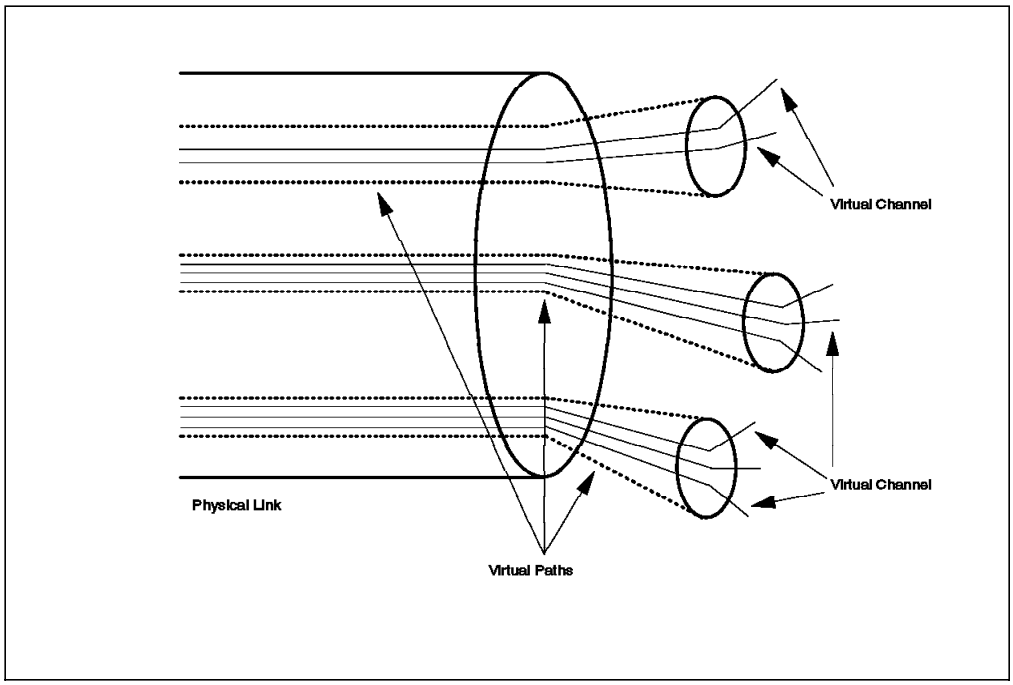


Figure 144. Physical Links, Virtual Paths, and Virtual Circuits

As can be seen in Figure 145 on page 277, virtual paths (VPs) may either terminate or connect within a switch. If they connect (are switched), then all the virtual channels (VCs) in them are switched with the virtual path. A virtual path that is switched is called a virtual path connection (VPC). Virtual channels will always terminate in an end system, but can be switched to a different virtual path within the intermediate node.

A virtual channel link is one channel within the virtual path. A virtual channel connection (VCC) is a sequence of concatenated virtual channel links that connects two end systems. This is a unidirectional path. It takes a pair of VCCs to create a bidirectional data path between two end systems.

VPCs and VCCs may be either provisioned as permanent virtual circuits (PVCs) or they may be established via signaling protocols as switched virtual circuits (SVCs).

The virtual path and virtual channel numbers are only significant on their corresponding link. The VPI/VCI numbers will change throughout the network route for any given VCC.

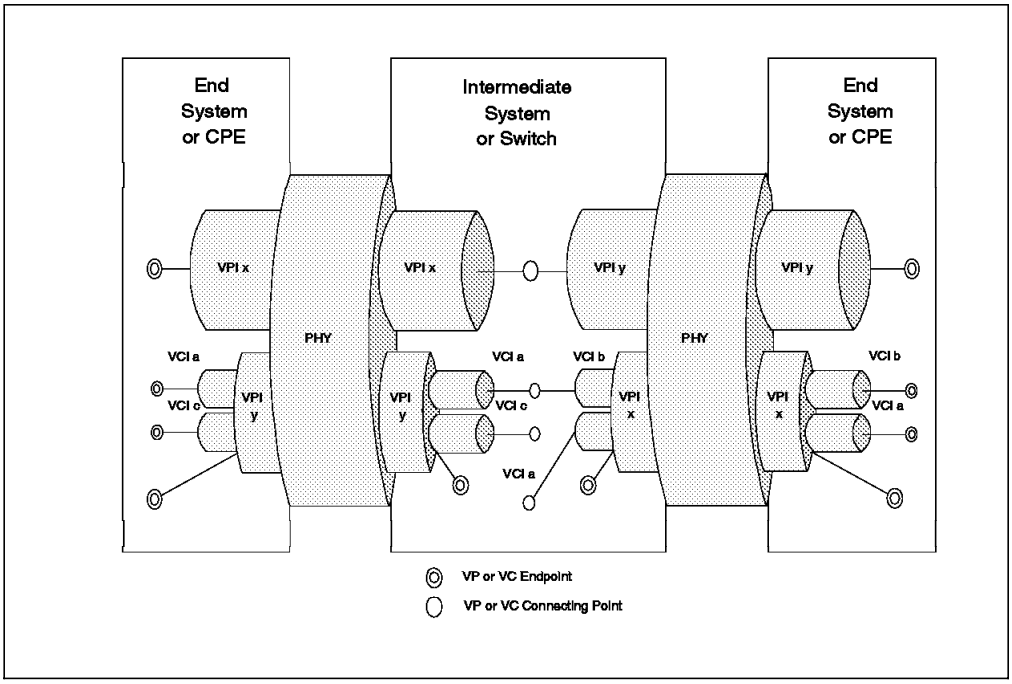


Figure 145. Terminating Virtual Paths and Virtual Circuits

As illustrated in Figure 146 on page 278, VPs may exist:

1. Between ATM endpoints (as between CPN 1 and CPN 2 and between CPN 2 and CPN 3)
2. Between ATM switches and ATM endpoints (as between NN 1 and CPN 1, NN 1 and CPN 2, and NN 2 and CPN 3)
3. Between ATM switches (as between NN 1 and NN 2)

A VP may be routed through an ATM switch by reference only to the VP number, or it may terminate in an ATM switch. A VP entering an endpoint always terminates in that endpoint.

The VP numbers are only significant to an adjacent pair of nodes.

In ATM switching product implementations, the actual number of virtual path numbers (VPIs) and virtual circuit numbers (VCIs) supported are often less than the maximum defined in the standards. This is due to memory constraints on the amount of RAM needed to maintain VPI and VCI tables. In these cases, only a certain number of the low order bits of the VPI and VCI fields are usable. The end node device and the switch negotiate the numbers to be used when the end node device gets initialized.

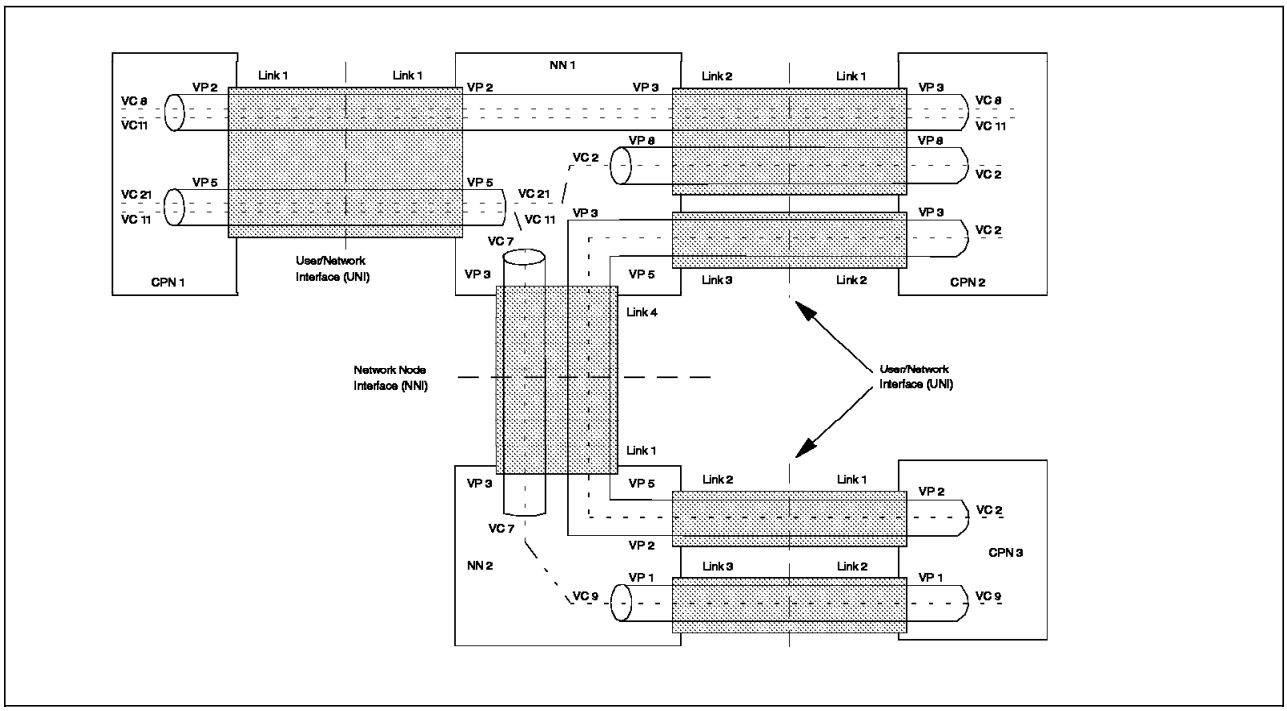


Figure 146. A Virtual Network

10.1.2 ATM Cell Format

Figure 147 on page 279 shows the ATM cell format at the User/Network Interface (UNI). ATM cells are fixed at 53 bytes in length with 5 bytes of header and 48 bytes of payload.

The VPI field is 8 bits, which allows for 256 VPs between any two adjacent nodes. The VCI field is 16 bits, which allows for 65,536 VCs between any two nodes. The VPI and VCI together define the virtual connection that the cell belongs to.

Notice that the cell does not contain the ATM address of either the source or destination device.

The range of VCIs between 0 and 31 are reserved for operation, administration, and maintenance (OAM). OAM includes such things as signaling and resource management.

Bit 0 of the PT field is used to indicate whether the cell is for user data or for OAM (bit 0=0 means user data). Bit 1 of the PT field is for Explicit Forward Congestion Indication (EFCI) and is set to 1 when the network is congested somewhere along the cell's route. (Bit 1 =1 means that the network is congested.) Bit 2 of the PT field is used by the ATM adaptation layers. For example, in ATM Adaptation Layer 5 (AAL-5), bit 2=1 means that the cell is at the end of a block of user data.

The CLP field is used to indicate that the cell may be discarded if the network is congested.

The HEC provides error detection *on the header only*, as ATM relies on upper layer protocols for error recovery.

Figure 147 on page 279 depicts the cell format for the UNI interface. The Network/Network Interface (NNI) cell format differs only slightly in that there is no GFC field. In this format, the VPI field is extended to 12 bits.

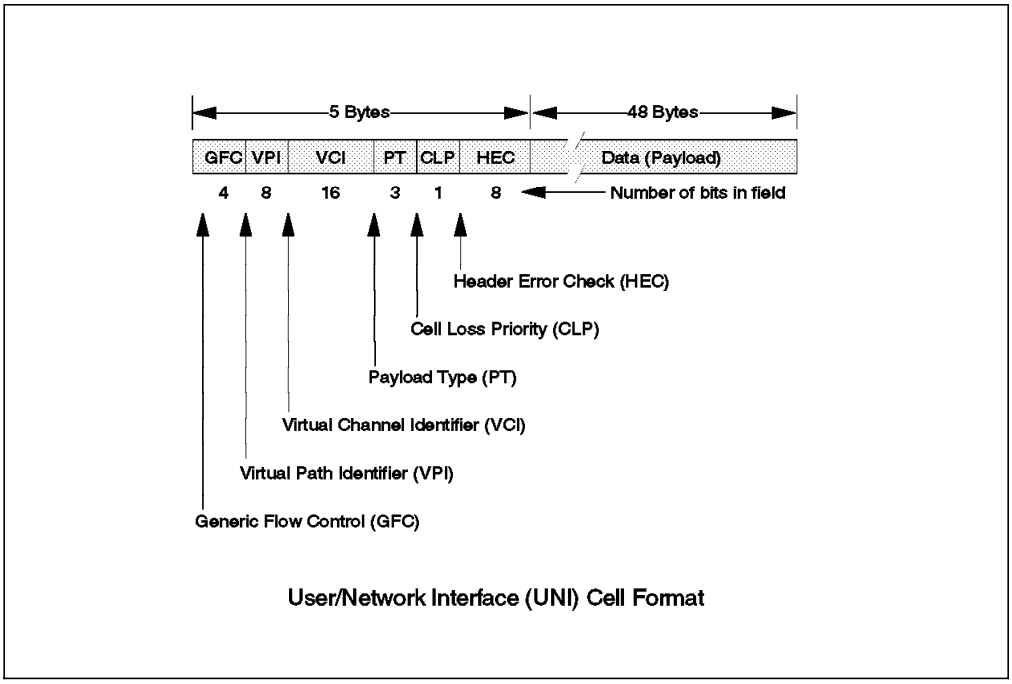


Figure 147. ATM Cell Format

10.1.3 Cell Switching

The concept of cell switching can be thought of as either a high-performance form of packet switching or as a form of statistical multiplexing performed on fixed-length blocks of data.

A cell is really not too different from a packet. A block of user data is broken up into packets or cells for transmission through the network. But there are significant differences between cell-based networks and packet networks.

1. A cell is fixed in length. In packet networks the packet size is a fixed maximum (for a given connection) but individual packets may always be shorter than the maximum. In a cell-based network, cells are a fixed length, no more and no less.
2. Cells tend to be a lot shorter than packets. This is really a compromise over requirements. In the early days of X.25 many of the designers wanted a packet size of 32 bytes so that voice could be handled properly. However, the shorter the packet size the more network overhead there is in sending a given quantity of data over a wide area network. To efficiently handle data, packets should be longer (in X.25 the default packet size supported by all networks is 128 bytes).
3. Cell-based networks do *not* use link-level error recoveries. In some networks there is an error checking mechanism that allows the network to throw away cells in error. In others, such as in ATM (described below) only the header field is checked for errors and it is left to a “higher-layer” protocol to provide a checking mechanism for the data portion of the cell if needed by the application.

Figure 148 on page 280 shows a sequence of cells from different connections being transmitted on a link. This should be contrasted with the TDM (Time Division Multiplexing) technique where capacity is allocated on a time slot basis regardless of whether there is data to send for that connection. Cell-based networks are envisaged as ones that use extremely fast and efficient hardware-based switching nodes to give very high throughput, that is, millions of cells per second. These networks are designed to operate over very low error rate, very high-speed digital (preferably optical) links.

The reasons for using this architecture are:

- If we use very short fixed-length cells then it simplifies (and therefore speeds up) the switching hardware needed in nodal switches.
- The smaller the cells can be made, the shorter the transit delay through a network consisting of multiple nodes.
- The statistical principle of large numbers means that a very uniform network transit delay with low variance can be anticipated with the cell approach.
- Intermediate queues within switching nodes contain only cells of the same length. This reduces the variation in network transit delays due to irregular-length data blocks (which take irregular lengths of time to transmit) in the queues.
- When an error occurs on a link (whether it is an access link or a link within the network itself) then there is less data to retransmit. This could be the case, but with ATM if a cell is lost for any reason (such as link error or discard due to congestion) the whole frame of which it is part must be retransmitted. In a well-designed network using optical links (low error rates) this should not bother us too much.

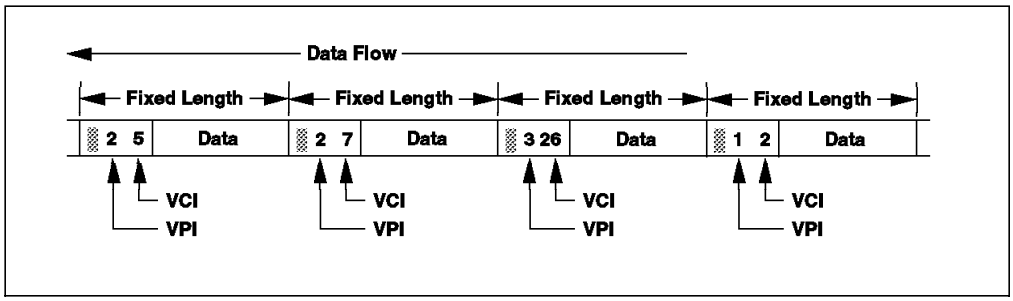


Figure 148. Cell Multiplexing on a Link

Figure 149 on page 281 depicts at a high level how a cell is routed through a switching node. As the cell enters the node, the VPI is used to locate an entry within the VPI table.

From the table, it is determined whether the VP terminates in this node or not. If the VP is switched (does not terminate), then the new VPI number and the outbound routing information are fetched from the VPI table. Only the VPI needs to be replaced here because the VCI does not change. (This case is not illustrated.)

If the virtual path terminates in the node, then the VCI is used to locate the correct entry in the VCI table. (Note that there is a separate VCI table for each terminating VP.)

The new VPI and VCI values are fetched from the table and the cell is updated with these new values. The cell is then routed on towards its destination using the new VPI/VCI entries.

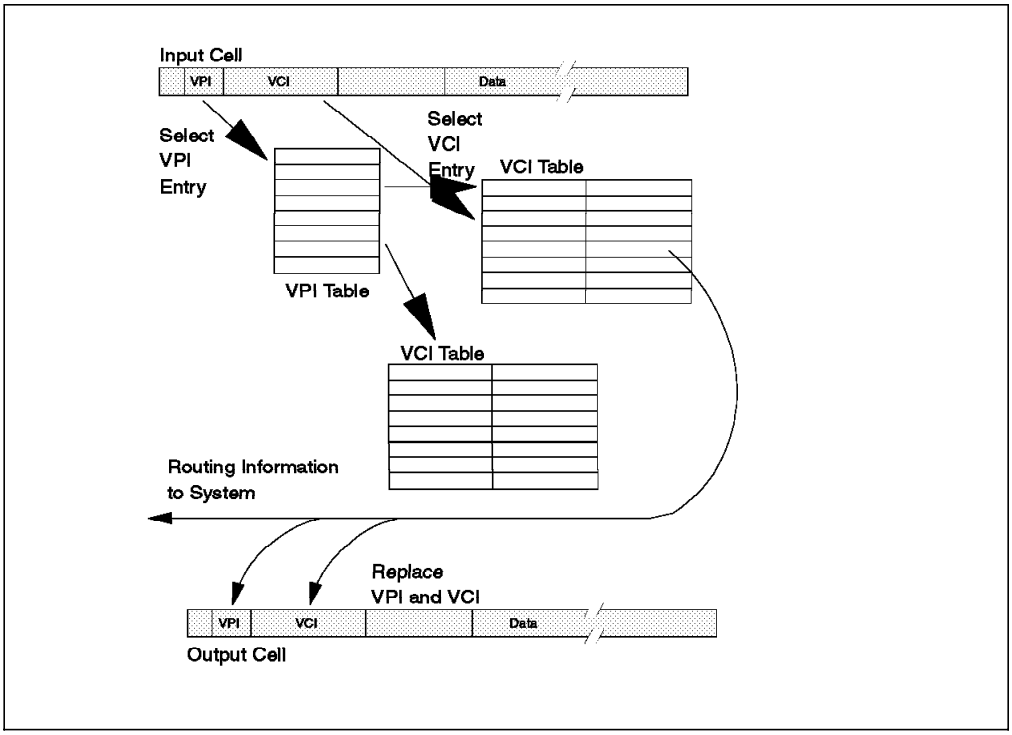


Figure 149. Switching ATM Cells

10.1.4 User/Network Interface (UNI)

The UNI defines completely the interface between the end system and the switch including the cell format. One of the most important definitions within the UNI specifications is the signaling protocol. This includes how the end system registers with the switch at initialization time and how the end system requests access to the network.

The end system also uses UNI signaling to request connection establishment with another end system and the class of service for this connection.

IBM UNI product implementations such as the 2210/16 and the MSS server support auto-configuration of the UNI version. These products will detect the UNI version at the switch and then configure the interface accordingly. If both the switch and the end station are set for auto-configuration, then the devices will use the highest level supported on both ends of the interface.

Note: Auto-config is the recommended setting because if one end is set to Version 3.0 and the other is set to 3.1, then the interface will not come up to an operational state.

10.2 ATM Addresses

Figure 150 shows the ATM address format. ATM uses 20-byte hierarchical addressing to uniquely define each device in the network. The first 13 bytes of an ATM address are called the network prefix and end systems obtain the network prefix component of their addresses from their adjacent switch.

The next six bytes of the address are called the end system identifier (ESI). The ESI is the same length as a LAN MAC address and has a burned-in value such as a MAC address that can be overridden when configuring the ATM adapter.

The final byte is called the selector. The selector is only significant within the end system and is used within end systems to uniquely identify called/calling parties. For example, when configuring multiple LAN emulation clients on the same ATM interface, each client needs to have a different selector defined. The 2210/16 will generate a unique selector if you do not specify one.

End systems form their addresses by appending an ESI and selector to the network prefix provided by the switch.

The ATM address is used for circuit establishment. After the virtual circuit has been established, the ATM address is not used. The ATM cells are switched through the network using the VPI/VCI as discussed previously.

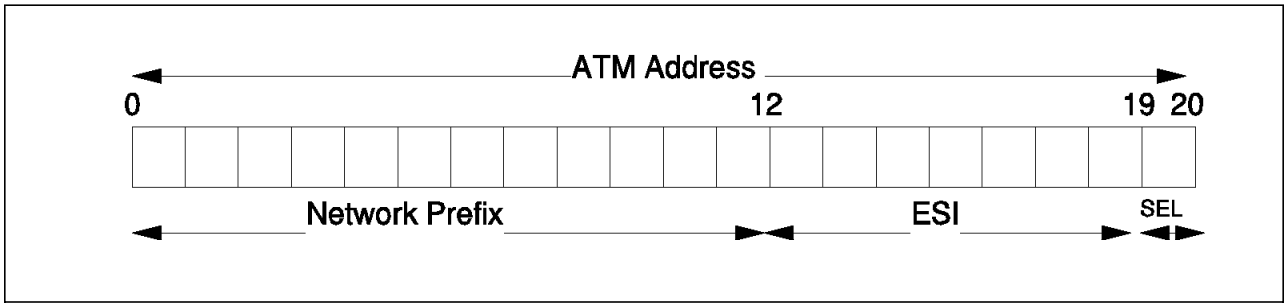


Figure 150. ATM Addresses

The network prefix and ESI components of ATM addresses must be registered with ATM switches before calls can be placed or received. If the address is not unique (that is, if it duplicates an address already registered with the switch), the switch will reject the registration.

One way to guarantee a unique ATM address is to use the burned-in (universally administered) IEEE MAC address as the ESI. Each ATM interface on the IBM 2216 Nways Multiaccess Connector contains a burned-in MAC address that may be used in this manner. The IBM 2216 also allows users to configure locally administered ESIs on each ATM interface.

10.2.1 Call Setup Example

Figure 151 on page 283 depicts the progression of a call setup using the UNI signaling protocol. To initiate a call, the calling party (device A) first notifies the switch that it wants to set up a connection to device B. The switch responds to device A with a call proceeding message while at the same time beginning to traverse the network to find a path to device B.

Once a path is found, device B is sent a setup message (from the switch it attaches to) with the VPI/VCI to use if it chooses to accept the call. Device B

accepts the call by returning the connect message, which is propagated back to device A.

In the message back to device A, the local switch gives it the VPI/VCI to use on its end. (Remember that the two VCI/VPI pairs will be different on each end.)

The connect acknowledgment is sent to device B to complete the handshake to the called party. After device A receives the connect message, it then responds to the switch with a connect acknowledgment.

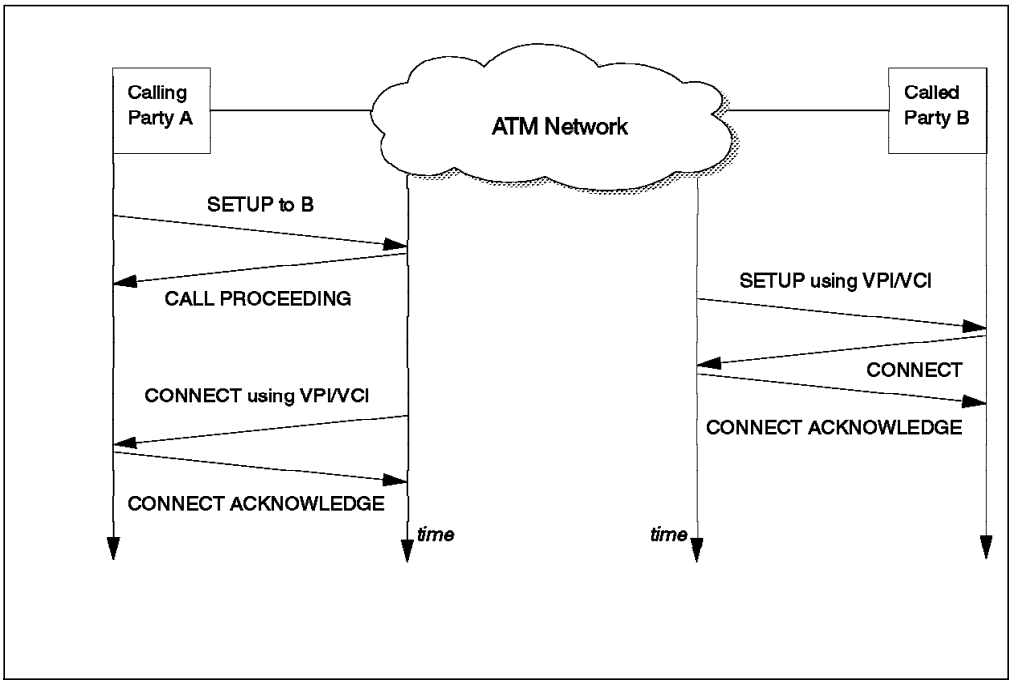


Figure 151. Establishing a Switched Virtual Circuit (SVC) or Call Setup

Chapter 11. ATM Forum LAN Emulation

This chapter introduces the basic concepts of ATM Forum-compliant (FC) LAN emulation and how this support is implemented in the IBM 2216 Nways Multiaccess Connector and IBM 2210 Nways Multiprotocol Router.

Reading this section will assist you in understanding and implementing emulated LANs (ELANs) using these and other products that provide LAN emulation services. Where relevant, we have included specific references to both the 2210 and the 2216.

11.1 Overview

Today′s networking applications are running primarily on Ethernet and token-ring networks that interface to LAN adapters via standard interfaces such as ODI and NDIS. ATM APIs (application programming interfaces) are under development that will allow applications to interface directly with the ATM layer and take advantage of all of ATM′s advanced features (such as quality of service). In the meantime, a service is required that will allow existing applications to take advantage of at least some of ATM′s benefits today, such as high-speed switched connections and scalability. This service is called LAN emulation.

Figure 152 on page 286 shows a physical view of an ATM network and a logical view of two emulated LANs (ELANs) that could be implemented with this physical network. The LAN emulation protocols used in the end devices provide the appearance of Ethernet and token-ring LANs to the *legacy* applications that interface to them such that they and the existing protocol stacks are able to run unmodified over the ATM cell relay network. (ELANs emulate either token-ring or Ethernet, but not both simultaneously.)

ELANs are independent of each other. An end system can join two ELANs simultaneously by using two instances of the LAN emulation client. This is shown in Figure 152 on page 286 with the host being attached to both ELANs.

LAN emulation allows ATM coexistence with legacy LANs and at the same time allows for a smooth transition to an all-ATM network. It also provides investment protection for existing applications and LAN equipment.

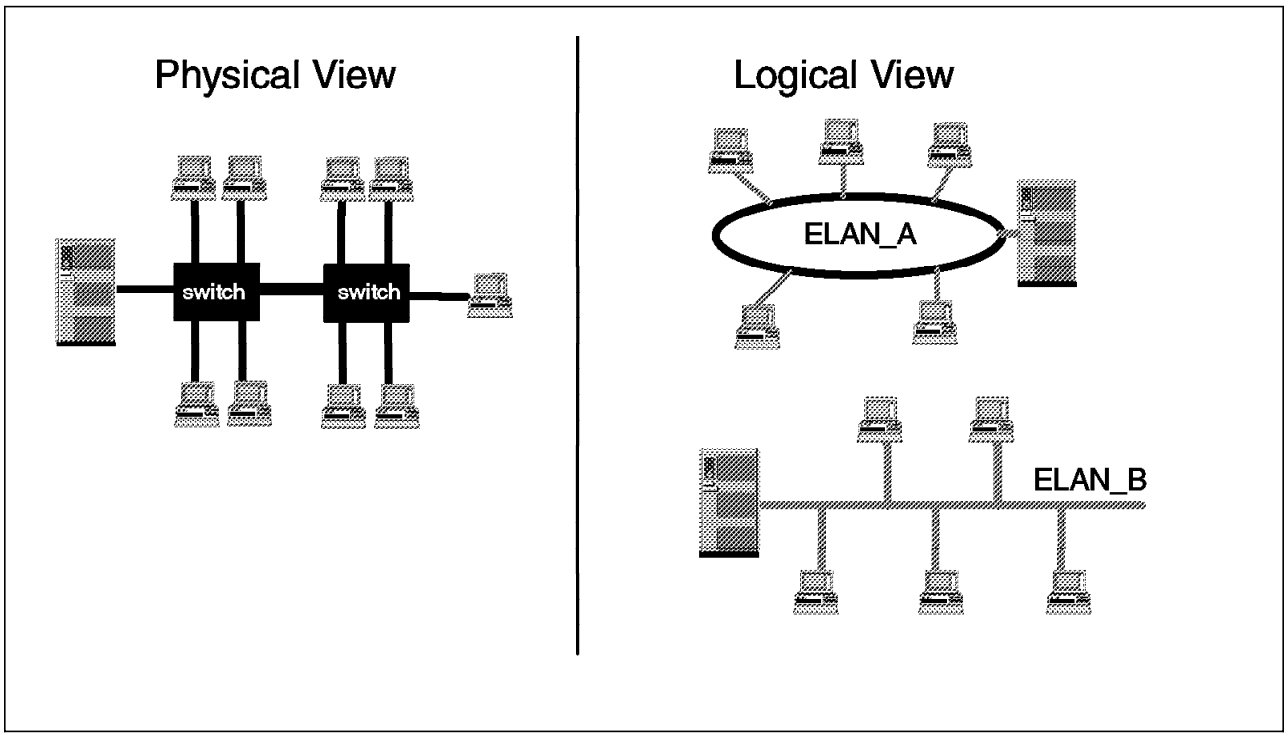


Figure 152. Physical and Logical Views of LAN Emulation

The 2210 and 2216 can be used to route/bridge between ELANs on the same ATM interface and also between ELANs and other router interfaces. The routers use their LAN emulation client capability to participate in the ELAN, acting as a proxy for devices downstream of their ATM interface.

Figure 153 on page 287 shows an example of an ATM device (device A on ELAN_A) communicating with a device on a legacy LAN segment (device B). In this example, device A will establish a switched virtual circuit (SVC) to the LAN emulation client on the router interface and the router will bridge/route all traffic between the two devices.

Figure 154 on page 287 shows the functions within the 2210 and 2216 that allow this to happen. As the figure shows, LAN emulation is a layer 2 service: it is completely independent of any layer 3 or upper-layer protocols. This means that it can be used with both routable protocols such as TCP/IP, IPX, and APPN and non-routable protocols such as NetBIOS. The LAN emulation client in the 2210/16 allows the router to participate in an ATM network and route/bridge any layer 3 protocols just as it does on any other interface.

Another point that this figure makes is the fact that LAN emulation is completely transparent to the underlying ATM cell relay network. The 8260/8285 is completely oblivious to the fact that it is transporting cells that comprise LAN emulation packets.

The figure also shows another important point about LAN emulation. On the ATM client device, LAN emulation allows the use of legacy protocol stacks and applications to run unmodified. The LAN emulation driver simply snaps in like an ordinary NDIS or ODI MAC driver. The protocols see the same API that they would for a real token-ring or Ethernet MAC driver (depending on the LAN being emulated).

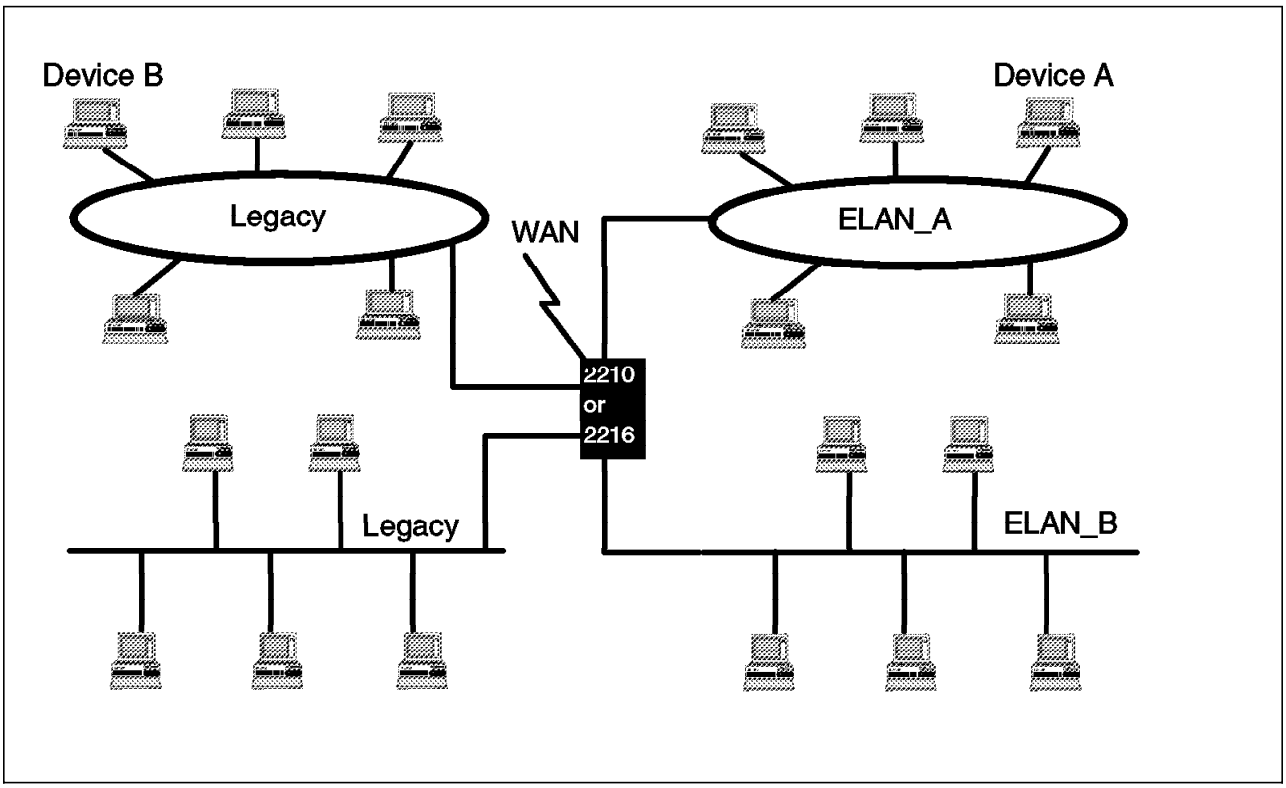


Figure 153. Routing between ELANs and Other Interfaces

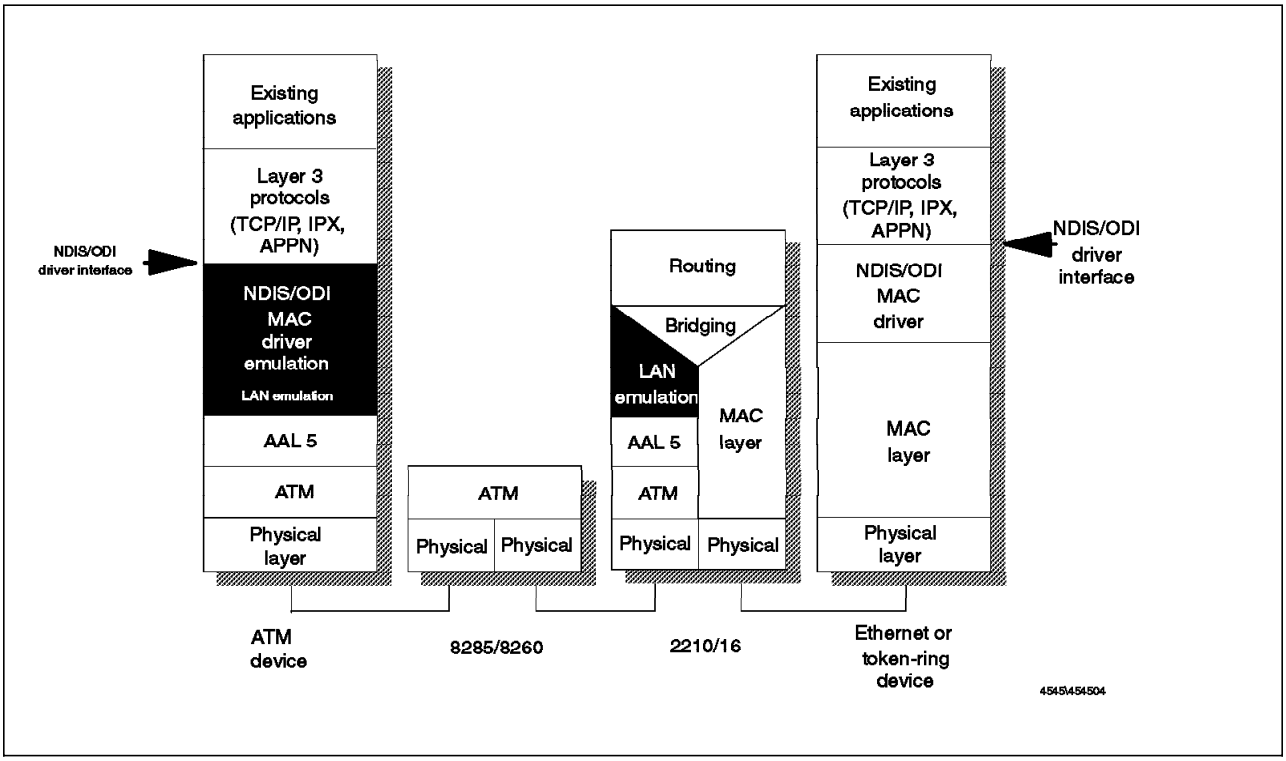


Figure 154. How the 2210 and 2216 Work in an Emulated LAN

The IBM 2210 Nways Multiprotocol Router and the IBM 2216 Nways Multiaccess Connector provide a fully compliant implementation of LAN Emulation 1.0, as specified by the ATM Forum.

The ATM adapters for the 2210/16 support multiple ELANS over the same interface. They can support up to 63 LECs per ATM interface.

11.2 LAN Emulation Benefits

Some of the benefits of LAN emulation are in the following areas:

- Migrating to ATM technology

  LAN emulation allows incremental upgrades to ATM. LAN segments can be upgraded one at a time while the remainder of the network can be left totally undisturbed.

- Enabling you to utilize high-speed ATM links

  When you start to migrate, you can first install ATM adapters in stations with high bandwidth requirements such as servers, engineering, and multimedia workstations. This way, these devices can begin to take advantage of the higher throughput links while providing the same connectivity as before.

- Lowering network management costs

  The network management benefits of emulated LANs (ELANs) come from increased flexibility in handling moves, additions and changes. Membership in an ELAN is not based on physical location; instead, logically related stations are grouped to form an ELAN. As long as ELAN memberships are retained, no reconfiguration is needed when stations move to new physical locations. Similarly, no wiring modifications are needed to move stations from one ELAN to another.

- Protecting your hardware and software investments

  Hardware investments are protected with the use of forwarding engines such as the 2210 and 2216 that bridge LAN and ATM networks so that existing adapters and wiring can continue to be used.

  Software investments are protected because application interfaces are unchanged. (Remember LAN emulation is implemented at the MAC layer, which allows existing protocol stacks to continue to be used.)

11.3 LAN Emulation Components

The components of an emulated LAN are:

- One LAN emulation server (LES)
- One LAN emulation configuration server (LECS)
- One broadcast and unknown server (BUS)
- LAN emulation clients (LECs), such as user workstations, bridges, routers, etc.

These components are shown in Figure 155 on page 289 as they relate to one another on an ELAN.

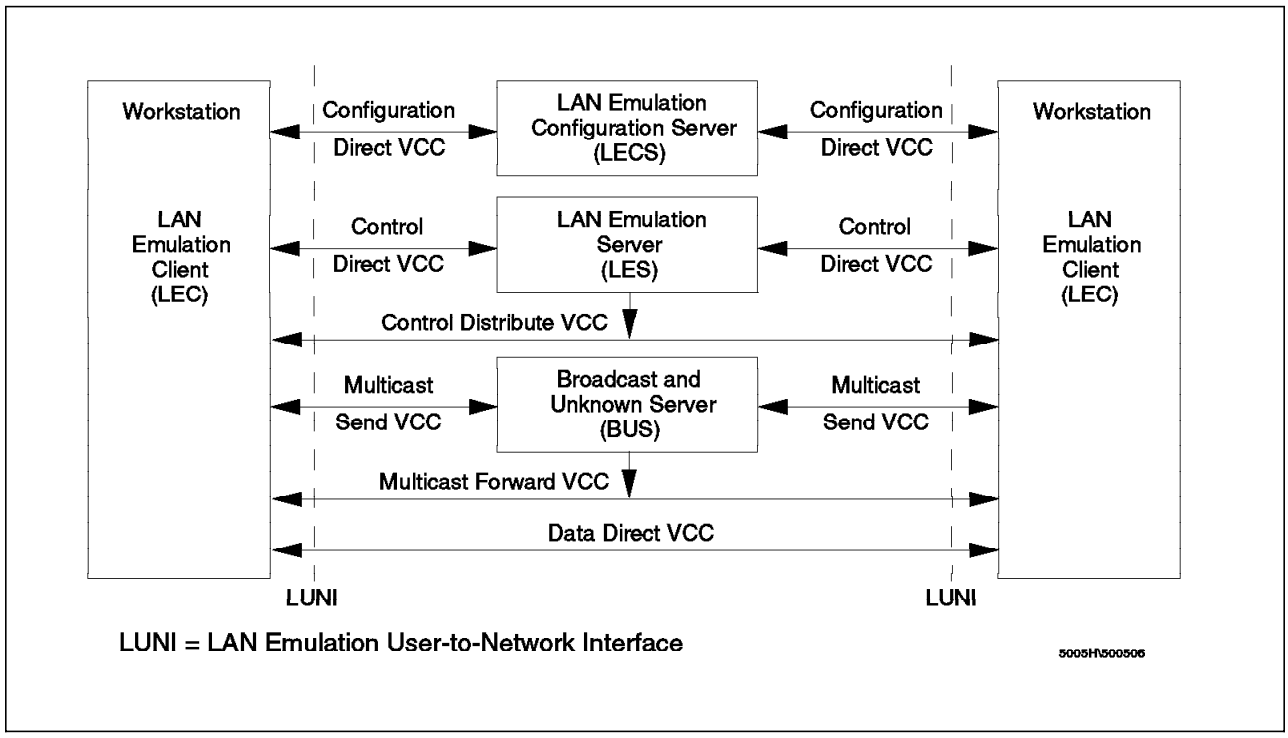


Figure 155. LAN Emulation Components

The LES, BUS and LECS are collectively referred to as the LE service components.

End users utilize their LE client component(s) to request services through the LAN emulation User-to-Network Interface (LUNI).

Logically, each LE service component has a distinct function. However, physically the services may be implemented in the same physical machine.

They may be part of the ATM network in switches such as the 8260 and 8285 or in one or several ATM end systems, such as the IBM Nways MSS Server. The MSS server is capable of providing all of these services simultaneously for multiple ELANs.

Figure 155 also shows that LANE uses a variety of VCC types. These VCCs are dynamically established by the different components when needed. You as an administrator usually are not aware of these different connections, but you should know about them, as they are often referenced in the documentation.

Some of these VCCs are used for configuration and control and others are used for data transfer. The configuration direct and control direct are bidirectional connections (use pairs of VCCs). The Control Distribute VCC is unidirectional and may either be point-to-point or point-to-multipoint if supported by the ATM implementation of the products.

The Data Direct VCC is the method in which two end systems communicate after a circuit has been established. This is the type that the end systems use to do productive work.

The Multicast Send VCC is used to establish a bidirectional, point-to-point connection to the BUS. This connection is used when the LEC needs to send

broadcast and multicast data frames. The BUS may use this connection also to send data to LECs. It is also used by the client to send unicast frames until the Data Direct VCC has been established between two clients.

The unidirectional multicast forward VCC is used by the BUS to forward multicast frames to the clients on the ELAN when it receives a multicast from another LEC.

11.3.1 LAN Emulation Server (LES)

The basic function of the LE server is to provide directory and address resolution services to the LECs of the emulated LAN. Each emulated LAN must have an LE server. An LE client registers the LAN address(es) it represents with the LE server. When an LE client wants to establish a direct connection with a destination LEC, it gets the destination′s MAC address from the higher-layer protocols and has to ask the LE server for the ATM address of the destination.

The client uses the LAN Emulation Address Resolution Protocol (LE_ARP to communicate with the LES. LE_ARP is similar in principle to TCP/IP ARP. With TCP/IP ARP, you translate an IP address into a MAC address. With LE_ARP, you translate a MAC address into an ATM address.

The LE server will either respond directly (if the destination client has registered that address), or forward the request to other clients to find the destination.

An emulated token-ring LAN can′t have members that are emulating an Ethernet LAN (and vice versa). Thus, an instance of an LE server is dedicated to a single type of LAN emulation.

The LE server may be physically internal to the ATM network (as in the switch itself) or it can be provided in an external device. Logically it is always an external function that simply uses the services provided by ATM to do its job.

In the IBM product space as of the time of publication of this redbook, the IBM 8260, 8285, and the MSS server implement ATM Forum-compliant LAN Emulation Servers.

The MSS server has also implemented an extension to the LES, called intelligent LES (ILES). ILES offers the option to use two separate Control Distribute VCCs, one to the proxy LE clients (that is, the LAN-ELAN interconnect devices), and one to the non-proxy LE clients. ILES reduces broadcast traffic from the LES by sending the LE_ARP requests only on the proxy Control Distribute VCC.

The MSS server is also capable of implementing redundant LES/BUS services and a robust LAN emulation security feature.

11.3.2 LE Configuration Server (LECS)

The job of the LECS is to assign individual LE clients to the proper emulated LAN on the ATM network. It does this by providing the ATM address of the LE server for the ELAN to which the client should be connected. This occurs during initialization of the client.

Note: An LE client is not required to request this information from the LECS; an LE server′s ATM address may be configured (system-defined) in the LE client.

Using a LECS to assign clients to the different ELANs allows for central configuration and administration of multiple ELANs in an ATM network. LECS

assigns the client to an ELAN based on an ELAN policy. The policy may be as simple as a table lookup based on the ATM or MAC address, or it may include such factors as the ELAN type or the maximum frame size supported.

In the IBM product space as of the time of publication of this redbook, the IBM MSS server is the only product that implements an ATM Forum-compliant LAN Emulation Configuration Server.

11.3.3 Broadcast and Unknown Server (BUS)

The BUS has two main functions:

1. Distribute multicast and broadcast frames to all LECs in the ELAN

   Since there is no way for a LAN emulation client to broadcast as a legacy LAN client would do, it uses the BUS to forward such traffic to the other LE clients over point-to-multipoint connections that the BUS has with the other clients on the ELAN.

2. Forward unicast frames to the appropriate destination

   A LEC sends unicast frames to the BUS if it does not have a direct connection to the LEC representing the destination. To avoid creating a bottleneck at the BUS, the rate at which a LEC can send unicast frames to the BUS is limited.

IBM products that implement the ATM Forum LAN Emulation Broadcast and Unknown Server function are the 8260, 8285, and the MSS server.

In the IBM MSS Server implementation, the BUS has two modes of operation. The mode is determined by configuring the number of Multicast Forward VCCs. The BUS operation is very simple when a single Multicast Forward VCC is used. All received frames are simply forwarded to all LECs. If two Multicast Forward VCCs are used, the BUS will not broadcast unicast frames to all LECs. Instead, unicast frames destined for non-proxy LECs will be transmitted directly to the destination LEC on a Multicast Send VCC. All other unicast frames will only be transmitted to proxy LECs (using the proxy Multicast Forward VCC).

One advantage of this Intelligent BUS (IBUS) mode is a reduction in client disturbance due to nuisance unicast frames (that is, unicast frames not destined for the client). Proxy clients do not receive unicast frames destined for non-proxy clients and non-proxy clients never receive nuisance unicast frames. Another advantage is the reduction in network bandwidth devoted to nuisance frames. Disadvantages include increased BUS processing requirements and the fact that multicast frames must be transmitted twice (once on each Multicast Forward VCC). However, this option should be disabled in configurations with source-route bridges that join the ELAN as non-proxies.

The MSS server also implements what is known as the Broadcast Control Manager (BCM). BCM is a value-added feature that helps control the broadcast traffic in a network. BCM reduces the level of broadcasts in a network in the following ways:

- Dynamically learns endstation information (for example, IP addresses, IPX server and router addresses, NetBIOS names, and their associated information)
- Converts broadcast frames to unicast frames when endstations are known

- Sends unicast frames only to the interested LECs and legacy LAN endstations

BCM learns its information from its associated BUS and can be enabled and/or disabled for individual ELANs and individual protocols. Protocols supported by BCM are IP, IPX and NetBIOS.

11.3.4 LAN Emulation Client (LEC)

Each workstation connected to the ELAN has to implement the LE layer (also called LE entity), which performs data forwarding and control functions, such as address resolution, establishment of the various VCCs, etc. The LE layer functions could be implemented completely in software, in hardware on a specialized LAN emulation ATM adapter, or in a combination of both. The layered structure of the LEC is shown in Figure 156.

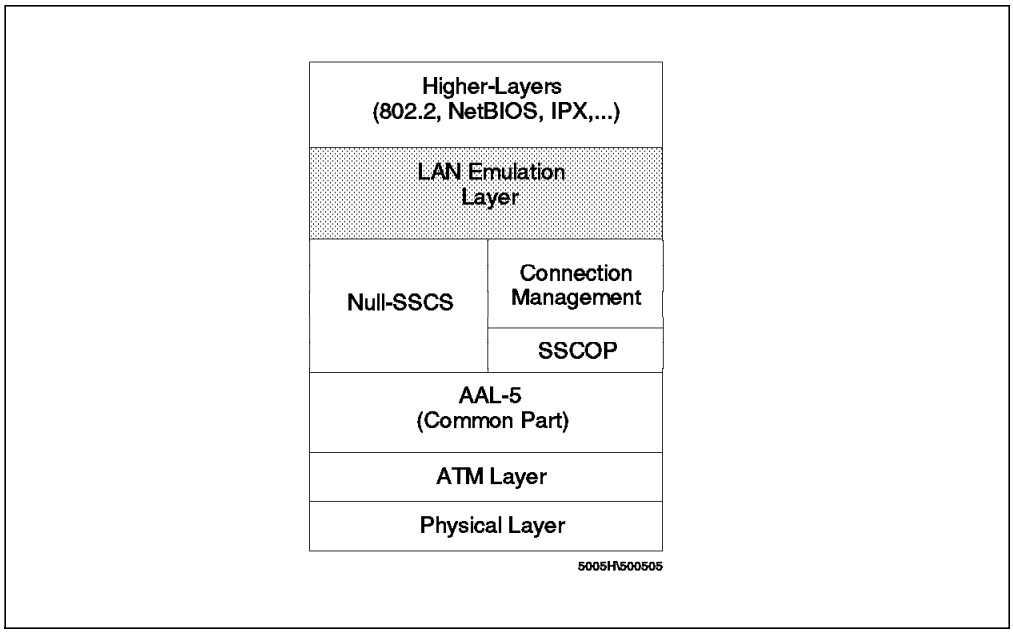


Figure 156. LAN Emulation Client Functional Layers

The LE layer provides the interface to existing higher-layer protocol support (such as IPX, IEEE 802.2 LLC, NetBIOS, etc.) and emulates the MAC-level interface of a real shared-media LAN (802.3/Ethernet or token-ring). This means that no changes are needed to existing LAN application software to use ATM services. The LE layer implements the LUNI interface when communicating with other entities in the emulated LAN.

The primary function of the LE layer is to transfer LAN frames (arriving from higher layers) to their destination, either directly or through the BUS.

A separate instance of the LE layer is needed in each workstation for each different LAN or type of LAN to be supported. For example, if both token-ring and Ethernet LAN types are to be emulated within a single station, then you need two LE layers. In fact, they will probably just be different threads within the same copy of the same code, but they are logically separate LE layers.

Separate LE layers would also be used if one workstation needed to be part of two different emulated LANs, both emulating the same LAN type (for example, token-ring). Each separate LE layer needs to have a different MAC address and

must be attached to its own LE server, but it can share the same physical ATM connection (adapter).

11.4 ATM Addresses of LAN Emulation Components

In general, ATM addresses must be unique among LAN emulation components. The only exception is that a LES and BUS serving the same ELAN may share an ATM address.

LAN emulation components are configured for a particular ATM interface, and the user may decide to use the burned-in MAC address as the ESI portion of the component′s ATM address, or select one of the locally administered ESIs defined for the ATM interface. Multiple LE components may share the same ESI if they have unique selectors. By default, the configuration interface assigns each LE component a unique selector value for the configured ESI; however, the user may override this assignment and explicitly configure a particular selector value.

An ATM interface parameter determines the number of selectors per ESI reserved for explicit assignment. (The remainder are available for dynamic assignment by the ATM interface at run time.) LE components only use the selectors reserved for explicit assignment; by default, 200 of the 256 possible selectors per ESI are reserved for explicit assignment. Run-time selector assignment is beneficial when the user does not need to control the assigned selector. (Classical IP clients are an example.)

While ATM addresses must be unique among LE components, LE components may use the same ATM addresses as non-LE components such as Classical IP clients/servers.

11.5 ATM Connection Procedure

A LAN emulation client must go through a series of steps in order to successfully connect to an ELAN. These steps are:

1. Connect to the LECS
2. Connect to the LES
3. Address Registration
4. Address Resolution
5. Connect to the BUS
6. Establish Data Direct VCCs

This section explains this process as well as provides an overview of the Interim Local Management Interface (ILMI) used in the process. For more detailed explanations, please see *Understanding and Using the IBM MSS Server,* SG24-4915-00.

11.5.1 Overview of ILMI Functions

The Interim Local Management Interface (ILMI) defines a set of SNMP-based procedures used to manage the User-to-Network Interface (UNI) between an ATM end system and an ATM switch. The following three ILMI functions are particularly relevant to LAN emulation:

1. ATM address registration
2. Dynamic determination of UNI version being run on the switch
3. Acquisition of the LECS ATM address(es)

By default, the ATM interfaces of the IBM 2210 and the IBM 2216 use UNI 3.0. If both ends have defined different UNI versions, connection establishment fails. In addition to explicit definition, either or both ends can specify auto-detection of the other end′s UNI version as well. If both ends have auto-detection selected the latest UNI version supported will be selected. In the case of the 2210 and 2216 this is UNI Version 3.1.

ILMI is also the method of choice for locating the LECS. The ILMI MIB at the ATM switch includes a list of LECS ATM addresses that may be retrieved by the LECs. This is useful because the LECS ATM address(es) has to be configured at the ATM switches only, not at LECs, and there are fewer switches than LECs.

11.5.2 Connecting to the LECS

LECs are not required to use the LECS, although it is recommended. If you don′t use the LECS, each LEC must be configured with the ATM address of the LES serving its ELAN. The LECS reduces the network management burden by serving as a centralized repository for configuration data, minimizing configuration at the LECs.

LECs connect to the LECS using well-defined procedures. The following steps are attempted, in order, until a VCC to the LECS is established.

1. Connect to the LECS using a configured ATM address. (Configuration of a LECS ATM address at LECs is optional, and not recommended.)
2. Obtain a list of LECS addresses using ILMI and attempt to connect to each LECS on the list until a VCC is established.
3. Establish a VCC to the well-known LECS ATM address defined by the ATM Forum.

As previously stated, ILMI is the preferred method for a LEC to locate the LECS. The well-known LECS address is needed because some switches do not support the ILMI method. Configuring the LECS addresses at LECs is a last resort for situations where the switch does not support the ILMI method and the LE Service does not support the well-known LECS address. The IBM 2216, IBM 2210 and IBM 8260 switch support all three methods.

The function of the LECS is to provide initial configuration data to the LECs, with the most crucial piece of data being the ATM address of the LES. In order to provide this information to a LEC, the LECS must be able to identify the LEC and determine the proper LES for that LEC. The LECS identifies a LEC using information in the LE_CONFIGURATION_REQUEST frame sent by the LEC. The configuration request may also contain information to identify the ELAN desired by the LEC. The following information may be included in the configuration request:

1. Primary ATM address of the LEC

   This field is required and uniquely identifies the LEC.

2. LAN Destination associated with the LEC

   This field may contain a MAC address or a route descriptor that uniquely identifies the LEC, or it may be unspecified.

3. ELAN Name

   This field may contain a name identifying the requested ELAN or the requesting LEC. The ELAN name may be unspecified in the request.

4. ELAN Type

   This field may specify that an Ethernet or token-ring ELAN is desired, or may be unspecified. If the LEC specifies the type of ELAN desired, the LECS cannot assign the LEC to an ELAN of a different type.

5. Maximum frame size supported by the LEC

   This field may specify the upper bound on the size of a data frame that can be processed by the LEC, or it may be unspecified. The LECS cannot assign a LEC to an ELAN with a maximum frame size larger than that specified by the LEC (since the LEC may not be able to process some of the frames on the ELAN).

Given this information, the LECS returns an ATM address for the appropriate LAN emulation server (LES). This is accomplished through the use of policies and policy values. A policy is a criteria that the LECS uses to make LEC-to-LES assignment decisions. A policy value is a (value, LES) pair indicating that the specified value should be assigned to the specified LES. An example of a policy is the LEC′s MAC address. An example of a policy value is (MAC_ADDR_A, LES_1). Using this policy the LECS would direct a LEC to LES_1 when the LAN Destination field of the configuration request contains MAC_ADDR_A. In accordance with the ATM Forum′s LE Service MIB Specification, six policies are defined:

1. ATM address
2. MAC address
3. Route descriptor
4. ELAN type
5. Max frame size
6. ELAN name

Policies also have priorities. The LECS examines policies in prioritized order. Policies with smaller values in the priority field are considered before policies with larger values in the priority field. Policies with equal values are considered at the same time and must both be in agreement for the LES to be assigned. The LECS assigns a LEC to a LES when all of the policies at the current priority level are in agreement. If these conditions are not met, the LECS considers the policies at the next priority level. If the LECS is unable to find a LES at any priority level, an unsuccessful configuration response is returned to the LEC.

After determining the proper LES for a LEC, the LECS returns a configuration response to the LEC that includes the following:

- LES ATM address

- ELAN type
- Max frame size
- ELAN name

The configuration response may also include Type/Length/Value (TLV) parameters. TLVs provide a method to download optional or user-defined parameters to the LEC.

11.5.3 Connecting to the LES

After obtaining the ATM address of the LES, the LEC initiates a Control Direct VCC to the LES. When this VCC has been established, the LEC sends an LE_JOIN_REQUEST to the LES. The LES responds by adding the LEC to the appropriate point-to-multipoint Control Distribute VCC and returning an LE_JOIN_RESPONSE.

If you have the IBM MSS Server as your LES, then by default it will partition proxy and non-proxy LECs onto separate Control Distribute VCCs. However, the user can configure the LES to use a single Control Distribute VCC for all LECs in order to reduce the number of point-to-multipoint VCCs that are required. Partitioning the VCCs is generally useful as it reduces the amount of traffic that is sent to non-proxy clients. (For example, no LE_ARP_REQUESTs are sent to non-proxy LECs as described in 11.5.5, “Address Resolution.”)

11.5.4 Address Registration

LECs register LAN destinations with the LES to ensure uniqueness and allow the LES to answer LE_ARP_REQUESTs (which LECs issue to learn the ATM address associated with a particular LAN destination). Registrations include the LAN destination and the ATM address that the LEC associates with the LAN destination. A LAN destination may be either a MAC address or a route descriptor.

Proxy LECs do not register the MAC addresses of stations on LAN segments that they are bridging to the ELAN, while non-proxy LECs must register all the LAN destinations that they represent. All route descriptors must be registered, regardless of whether or not they are associated with a proxy or non-proxy LEC. Route descriptors are only applicable to proxy LECs that are performing source-route bridging. A route descriptor contains the bridge number of the proxy LEC and the segment number of a ring (one hop from the ELAN) that the LEC is bridging to.

11.5.5 Address Resolution

LAN communications are based on source and destination MAC addresses. To enable communications on an ATM network, MAC addresses must be resolved to ATM addresses. A LEC sends an LE_ARP_REQUEST to the LES to learn the ATM address of a particular LAN destination. If the LAN destination is registered, the LES responds with the ATM address associated with the LAN destination. Otherwise, the request is forwarded to all proxy LECs on the Control Distribute VCC. There is no need to forward the request to non-proxy LECs, since all of their LAN destinations are registered. If the LES, however, is configured to use a single Control Distribute VCC, all of the LECs will receive the request. Control Distribute VCCs provide an efficient way for the LES to distribute control frames to multiple LECs.

Proxy LECs respond to LE_ARP_REQUESTs for unregistered MAC addresses that they represent. The LE_ARP_RESPONSE is sent to the LES on the Control Direct VCC and the LES forwards the response to the LEC that issued the request.

11.5.6 Connecting to the BUS

After connecting to the LES, the LEC issues an LE_ARP_REQUEST for the all 1′s broadcast MAC address. The LES responds with the ATM address of the BUS. The LEC then initiates establishment of a Multicast Send VCC to the BUS. The BUS responds by adding the LEC to the appropriate point-to-multipoint Multicast Forward VCC.

The IBM MSS Server has an added function, known as the intelligent BUS (IBUS), as mentioned in 11.3.3, “Broadcast and Unknown Server (BUS)” on page 291. The IBUS by default partitions proxy and non-proxy clients onto separate Multicast Forward VCCs, as illustrated in Figure 157. As was the case with the Control Distribute VCC, however, the user can configure the BUS to use a single Multicast Forward VCC for all LECs.

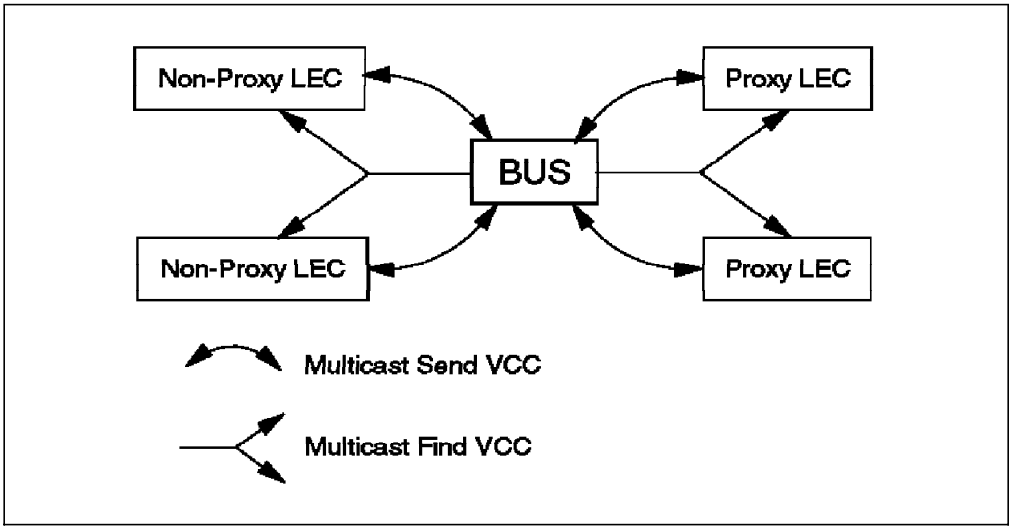


Figure 157. Default Connections between LECs and the BUS

11.5.7 Establishing Data Direct VCCs

Data Direct VCCs connect two LECs and are used to exchange unicast frames without involving the BUS. The LEC uses the address resolution procedures to determine the ATM address associated with the desired LAN destination. If the LEC already has a Data Direct VCC to the ATM address (perhaps for another LAN destination represented by the target LEC), unicast data frames are subsequently transmitted on the existing VCC. Otherwise the LEC invokes the signaling protocol to establish a new VCC.

The LEC maintains an LE_ARP cache containing LAN destination to ATM address mappings. Entries in this cache are aged and must be periodically refreshed. Utilization of Data Direct VCCs is also monitored and the VCCs are released if there is no traffic for the VCC time-out period (which is configurable). Additionally, Data Direct VCCs are released in a least recently used manner when establishment of a new Data Direct VCC fails due to insufficient resource availability.

11.5.8 Example of a 2210 or 2216 Routing from Legacy

This section uses an example to illustrate the methods that the 2210 and 2216 use in connecting a workstation on a legacy LAN to a workstation across ATM. It helps in understanding how VCCs are set up using LAN emulation and how the 2210 and 2216 provide connection for downstream devices.

Figure 158 depicts our example in which PC 1 needs to communicate to PC 2. For this example, let's assume the protocol is SNA over 802.2 Logical Link Control (LLC) which is non-routable and must be bridged.

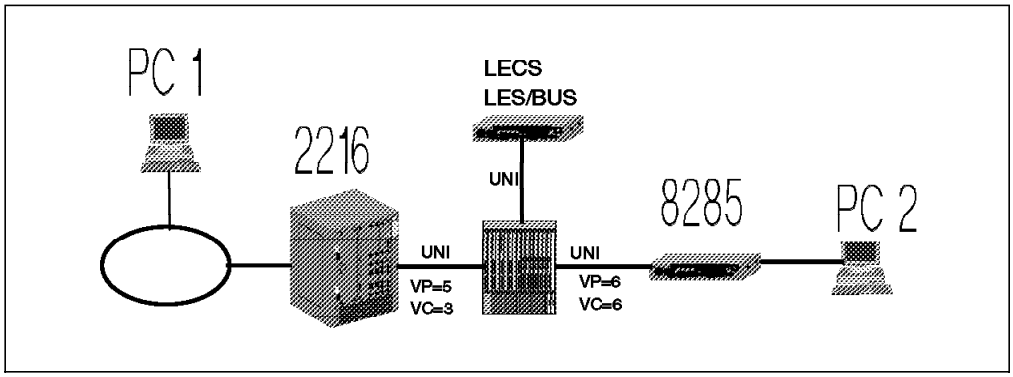


Figure 158. Example Network

11.5.8.1 Device Initialization and Registration

The first step that the 2210 or 2216 must execute before it can be used to send traffic across a Forum Compliant LAN Emulation ATM network is to receive the parameters for the User to Network Interface (UNI) and register with the switch. This is done using the Interim Local Management Interface (ILMI) function. (See 11.5.1, "Overview of ILMI Functions" on page 294.)

The next step is for the LE client in the router to register with the LAN emulation configuration server (LECS) assuming as in our example that a LECS is being used. During this process, the LEC receives back the ATM address of the LES that it is assigned to. (See 11.5.2, "Connecting to the LECS" on page 294.)

The 2210 or 2216 then registers with the LES and sets up a connection with the BUS and is then ready to send or receive data over the ATM network. (See 11.5.4, "Address Registration" on page 296.)

11.5.8.2 Resolving the Address of PC 2

The 2210 and 2216 act as a proxy LEC for all of the stations connected via the other router interfaces. That is, if a device connected via another interface needs to communicate with an ATM-attached device, the router will use its ATM address to represent the downstream station. All ATM cell relay traffic is between the LE client in the router and the other LE client in the ATM-attached device. (See Figure 154 on page 287.)

PC 1 knows the MAC address of PC 2. (In this case, it has been configured into the client code.) If PC 1 does not already have a link with PC 2, then it will have to use token-ring source route broadcasting to find PC 2. If it already has a link with PC 2, then it will already have the route indicators to use to find PC 2. In both cases, the token-ring interface on the 2216 will copy the frame and bridge it to the ATM interface.

If the LEC client in the router recognizes the destination MAC address and has the corresponding ATM address cached, it will initiate a VCC to that ATM address using the UNI call setup signaling procedures described in 10.2.1, “Call Setup Example” on page 282.

If the LE client does not recognize the destination MAC address, it must send it to the LES in the form of an LE_ARP_REQUEST so that the address can be resolved to an ATM address. The LES checks to see if the MAC address is in its table and if so it sends back the corresponding ATM address.

Note: If the MAC address isn′t present (for example, the device is on a token-ring connected downstream from another router ATM interface) then the LES will broadcast the address to all of its known proxy LECs and wait for a response. The appropriate proxy responds to the LES with the ATM address of its associated LE client. The LES then forwards this ATM address to the LE client in the 2216.

11.5.8.3 Setting Up the SVC

Once the destination ATM address of PC 2 (or its proxy) is known, the 2216 is able to set up a Data Direct VCC to it using the same call setup procedures.

As part of these call setup procedures, the switch adjacent to the 2216 sets up a Virtual Connection Link (VCL) to the 2216 and gives it a VP and VC number to use for this VCC. The switch adjacent to PC 2 will set up a VCL with PC 2 using different (most likely) VP and VC numbers.

All traffic between the two LE clients *on that VCC* will then be subsequently switched via the method described in 10.1.3, “Cell Switching” on page 279.

11.5.8.4 Normal Traffic Flow

At this point, we have an 802.2 logical link between PC 1 and PC 2 that is carried over the legacy LAN segment and the SVC between the 2216 and PC 2. When PC 1 has something to send over this link, it will begin to send 802.2 frames over the token-ring with a route indicator that the 2216 token-ring adapter recognizes. It copies the frames and bridges them to the LE client that belongs to the same ELAN as PC 1. The LE client then passes the frames to the ATM adaptation layer 5 (AAL-5) component within the 2216.

AAL-5 is responsible for segmenting the frames into 48-byte data units so that they can be transported via ATM cells through the network. This is referred to as the Segmentation and Reassembly (SAR) function within the adaptation layer. (See *Asynchronous Transfer Mode Technical Overview*, SG24-4625-00 for more information.)

The cells are then sent out over the ATM interface and switched through the network to PC 2.

Note: If the 2210 or 2216 is routing/bridging between two emulated LANs (ELANS), the cells must go through the SAR function twice. First, as they are received they are reassembled into frames. Then, they get passed to the router/bridge to find the next hop. Finally, they must go back through the SAR process to get segmented back into frames before they can go back out onto the ATM connection.

The MSS server has a feature called short-cut bridging, which allows a Data Direct VCC between two LECs on different ELANs. This feature, however, is not currently implemented the 2216 and 2210.

11.6 Key Configuration Parameters for LAN Emulation

This section gives a brief description of the main parameters that need to be configured for LAN emulation. The prerequisites for these tasks are:

Notes:

1. The ATM interface(s) must be configured before the LE components can be created.
2. The LES/BUS for the ELAN that the LE client will join must be operational before the LE client in the router can become active. For more information on configuring a LES/BUS or a LECS see the *Understanding and Using the IBM MSS Server*, SG24-4915-00.

11.6.1 Configuring a LAN Emulation Client (LEC)

To create a LEC, the user needs to specify, at a minimum, the ELAN type of token-ring or Ethernet. Additionally, other parameters may be required.

For example, since two LECs cannot have the same MAC address, if two LECs are defined on a single ATM interface and are bridged together, then one of the LECs must use something other than the default burned-in MAC address.

The default Max Frame Size is another parameter that you might need to change. It defaults to 1516 bytes for Ethernet LECs and 4544 bytes for token-ring LECs. This parameter is important because LECs will not be allowed to join the ELAN if their maximum frame size is less than the maximum frame size of the ELAN. LECs that have a larger maximum frame size will be allowed to join the ELAN, but will use the maximum frame size of the ELAN as a result of join-time negotiation with the LES.

The size of a LECs LE_ARP cache can be an important performance tuning parameter since it controls the maximum number of Data Direct VCCs that can be established. A cache that is too small can lead to VCC thrashing (that is, constantly tearing down one VCC to set up another one), while a cache that is too large wastes memory. Naturally, the optimal size varies considerably depending on the ELAN′s size and traffic patterns. Ideally, there should be sufficient Data Direct VCCs to support the number of stations that will be simultaneously contacted through the IBM 2216 or IBM 2210 to that particular ELAN. The default LE_ARP cache size is 10 entries.

11.7 Configuring LAN Emulation on the 2210 and 2216

This section covers the basic steps required to configure LAN emulation functions on the 2210 and 2216 using the Configuration Program.

Note: Detailed scenarios using the command line interface are included later in Chapter 14, “ATM Scenarios” on page 343.

The different configuration steps to be completed depend on the functions that need to be activated. The basic steps include:

1 Add the adapter to the slot that it is installed in.

This is done by selecting **Slots** in the configuration program.

Note: This only has to be done for the 2216. The 2210's interfaces don't need to be added, as their values can't be changed.

2 Define the ATM Interface(s).

LE clients are components of the 2210 and 2216 that need to be associated with an ATM interface. When associated, all ATM traffic of the component will take place on the ATM interface specified.

During configuration of the ATM interface, you have to configure:

a. The ATM interface attributes

When configuring an ATM interface on the IBM 2210 or IBM 2216, the following parameters should be carefully considered:

max-data-rate
The *max-data-rate* value defines the speed of the physical ATM interface.

Note: In the configuration program this parameter is referred to as *maximum VCC data rate*.

ATM Maximum Frame Size
The *ATM Maximum Frame Size* parameter defines the maximum AAL-5 CPCS PDU payload size. Any of the frames received by, or sent from, the 2210 or 2216 must not exceed this value. Make sure that the maximum frame sizes defined on your ELANs and LISs do not exceed this value. The default value is 9234.

Maximum Calls
The *Maximum Calls* parameter defines an upper boundary to the number of simultaneously active, point-to-point (PtP) and point-to-multipoint (PtMP), VCCs on the 2210 or 2216. This parameter includes the VCCs established by the 2210 or 2216 and the VCCs started by remote clients. The default value is 1024.

Maximum Protocol Users
The *Maximum Protocol Users* parameter sets an upper boundary to the number of LE clients, IPX (RFC 1483) clients, LIS clients, and ARP servers that can be simultaneously active on the 2210 or 2216. The default value is 209.

Selectors per ESI Reserved for Explicit Configuration
The *Selectors per ESI Reserved for Explicit Configuration* specifies the maximum number of selectors bytes (SELs) that can be specified per end system identifier (ESI). This number includes the manually assigned ESIs, and the ESIs generated by the configurator. The default value is 200.

Note: The remaining ESI numbers (out of a total of 256 per ESI) are used by the 2210 or 2216 to assign ESIs at run-time.

Maximum Parties on Outbound PtMP Call
The *Maximum Parties on Outbound PtMP Call* defines the maximum number of leaves (or parties) that any of the 2210 or

2216 components, accept on their point-to-multipoint connections. The default value is 512.

Trace

The *Trace* parameter, if on, allows tracing on specific VPI/VCI ranges. By default, tracing is disabled.

Signalling Protocol

The *Signalling Protocol* parameter specifies the UNI version that the 2210 or 2216 uses on its ATM connection. This value can be 3.0, 3.1 or AUTO. AUTO will let the 2210 or 2216 discover if the adjacent switch supports UNI 3.0 or 3.1 and configures it accordingly. The same values have to be defined on both sides of the ATM link. If UNI=AUTO has been configured at both ends, the latest UNI version supported (that is, UNI Version 3.1 for the 2210 or 2216 and 8285/8260) will be selected. By default UNI Version 3.0 is used.

b. The end system identifiers (ESIs) associated with the ATM interface.

During the definition of any of your LE client components, either the burned-in end system identifier (ESI) or a user-defined ESI must be used. To simplify troubleshooting, we recommend that you use a locally administered ESI. ESIs are administered per ATM interface. A separate value has to be defined per ATM interface. All LE clients that connect using a particular interface can use the same ESI. Make sure that when defining multiple 2210s or 2216s, the user-defined ESIs are unique.

The ATM interface configuration must be repeated for each ATM interface on your 2216 that is used for LE functions. The 2210 only supports a maximum of one interface.

3 Configure LE clients.

Basic definition steps to define your LE clients include:

a. Define LE client addresses.

Associate the LE client with an ATM interface and specify its ESI, SEL, and MAC address.

b. Define the ELAN name and type.

Specify the ELAN name, type and maximum frame size.

c. Define the LE server (LECS or LES).

Identify how the LECS or LES ATM address is obtained (hard-coded or dynamically).

d. Define the higher-layer functions.

In addition to the basic LE client configuration, higher-layer (bridging or routing) functions need to be configured. For details on IP routing, IPX routing, and bridging, see 13.2.2, “IP Routing Protocols” on page 334, 13.2.3.1, “Routing IPX over RFC 1483 Connections” on page 335, and 13.3, “Bridging Overview” on page 341.

In addition to the basic LEC parameters that have already been mentioned, there are some extra parameters that may be configured. We suggest that the default values be used for these parameters but there may be a reason for specifying a value different from the default. Therefore a brief

description of each parameter and its valid values and default value are given in the following list:

Control Timeout
This is the timeout period used for timing out most request/response control frame interactions. The valid range is 10 to 300 seconds. The default value is 30 seconds.

Maximum Unknown Frame Count
Specifies the maximum number of frames for a given unicast MAC address or route descriptor that may be sent to the BUS within the specified time period. The valid values are 1 to 255, with a default value of 10.

Maximum Unknown Frame Time
The LEC may not send more frames to the BUS, for a given unicast LAN destination, than the Maximum Unknown Frame Count during this time period. The valid values are 1 to 60 seconds. The default value is 1 second.

VCC Timeout
If a Data Direct VCC has been idle this long it will be released. The valid range is 1 to an infinite number of seconds. The default value is 1200 seconds.

Maximum Retry Count
This sets the maximum number of times the LEC must retry an LE_ARP_REQUEST for a given LAN destination. The valid range is 0 to 2 and the default value is 1.

Aging Time
This is the maximum time that a LEC will maintain an entry in its LE_ARP cache in the absence of verification. The valid values are 10 to 300 seconds. The default is 300 seconds.

Forward Delay Time
This sets the maximum time that a LEC will maintain an entry for a non-local MAC address in its LE_ARP cache without verification of the LE_ARP relationship. The valid range is 4 to 30 seconds and the default is 15 seconds.

Expected LE_ARP Response Time
This sets the expected ARP response time. The valid values are 1 to 30 seconds with a default of 1 second.

Flush Timeout
The LEC will wait this amount of time to receive an LE_FLUSH_RESPONSE after sending an LE_FLUSH_REQUEST before taking recovery action. The valid values are 1 to 4 seconds with a default of 4 seconds.

Path Switching Delay
This is the time that the LEC has to wait, after sending something to the BUS, before it assumes that the frame has reached the destination. The LEC can then send frames directly to the destination on a different path. The valid values are 1 to 8 seconds with a default of 6 seconds.

Note: The Path Switching Delay may be used to bypass the flush protocol.

Multicast Send VCC Type

This specifies the type of VCC used for the Multicast Send VCC. The valid values are Best-Effort, Variable or Constant. The default is Best-Effort.

Multicast Send VCC Average Rate

This is used by the LEC for reserving bandwidth on the VCC to the BUS. It specifies the average rate to be used for both the forward and backward sustained cell rates. It is requested by the LEC when setting up the Multicast Send VCC when using reserved bandwidth connections (Variable or Constant VCC Type). Setting and default values depend on the parameters chosen for the Multicast Send VCC Type. The default values are:

- If the VCC Type is Best-Effort, the value defaults to the line speed of the ATM device.
- If the VCC Type is Reserved, there is no default and the Multicast Average Rate must be specified.

The valid values are 1 to 155,000 kbps.

Multicast Send VCC Peak Rate

This is used by the LEC for reserving bandwidth on the VCC to the BUS. It specifies the peak rate to be used for the forward and backward sustained cell rates. It is requested by the LEC when setting up the Multicast Send VCC when using reserved bandwidth connections (Variable or Constant VCC Type). Setting and default values depend on the parameters chosen for the Multicast Send VCC Type. The default values are:

- If the VCC Type is Best-Effort, the value defaults to the line speed of the ATM device.
- If the VCC Type is Reserved, there is no default and the Multicast Average Rate must be specified.

The valid values are 1 to 155,000 kbps.

Note: If you set the multicast average rate equal to the multicast peak rate then it is Constant. If you set the average less than the peak then it is Variable.

Connection Completion Time

This is the time interval in which data or a READY_IND message is expected from a calling party. Valid values are 1 to 10 seconds with a default of 4 seconds.

LEC ARP Cache Size

This sets the maximum number of entries in the ARP Cache. The valid range is 10 to 1024. The default is 10.

LEC ARP Queue Depth

This sets the maximum number of queued frames per ARP cache entry. The valid values are 0 to 10 with a default of 5.

Maximum Configuration Retries

This value specifies how many times the client will retry the configuration phase of joining an ELAN in the event of failure. The valid values are 0 to 5 with a default value of 3.

Best-Effort Peak Rate

This is used when establishing best-effort multicast send connections. Valid values are 1 kbps to the line speed of the ATM device. The default is the line speed.

These parameters can be used to fine tune your ATM network but unless there are performance problems it is recommended that the default values be used.

The previous steps must be repeated for every LE client. The configuration details are discussed in 11.7.2, “Configuring LE Clients” on page 308.

11.7.1 Configuring an ATM Interface

Figure 159 shows the Navigation Window of the 2216 configuration program. To configure ATM, start by selecting **Slots**. This allows you to add the adapters as they are physically installed in the 2216. The ATM adapter must be added in the configuration program before the interface parameters or LE-Clients can be configured.

Note: This step is not necessary for the 2210.

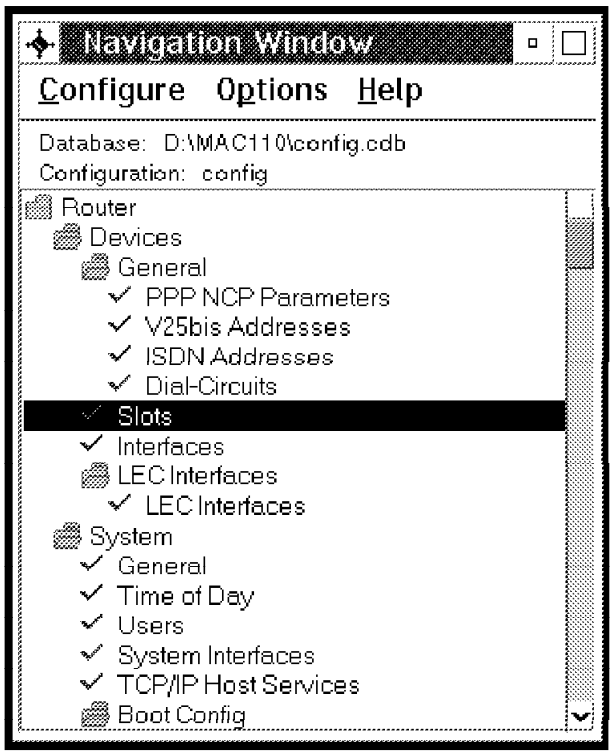


Figure 159. Navigation Window of the Configuration Program

Next, select **Interfaces** from the Navigation Window. This will allow you to configure any of the interfaces already added under the **Slots** section.

Select the interface that you want to configure and you will see a screen like the one in Figure 160 on page 306.

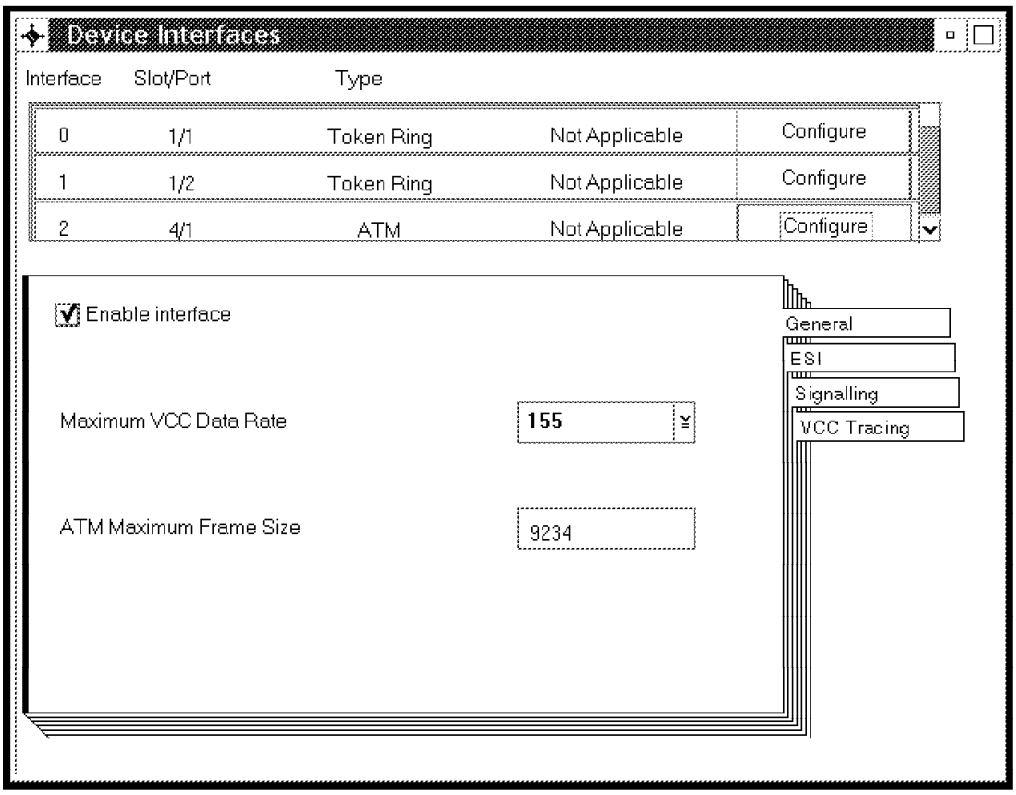
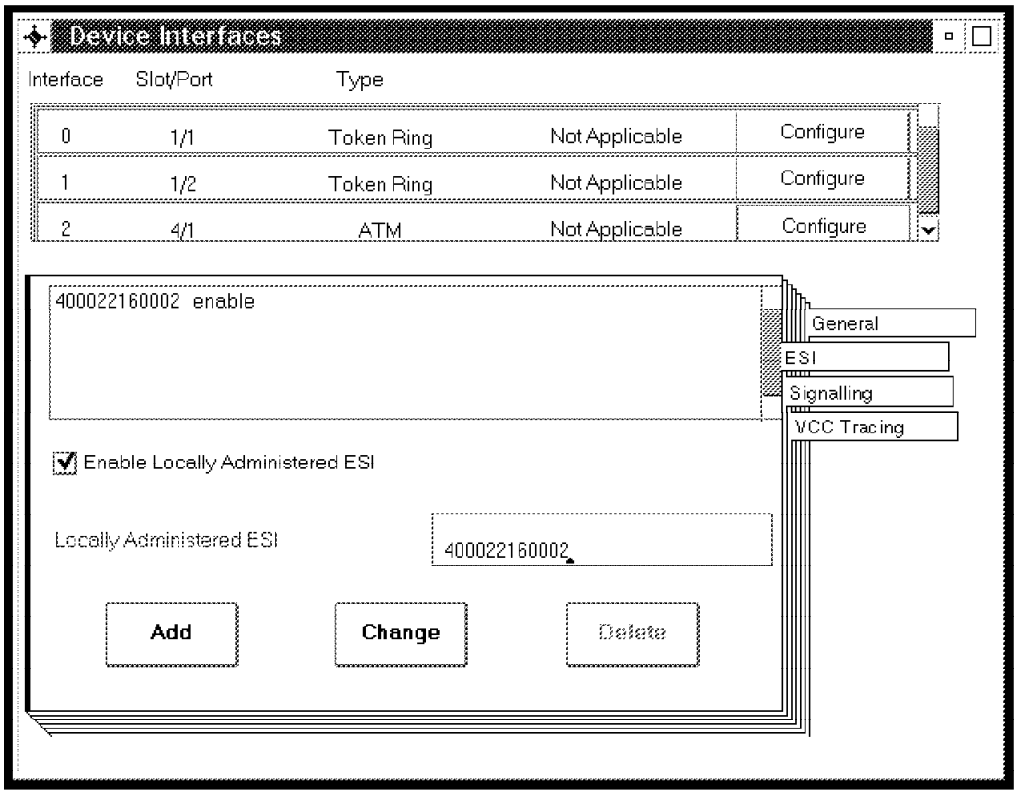


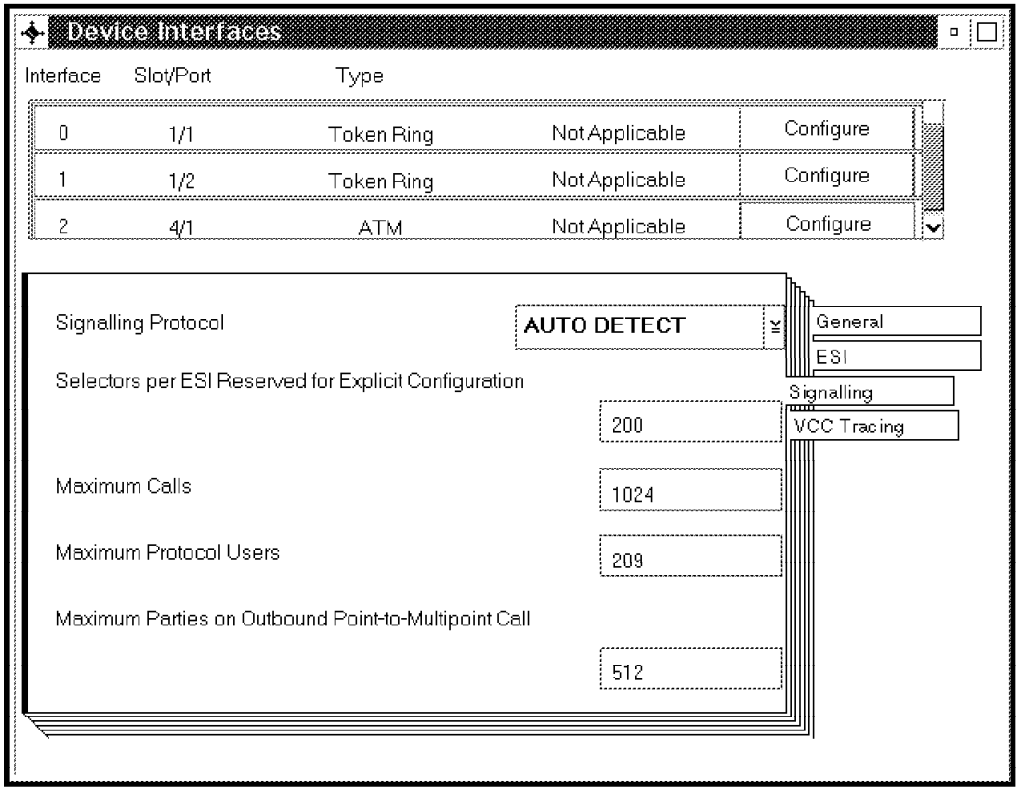
Figure 160. Configuring the ATM Interface

Figure 161 on page 307 reveals the three submenus available after clicking on **ESI**, **Signalling** and **VCC Tracing**, respectively. These parameters are described fully in 11.7, “Configuring LAN Emulation on the 2210 and 2216” on page 300.

ESI page:



Signalling page:



VCC Tracing page:

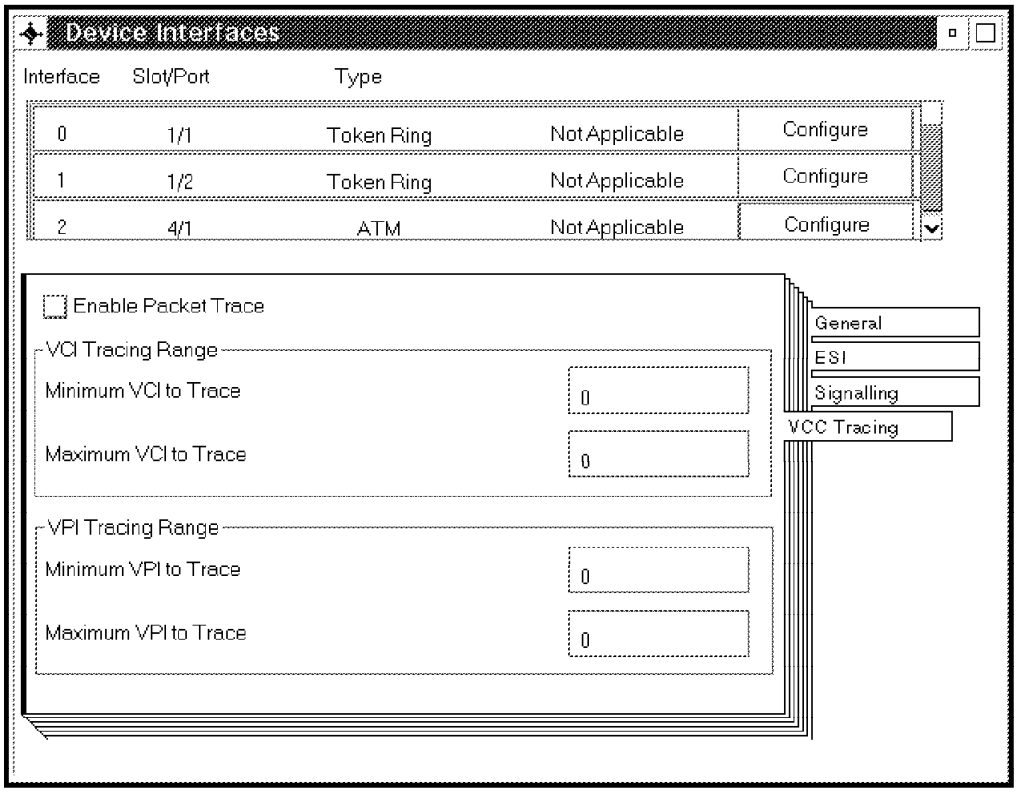


Figure 161 (Part 3 of 3). ATM Interface Configuration

11.7.2 Configuring LE Clients

To configure an LE client you need to first select **LEC Interfaces** in the Navigation Window, as shown in Figure 162 on page 309.

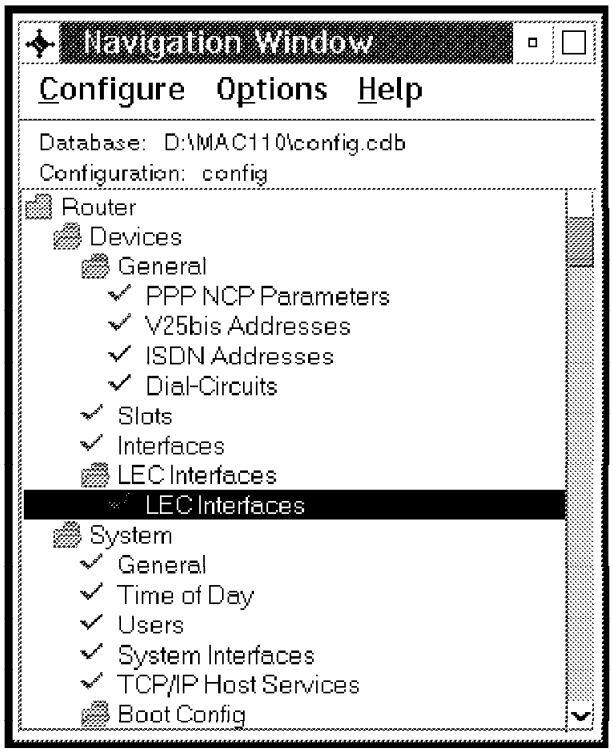


Figure 162. Define LEC Interfaces

The configuration steps discussed in this section need to be repeated for each LE client that you want to define.

To define an LE client, the following steps need to be performed:

1. Define LE client addresses.

   After selecting **LEC Interfaces** from the Navigation Window, Figure 163 on page 310 will appear.

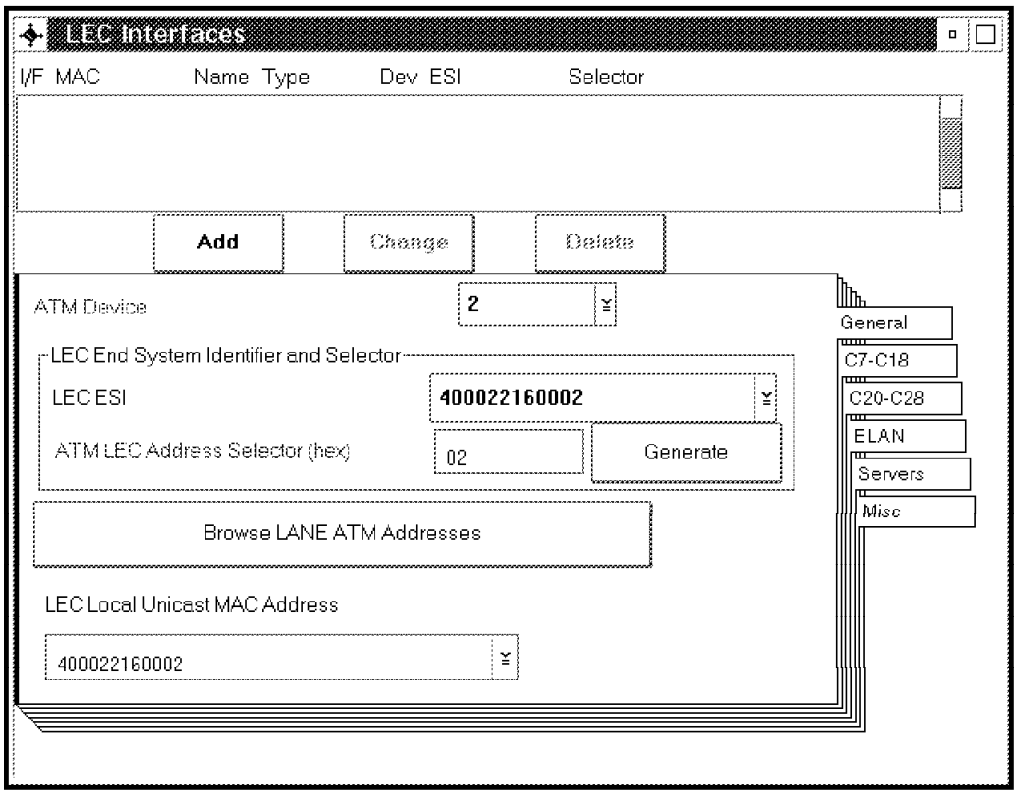


Figure 163. LEC Interfaces

During LE client definition, indicate the ATM interface it is associated with, the ESI and SEL used to construct the LE client's ATM address, and the MAC address associated with the LE client. To simplify problem determination, a locally administered ESI is recommended. Use a SEL that is generated by the configurator. Make sure the MAC address is unique.

Notes:

a. LE clients can be ATM Forum or IBM compliant. The 2210 and 2216 code provides support for ATM Forum-compliant LE services only.

b. When the LE client is added, a logical interface number will be generated. This interface number (I/F) is required when configuring higher-layer functions such as IP or bridging for this LEC.

c. To change the MAC address from the default burned-in address, you need to type over the text in the box. Even though you can choose an address using the arrow at the end of the box, you only get to select the ESIs you enabled on the interface this way. To make the MAC address unique you need to type over the burned-in address text in the box.

2 Define the ELAN name and type.

After selecting **ELAN** in Figure 163, Figure 164 on page 311 will appear.

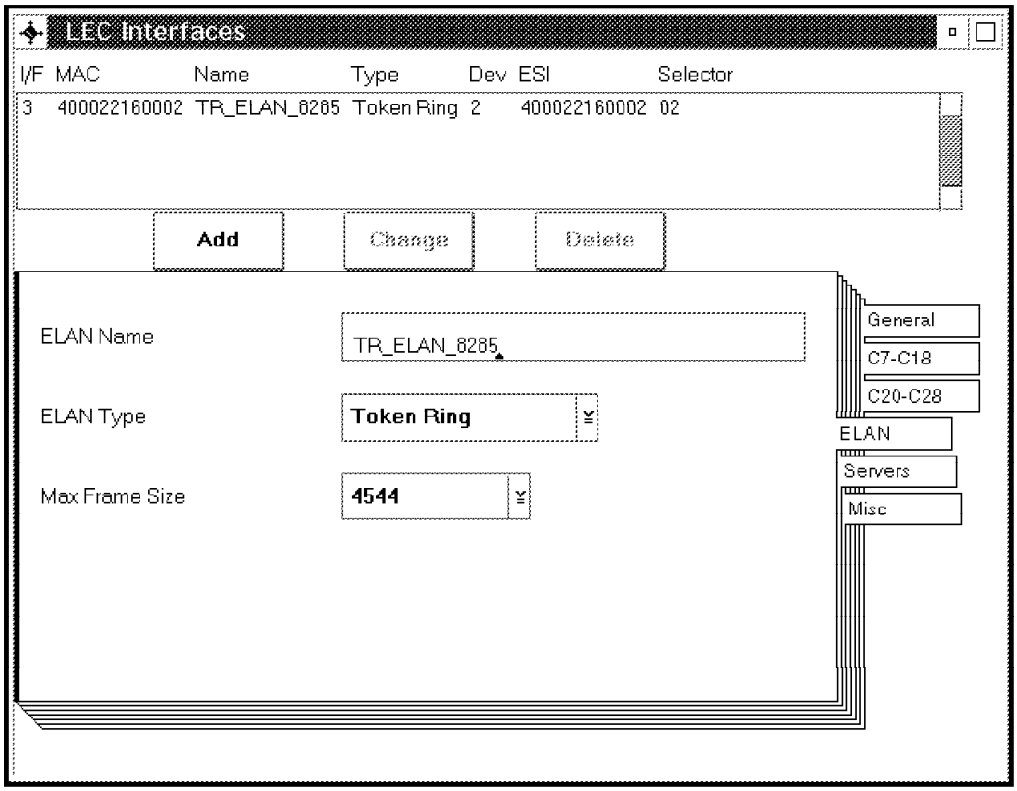


Figure 164. LEC Interfaces - ELAN

It is mandatory that you specify the ELAN type (token-ring or Ethernet) and maximum frame size. The ELAN name is optional. We advise that you define the same name on the LE client as on the LECS and LES.

3 Define the LE servers.

LE clients either obtain their LES address from the LECS, or use a hard-coded LES ATM address. The LECS can be hard-coded or, using ILMI, learned from the adjacent ATM switch.

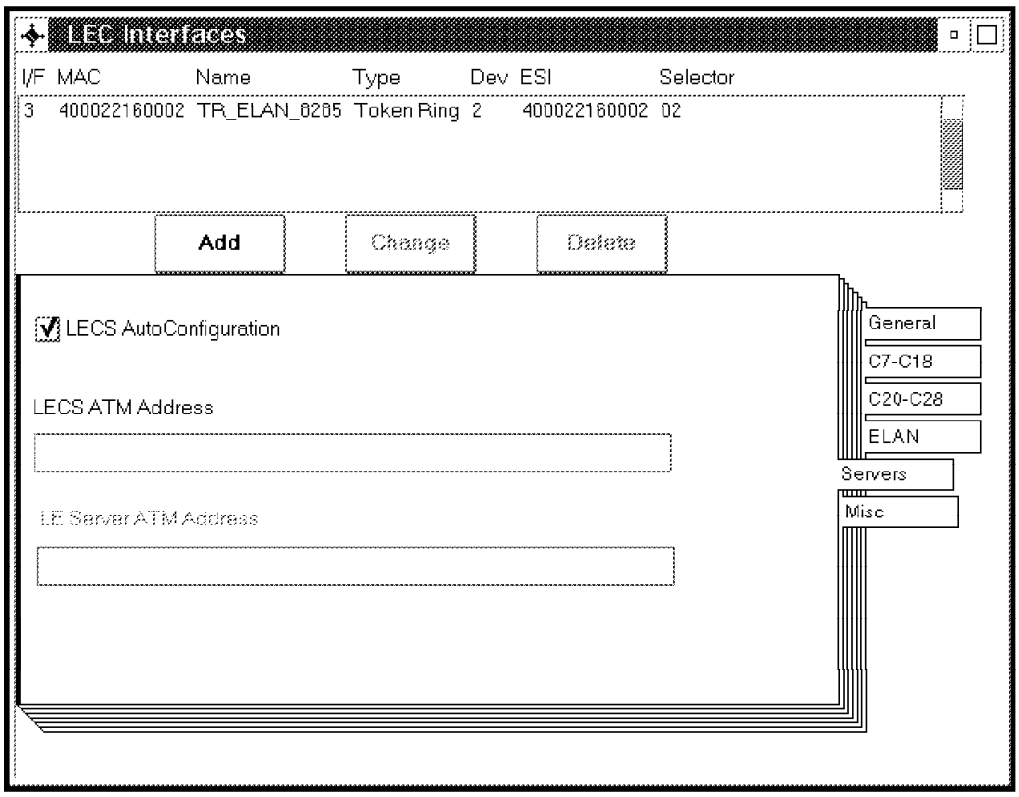


Figure 165. LEC Interfaces - LECS Auto-Configuration

Figure 165 results from selecting **Server** during LEC interface definition. Checking **LECS AutoConfiguration** specifies that the LE client will learn the LECS address from the adjacent ATM switch. Alternatively, a hard-coded LECS or hard-coded LES ATM address can be specified.

4 Define the higher-layer functions.

In addition to the basic LE client configuration steps listed earlier, configuration for higher-layer (bridging or routing) functions is required before the LE client can be used. For details on IP routing, IPX routing, and bridging, see 13.2.2, “IP Routing Protocols” on page 334, 13.2.3.1, “Routing IPX over RFC 1483 Connections” on page 335, and 13.3, “Bridging Overview” on page 341.

This completes the configuration of the 2210 and 2216 LAN emulation components.

Chapter 12. Classical IP

This chapter introduces the concepts of Classical IP (CIP) over ATM. It also details the steps required to configure a Classical IP client and ARP server on the IBM 2210 Nways Multiprotocol Router and IBM 2216 Nways Multiaccess Connector. Reading this section assists you in understanding and implementing Classical IP networks using the IBM 2210 and IBM 2216.

12.1 Introduction

The purpose of Classical IP as defined in RFC 1577 is to describe the methods for using the IP protocol over an ATM transport network. The problem with trying to run IP over ATM is not in the transfer of data. IP datagrams themselves are independent of the medium over which they travel. They can travel over an ATM VCC just as well as over a traditional shared-media LAN.

The problem is in trying to do the broadcast functions that traditional IP relies on to perform such functions as address resolution. Classical IP is simply an extension of the current IP paradigm that allows IP address resolution protocol (ARP) to operate in the non-broadcast environment of ATM.

Classical IP is a direct replacement for the traditional shared-media LAN (Ethernet or token-ring) and for IP links that interconnect them. It is called *Classical* IP because the IP stack interfaces to the ATM host adapter in the same way as traditional IP interfaces to a LAN adapter.

12.2 Classical IP Benefits

Applications that use IP will have the same functionality using CIP over ATM as they do in a legacy LAN or WAN environment. Their performance and throughput gains, however, may be substantial in the CIP environment.

This extra performance comes from the high link speeds that ATM provides in addition to the fact that Classical IP requires less overhead. The reduction in overhead results from three facts:

1. CIP makes more efficient use of packets.

   IP packets over LANs contain the source and destination MAC addresses in each packet sent. This is because the LAN provides connectionless service. CIP takes advantage of the connection-oriented virtual circuit of the ATM network and does not need to include the source and destination addresses in each packet. Therefore, less bandwidth is used for overhead bytes and more is used for data.

2. CIP does not use broadcasts.

   In a LAN environment, the traditional ARP is used to resolve IP host addresses to MAC addresses. These broadcast packets can adversely affect all stations in the subnet. With CIP, the ARP traffic is on a dedicated VCC between the ARP server and the client requesting the information. Other stations on the subnet are unaffected by this traffic.

3. CIP permits bandwidth reservation and guaranteed Quality of Service.

With the traditional shared-media LAN, each device on the LAN segment shares the bandwidth of the media. While a LAN station is transmitting, other devices are precluded from using the medium. With CIP, dedicated VCCs are established between devices on the subnet. These VCCs can be established with QoS parameters that protect the conversation from being impacted by other conversations.

The same benefits of moves, additions, and deletions to the network described for ELANs applies to the CIP Logical IP Subnet (LIS). Membership is not based on physical location. Logically related stations are grouped into the same LIS. The ease with which a client can register to the ARP server makes additions and changes trivial. Deletion from a subnet occurs naturally as the ARP server ages its entries.

While all members of a LIS must support the Classical IP model, the IBM 2210 and the IBM 2216 can route between subnets that are CIP-based and subnets that are LANE-based. Some equipment may be more adept at CIP, while other equipment may be more adept at LANE. This flexibility allows equipment to be utilized in the most effective manner.

Finally, investments in Classical IP are protected. Enhancements such as distributed ARP servers, Next Hop Resolution Protocol (NHRP), Multicast Address Resolution Service (MARS), Resource ReSerVation Protocol (RSVP) and other work that is being defined in the IETF will provide continual growth in functionality and performance. These are software-based enhancements and will not require hardware upgrades.

12.3 Classical IP Components

Classical IP, as described in RFC 1577, defines the operation of IP in what is known as a Logical IP Subnet (LIS) over an ATM transport network. As shown in Figure 166 on page 315, the LIS has two components:

- LIS clients
- One ARP server

The IBM 2210 and IBM 2216 can be configured as a LIS client or each can perform both roles simultaneously. (Since the ARP server is implemented on top of the LIS client function, the routers are not capable of being an ARP server without also being a client on the LIS.) A single ATM interface on the IBM 2210 or IBM 2216 can support up to 32 ARP clients/servers simultaneously.

The LIS contains all of the properties of a normal IP subnet. However, because ATM is a Non-Broadcast Multiple Access (NBMA) network, the existing broadcast method for resolving addresses can't be performed.

RFC 1577 defines the concept of an ARP server that is designed to solve this problem. The ARP server maintains a table of IP addresses to ATM addresses. Clients on the LIS needing to resolve an IP address make a request to the ARP server for the correct ATM address of the other device. This request is known as an *ATMARP*. The server either sends back a reply that includes the target ATM address (if the information is in its table), or a NAK (if no information is available). The client stores this ATM address in its ARP cache and then uses the ATM address to place a call to the target client. After the VCC is established, IP datagrams traverse the connection in much the same way as in a traditional LAN.

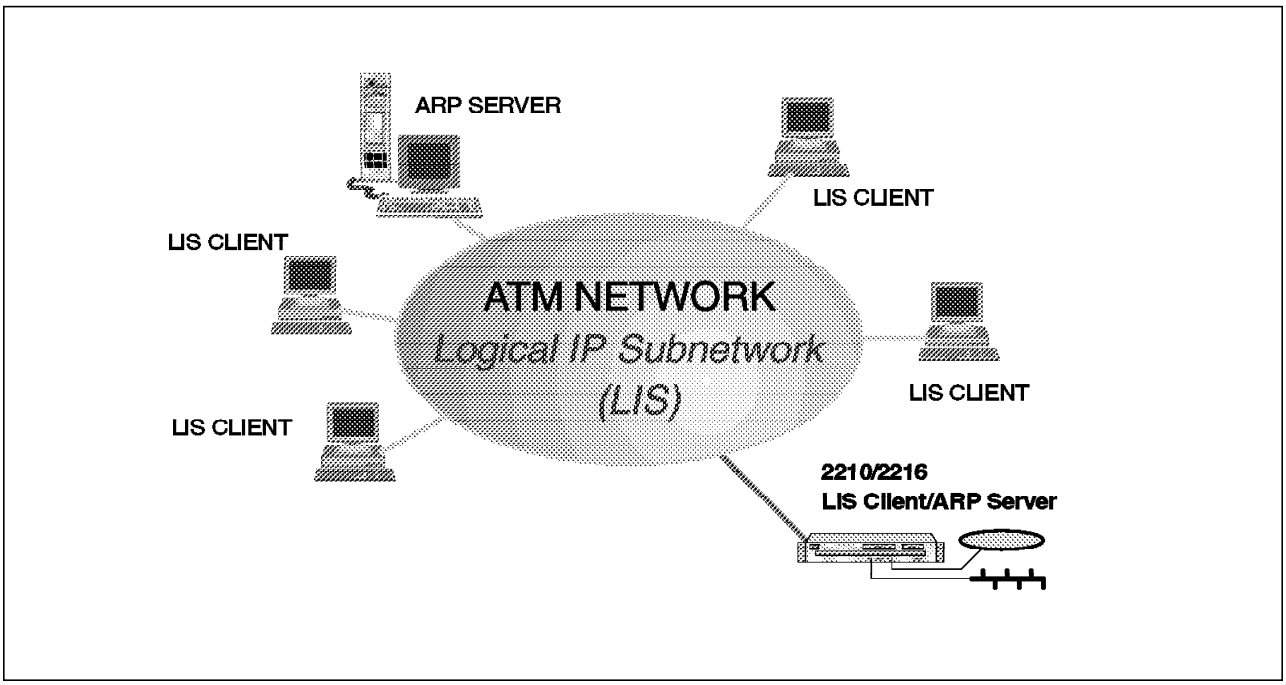


Figure 166. Components of Classical IP

Each LIS has one ARP server that is used for these purposes. (Backups can be defined with extensions to the standard such as those implemented by the IBM MSS server.) Each client must register with the ARP server during initialization of the client. This is done in the following manner:

1. Each client is configured with the ATM address of the ARP server.
2. As it initializes, each client places a call (establishes a direct VCC) to the ARP server.
3. The server, by definition, accepts all incoming calls.
4. Through the use of an InATMARP, the ARP server queries the IP host address and the ATM address of the calling device.
5. The ARP server updates its tables with the new information received from the client.

12.4 Table Refresh

Both clients and servers are responsible for managing their ARP cache by aging ARP entries in much the same way as with traditional IP. Once their timer expires, the ARP entries are deleted. If traffic is flowing when an ARP entry gets aged out, the traffic will cease until a new ARP entry is created.

To avoid an interruption in service in these cases, the 2210 and 2216 LIS client function provides an automatic refresh option. This option allows the LIS client to refresh these entries before they would otherwise expire.

The refresh can be done either via an ARP request to the ARP server or via an InATMARP to the target client. If using InATMARPs and the target replies, then the timer of the ARP entry is reset. If the target does not reply, then the entry is deleted. The default aging period for the CIP client in the 2210 and 2216 is 5 minutes.

The ARP server function in the 2210 and 2216 automatically sends out an InATMARP message before aging an entry out of its table. The default aging period for the ARP server function has a default of 20 minutes. Of course the timer values are configurable.

12.5 IP Addresses of CIP Components

When configuring the 2216 or 2210, the act of adding an IP address to the ATM interface automatically creates a CIP client with the default values. The user must then specify whether or not it is to also act as the ARP server for the LIS. An ARP server never exists without a paired client. The 2216 and 2210 support up to 32 LISs per ATM interface.

The creation of an IP address on a IBM 2216 or IBM 2210 interface enables packet forwarding behavior. Packets are forwarded between subnets even if no IP routing protocol is configured.

The routers also support the ICMP redirect function. That is, if a packet is sent to the 2216 or 2210 and the destination of the packet is for elsewhere on the same subnet as the source, the router will send an ICMP redirect message to the originator and forward the packet to the proper host.

12.6 ATM Addresses of CIP Components

In general ATM addresses must be unique among CIP components. On the 2210 and 2216, however, client/server pairs share an ATM address. This allows a single connection to be used for both control and data traffic.

The ESI portion of the ATM address defaults to the burned-in address on the ATM interface hardware and may be changed by selecting one of the locally administered ESIs defined for the ATM interface.

The selector byte of a CIP component′s ATM address may be explicitly configured or generated automatically at run time. If only a client is being created, then explicitly configuring the selector is not recommended. If a client/server pair is being created, then the selector should be specified in order to provide the server with a fixed address.

Note: Remember that each client on the LIS must be configured with the ARP server′s ATM address. If the selector is auto-generated, then the ATM address may change between reboots of the router.

12.6.1 Implementing CIP without an ARP Server

Classical IP can also be implemented without an ARP server. To do so, you need to define fully meshed RFC 1483 connections between every client on the LIS. This is the only way that connections between clients can be established over an ATM network in the absence of the address resolution functions provided by the ARP server.

You can well imagine that the administrative burden of such a task would get overwhelming for a LIS of any size and this is if the clients even supported such a configuration.

Since the IBM 2210 and IBM 2216 do support the definition of RFC 1483 connections, you could implement a LIS without using the ARP server function in

the router. However, since these products do provide this function, you will want to use it in most cases.

One situation that might require you to implement a LIS without an ARP server is when your ATM network does not support SVCs. For example, if you needed to connect routers over a wide area network (WAN) using ATM PVCs, you could create a LIS comprised only of the routers and define PVCs between them. This would allow you to route IP over the WAN.

12.6.2 Implementing CIP With PVCs versus SVCs

The IBM 2210 and IBM 2216 support RFC 1483 connections using both permanent virtual circuits (PVCs) and switched virtual circuits (SVCs). SVCs use UNI signaling to establish VCCs dynamically, when requested by a client needing to communicate with another client on the ATM network. The process only requires that the ATM address of the target device is known (which is provided via an ATMARP request).

PVCs are static connections that get established when the routers initialize themselves and they stay up as long as devices are powered on. PVCs require dedicated VPI/VCI pairs be defined between routers. These must be manually configured.

When PVCs are used, there is no need for an ARP server. Each member of the LIS is required to use the Inverse ATM Address Resolution Protocol (InATMARP) on each PVC to determine the IP address of the station at the other end of the connection. When the requesting station receives the InATMARP reply, it may complete the ARP table entry and use the provided address information.

Note: Information learned via InATMARP reply may be aged or invalidated under certain circumstances. It is the responsibility of each IP station supporting PVCs to revalidate ARP table entries as part of the aging process. The 2210 and 2216 will not validate pre-configured partner IP addresses on PVCs.

12.7 Logical IP Subnetwork Configuration

In Classical IP, each LIS operates and communicates independently of other LISs on the same ATM network. Hosts on the same LIS communicate via direct VCCs between each other.

However, communication to hosts outside of the local LIS (on any topology, ATM or not) must use an IP router. This router also is a client on the LIS and is capable of routing between the LIS and other interfaces on the machine.

This configuration may result in a number of disjointed LISs operating over the same ATM network. Hosts of differing IP subnets communicate via an intermediate IP router even though it may be possible to open a direct VCC between the two IP members over the ATM network. This is illustrated in Figure 167 on page 318.

The following are the requirements for all IP members (hosts, routers) operating in an ATM LIS configuration:

- All members must have the same IP network/subnet number and address mask.
- All members must have a direct connection to the ATM network.

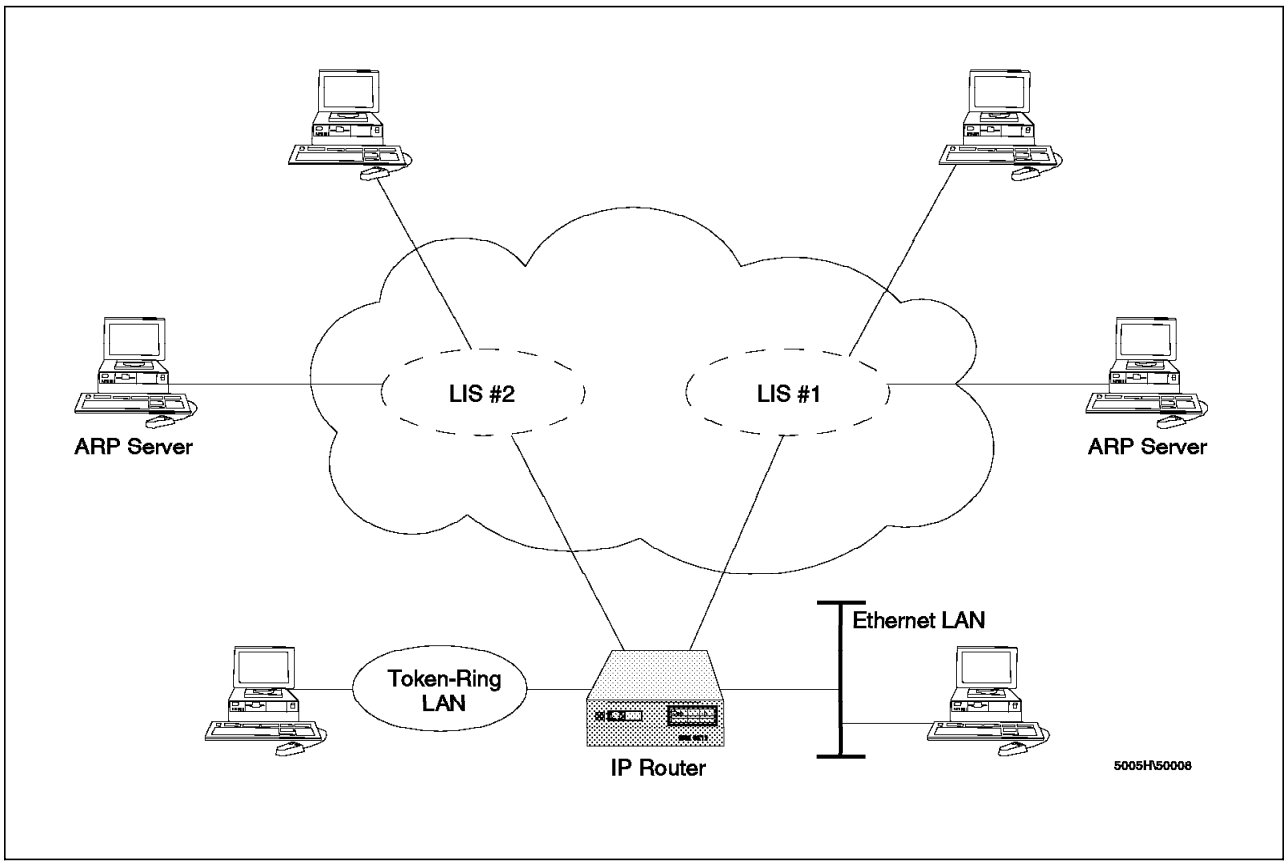


Figure 167. Logical IP Subnetworks

- All members must use the same maximum transfer unit (MTU) size.

  Note: The MTU is the maximum AAL-5 service data unit (SDU) minus 8. (see also item 2e on page 320).

- All members outside of the LIS are accessed via a router.
- A service must exist for resolving IP addresses to ATM addresses via ATMARP and vice versa via InATMARP when using SVCs.
- A service must exist for resolving VCCs to IP addresses via InATMARP when using PVCs.

12.8 Key Configuration Parameters for Classical IP

Due to the simplicity of CIP, very few configuration parameters are required. The information needed for a client-only configuration is:

1. IP address and subnet mask
2. ATM address of the ARP server (if SVCs are used with no static entries in the clients ARP table)
3. Maximum AAL-5 Service Data Unit (SDU) size

   When configuring CIP on the 2210 and 2216, you will be given the opportunity to override the default value for the SDU parameter. This parameter relates to the maximum transmission unit (MTU) size of the LIS and there is a direct relationship between the two parameters (SDU = MTU+8). There are a couple of points worth clarifying here:

- The ATM interface also has a parameter for the max SDU size (defaults to 9234) and the CIP client MTU size can be no larger than that specified for the ATM interface.
- All members of the LIS must use the same MTU size.
- The default value for the 2210/16 CIP client SDU of 9188 will result in an MTU of 9180 which is the same default MTU size of the IBM CIP drivers for client PCs.
- If you have more than one CIP client on the same 2210/16 ATM interface, they need to use the same SDU size.

Configuration of a client/server pair requires:

1. IP address and subnet mask
2. Answering yes to the question that the client is also a server
3. Specifying an explicit selector for the servers ATM address

12.9 Classical IP Configuration Overview

This section covers the basic steps required to configure Classical IP functions using the Configuration Program.

Note: Detailed scenarios using the command line interface are included within Chapter 14, “ATM Scenarios” on page 343.

The different configuration steps that need to be completed depend on the functions that need to be activated. The basic steps include:

1 Define the ATM interface(s).

ARP servers and LIS clients are components that need to be associated with an ATM interface. When associated, all ATM traffic of the component will take place on the ATM interface specified.

During configuration of the ATM interface you have to configure:

a. The ATM interface attributes.

For more details, see 11.7, “Configuring LAN Emulation on the 2210 and 2216” on page 300.

b. The end system identifiers (ESIs) associated with the ATM interface.

During the definition of the ARP server and/or clients either the burned-in end system identifier (ESI) or a user-defined ESI must be used. To ease the definition of the ATM addresses on remote LIS clients, for example, when referring to the ARP server, and to simplify troubleshooting it is recommended that you use a locally administered ESI. ESIs are administered per ATM interface. A separate value has to be defined per ATM interface. All LIS client/servers that connect using a particular interface can use the same ESI. Make sure that when defining multiple 2210s or 2216s, the user-defined ESIs are unique.

The ATM interface configuration must be repeated for each ATM interface on your 2216 which is used for Classical IP functions. The 2210 can only have a maximum of one interface; therefore this isn’t important for the 2210.

2 Configure the LIS client.

The configuration information that must be entered to define a LIS client is:

a. IP address

   Make sure that all clients (including the ARP server) use a unique address within the range of IP addresses associated with the LIS. During the definition, the IP address is associated with the 2210s or one of the 2216s ATM interfaces.

b. Subnet mask

   Make sure that all clients within a logical IP subnet (LIS) use the same subnet mask.

c. End system identifier (ESI)

   During the definition of the LIS client either the burned-in end system identifier (ESI) or a user-defined ESI must be used. When using an ARP server, the LIS client ATM addresses are learned dynamically and no predefinition of addresses is required. However, for management purposes we recommend the use of a locally administered ESI. All LIS clients using the same 2210 or 2216 ATM interface can use the same ESI.

d. Selector (SEL) byte

   The 1-byte selector byte (SEL) decides, together with the 6-byte ESI and the 13-byte ATM network identifier, the ATM address used by the LIS client. For LIS clients using ARP services we recommended that you use a selector byte generated by the 2210 or 2216 at run time.

e. Service data unit (SDU)

   Make sure that all clients within a logical IP subnet (LIS) use the same SDU. Use the default value (9188) whenever possible.

   The maximum SDU size can be configured on a LIS client basis, but cannot be greater than the maximum SDU size for the ATM interface (default 9234). Although the SDU can be defined on a client basis, values are not independent because all clients on an ATM interface share the same MTU. The MTU size is set to the smallest client SDU size-8 (frames have 8-byte header). Consequently, all clients with a given ATM interface must have the same MTU; therefore, care should be exercised when altering a client′s maximum SDU size.

f. ARP server ATM address

   When configuring a LIS client, the configurator requires you to specify if the LIS client is also an ARP server. If you want LIS client functions only, configure NO.

   To enable connectivity, LIS clients need to connect to an ARP server first. Make sure that the server ATM address specified is the ATM address of your ARP server.

Repeat the previous steps for every LIS client. For details, see 12.9.1, “LIS Client Using Dynamic SVCs” on page 322.

3 Configure the ARP server.

ARP servers defined on the 2210 or 2216 are both a LIS client and an ARP server. Therefore, the definitions required to define an ARP server are, to a large extent, equivalent to defining a LIS client. The configuration steps required are:

a. IP address

   Make sure that all clients (including the ARP server) use a unique address within the range of IP addresses associated with the LIS. During the definition, the IP address is associated with the 2210s or one of the 2216s ATM interfaces.

b. Subnet mask

   Make sure that all clients/servers within a logical IP subnet (LIS) use the same subnet mask.

c. End system identifier (ESI)

   During the definition of an ARP server it is recommended that you use a user-defined ESI.

d. Selector (SEL) byte

   The 1-byte selector byte (SEL) decides, together with the 6-byte ESI and the 13-byte ATM network identifier, the ATM address used by the ARP server. Because the ARP server's address needs to be hard-coded on LIS clients, we recommend that you use a user-defined value, instead of using a value decided at run time.

   Note: Make sure that when defining the selector byte, the combination of ESI and SEL on your IBM 2210 or IBM 2216 is unique.

e. SDU

   Make sure that all clients (including the ARP server) within a logical IP subnet (LIS) use the same SDU. Use the default value (9188) whenever possible.

f. ARP server ATM address

   When configuring a combined LIS client/ARP server, the configurator requires you to specify if the LIS client is also an ARP server. When defining an ARP server, configure YES.

Repeat the previous steps need to be repeated for every ARP server. For details, see 12.9.2, "Configuring an ARP Server" on page 326.

4 Configure PVC connection.

If some or all of your LIS clients do not support SVCs, PVCs can be used in addition to, or as an alternative for, the dynamic SVCs and/or static SVCs discussed in 2 on page 319 and in 5, respectively.

12.9.3, "LIS Client Using PVCs" on page 328 discusses how to define a PVC between two LIS clients. Note that before defining the PVC a LIS client has to be configured.

Notes:

a. The PVC is a connection between two LIS clients. Equivalent definitions are required at both ends.

b. Each LIS client can have PVCs defined to multiple remote LIS clients.

5 Configure static SVC connection.

If some or all of your LIS clients support SVCs but do not allow the use of an ARP server, static SVCs can be used in addition to, or as an alternative

for, the dynamic SVCs and/or PVCs discussed in step 2 on page 319 and step in 4, respectively.

12.9.4, “LIS Client Using Static SVCs” on page 330 discusses how to configure a predefined SVC between two LIS clients. Note that before being able to configure the SVC, a LIS client has to be configured.

Notes:

a. The SVC is a connection between two LIS clients. Although both ends need to be configured as a LIS client, only one end needs to configure the SVC.

b. At each LIS client you can define static SVCs to multiple remote LIS clients.

12.9.1 LIS Client Using Dynamic SVCs

In this section, we used the 2216 configuration program for the screen captures. The 2210 configuration program has very similar windows and the same procedures used here can be directly applied to the 2210. The only major difference is that the 2216 can have two ATM interfaces configured, whereas the 2210 can only have one.

If you are configuring the 2216, you initially need to configure slots to add adapters as they are physically installed. You then need to configure the ATM interface. These two procedures are described in 11.7.1, “Configuring an ATM Interface” on page 305. If you are configuring the 2210, you need to initially configure the ATM interface as for the 2216.

To start the Classical IP configuration select **Interfaces** in the Navigation Window as shown in Figure 168.

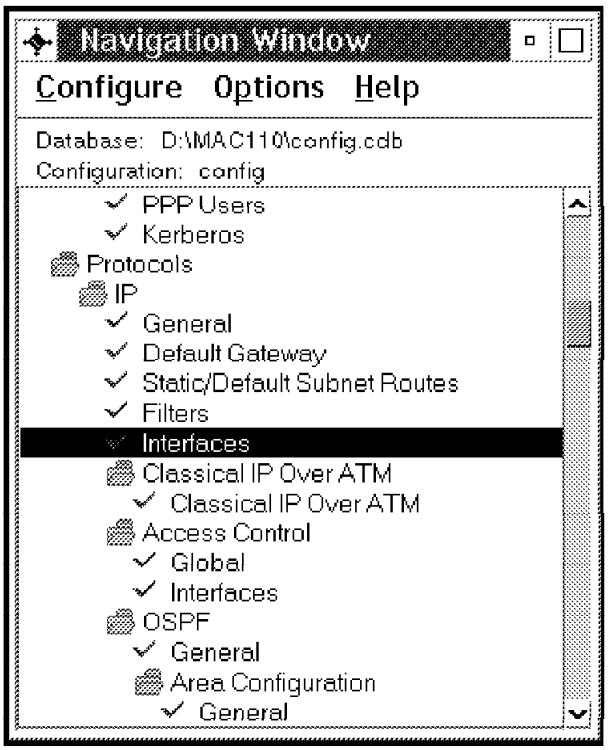


Figure 168. Interfaces

As a result Figure 169 on page 323 appears. Click on **IP Addresses** on the interface that you want to use for this LIS client. Add a unique IP address that is consistent with the range of IP addresses associated with the LIS. Make sure that all LIS clients within the same LIS use the same subnet mask.

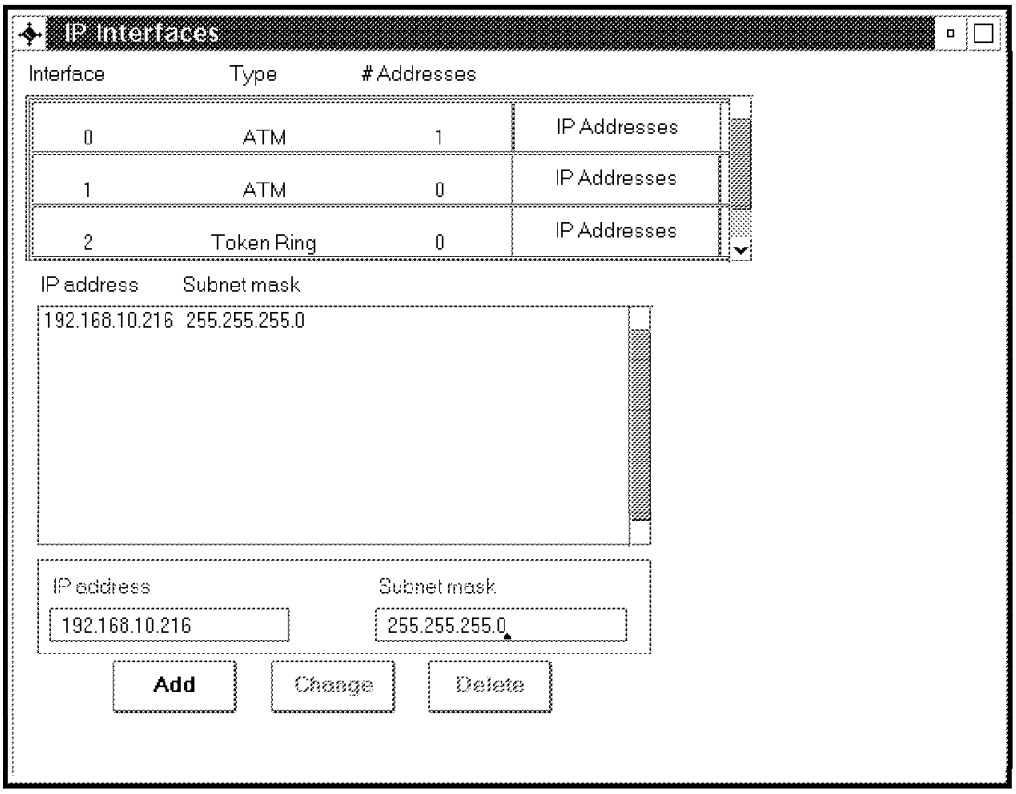


Figure 169. Add IP Address

Once an IP address is added on an ATM interface, Classical IP definitions are required. To configure Classical IP, select **Classical IP Over ATM** in the Navigation Window as depicted in Figure 170 on page 324.

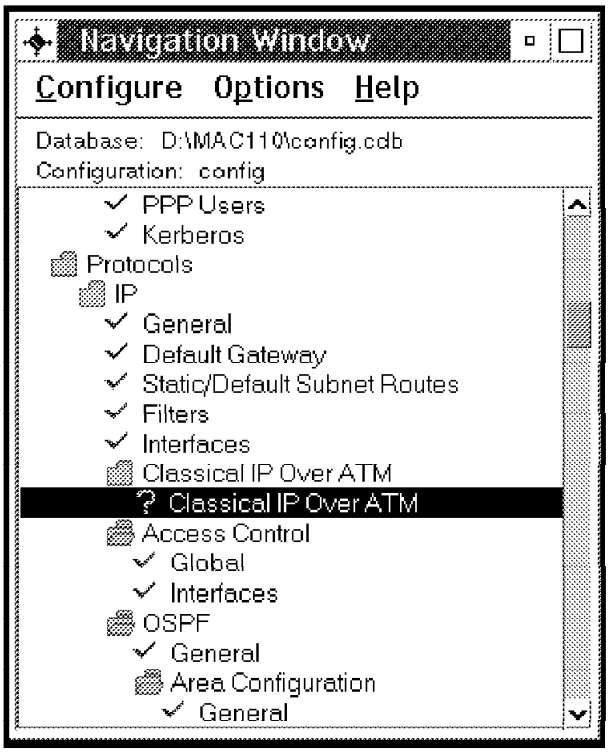


Figure 170. Classical IP over ATM Definitions

After clicking on **Classical IP Over ATM**, Figure 171 will appear. The configuration of the LIS client's specific parameters can start after you have selected the proper IP address (the address defined in Figure 169 on page 323).

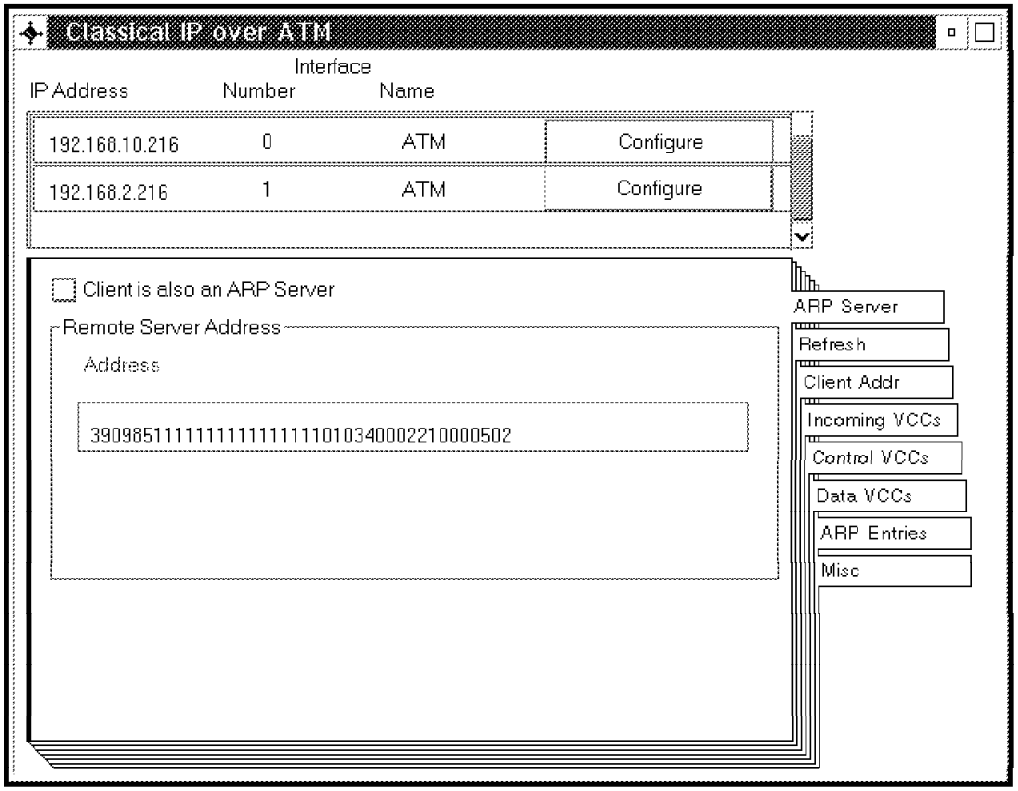


Figure 171. ARP Server

When defining a LIS client, do not enable **Client is also an ARP Server**. Instead, enter the 20-byte ATM address of the ARP server.

Using default values in the remaining configurator screens completes the LIS client configuration. Two screens, however, are worth mentioning.

Figure 172 shows that for a LIS client the configurator assumes that the selector is assigned at run time. This setting is adequate, unless using predefined SVCs between two clients (see 12.9.4, “LIS Client Using Static SVCs” on page 330). In this case, you have to make sure that on at least one of the clients, a preconfigured selector is used.

Figure 173 on page 326 shows the maximum SDU that is used by the LIS clients. Make sure that all LIS clients within the same LIS use the same value. Also make sure that this value is less than the maximum size allowed on the ATM interface.

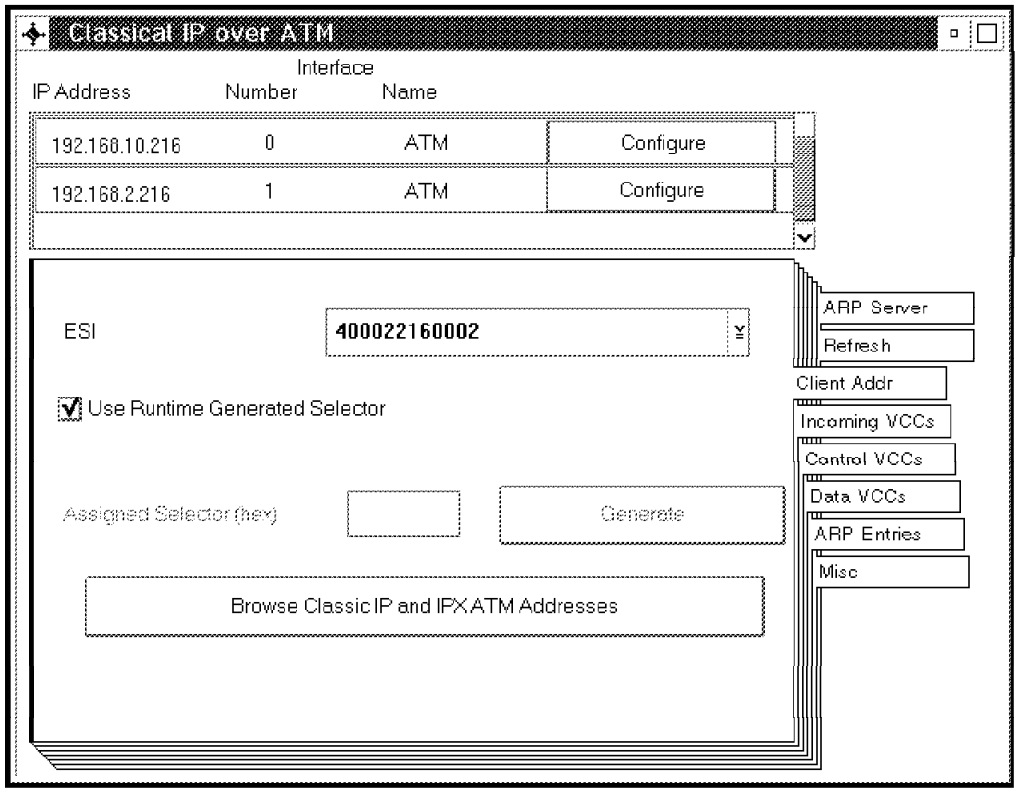


Figure 172. Run-Time Selector

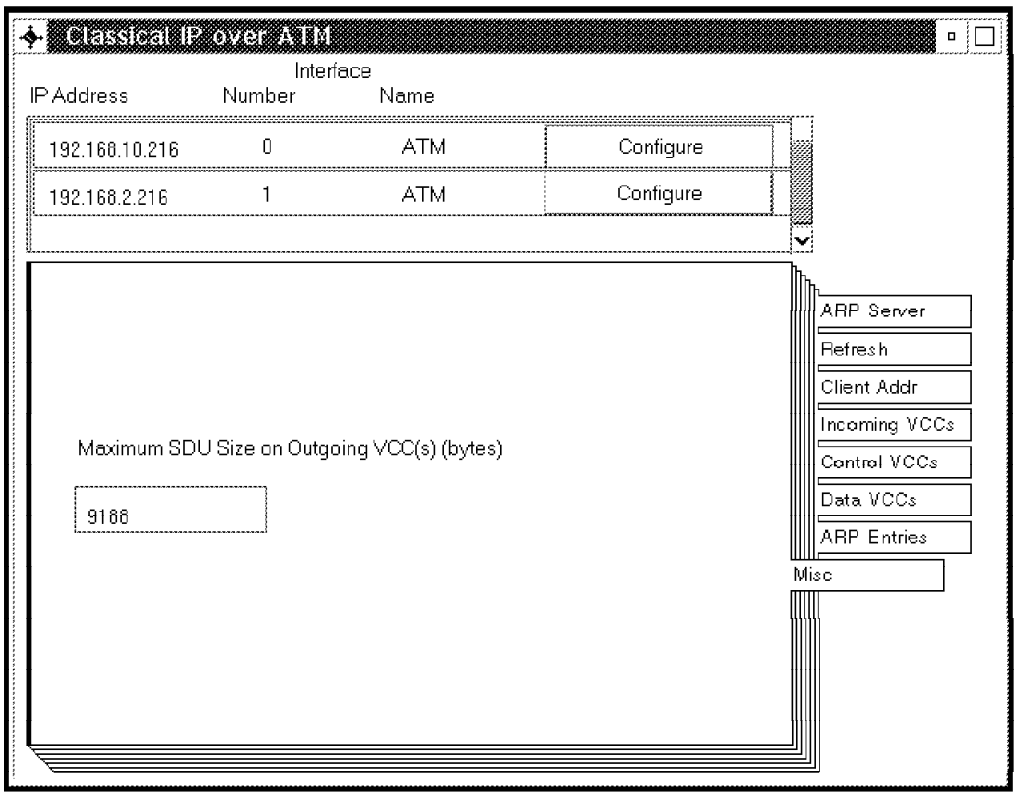


Figure 173. Maximum SDU Size

12.9.2 Configuring an ARP Server

ARP server and LIS client (see 12.9.1, “LIS Client Using Dynamic SVCs” on page 322) configurations are defined using the same configuration screens. For an ARP server you also have to define an IP address (+subnet mask) first and associate this address with a specific ATM interface (see Figure 168 on page 322, Figure 169 on page 323, and Figure 170 on page 324).

Figure 174 on page 327 will appear after clicking on **Configure** for the IP address of the ATM interface to which you want to add the ARP server.

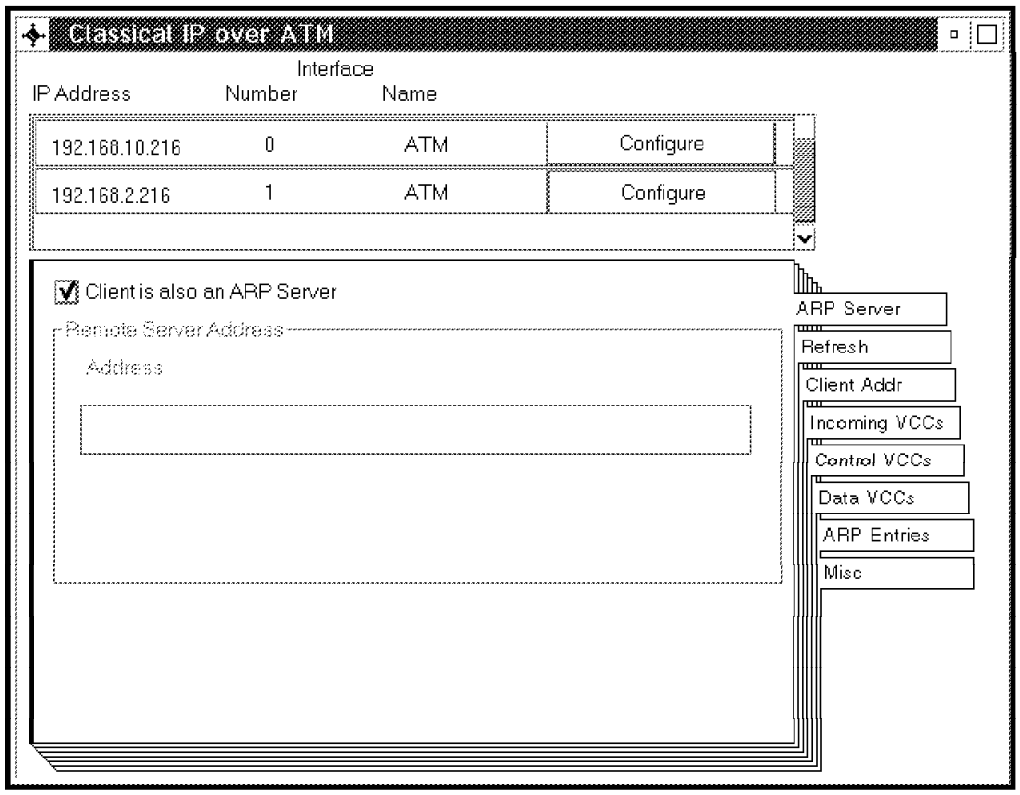


Figure 174. ARP Server Definition

When defining an ARP server, enable **Client is also an ARP Server**. Leave the Remote Server Address field empty.

One configuration screen that needs special attention is Figure 175 on page 328. This screen becomes available after selecting **Client Addr**. As the ARP server's ATM address needs to be specified during the configuration of remote LIS clients, the variables that comprise the address (in particular ESI and SEL) need to be fixed. It is, therefore, advised that you use a locally administered ESI and a user-defined selector.

For the remainder of the configuration screens, default values can be used. Make sure that the maximum SDU size does not conflict with the value configured on other LIS clients (see Figure 173 on page 326).

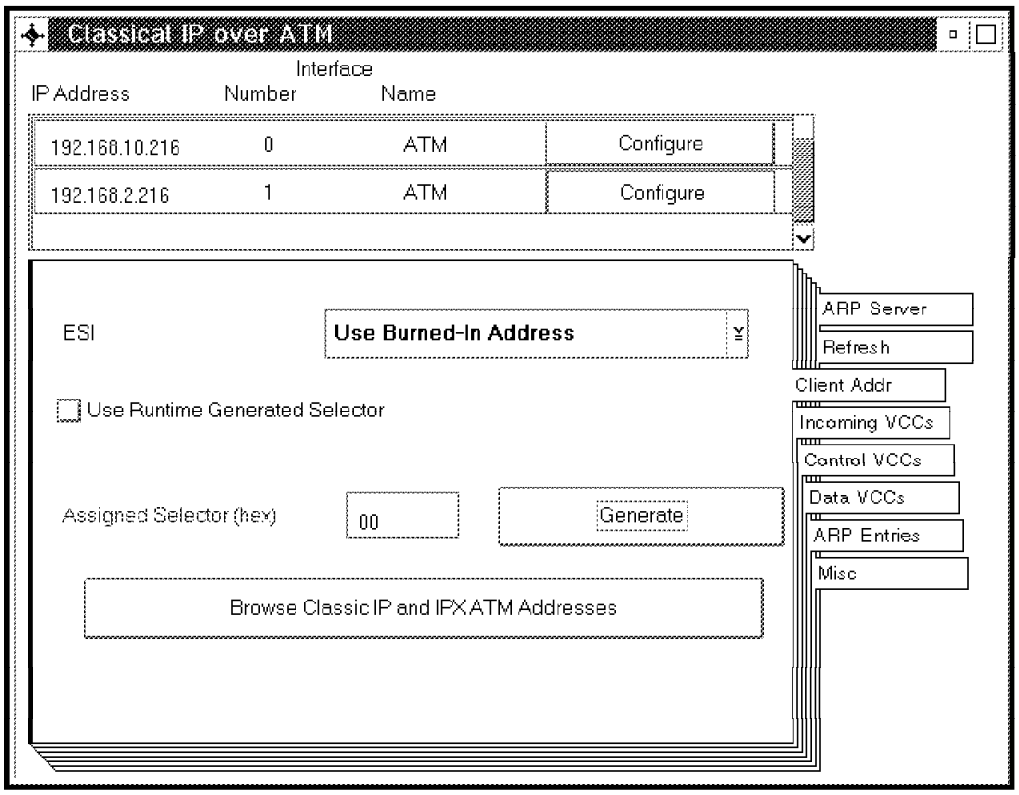


Figure 175. ESI and Selector

12.9.3 LIS Client Using PVCs

When defining a LIS client, you have the option to provide connectivity using SVCs or PVCs. The use of SVCs is more flexible and is recommended. However, in situations where your ATM switches do not support SVCs, or no ARP server is available for your LIS, PVC connections can be considered. PVCs can also be considered if UNI incompatibilities exist.

Note: PVCs can be used in conjunction with SVCs as well.

Defining a PVC to a remote LIS client requires two things:

- Definition of a LIS client
- Definition of a PVC

The LIS client definitions have been overviewed in 12.9.1, “LIS Client Using Dynamic SVCs” on page 322 and are not repeated. They are required at both ends of the PVC. The LIS client definitions define the throughput characteristics of the VCCs.

The PVC definition requires similar configuration at both ends. PVC definitions are entered during the definition of the LIS client. You can define multiple PVCs per LIS client (identified by its IP address).

The parameters that can be entered become available after selecting **ARP Entries** during the configuration of Classical IP over ATM. Figure 176 on page 329 appears once you have selected **ARP Entries**.

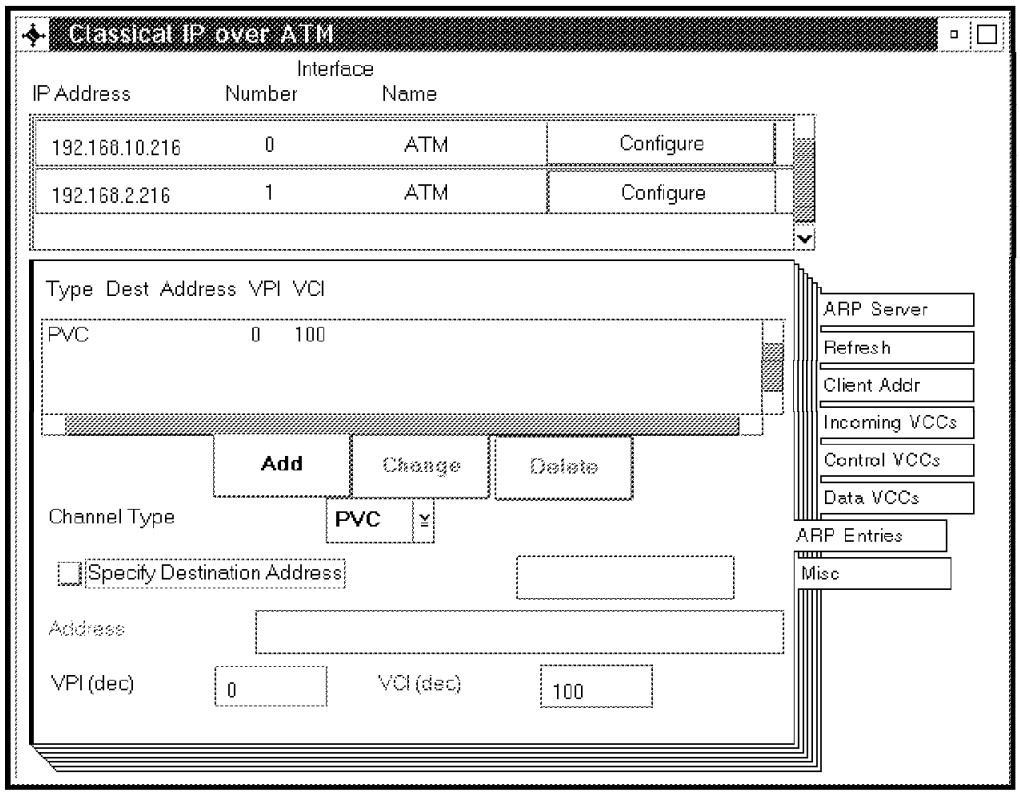


Figure 176. PVC Definition

Make sure that the virtual path identifier (VPI) and virtual channel identifier (VCI) match the definitions on the adjacent switch (see 12.9.3.1, “Defining PVCs on the ATM Switch”). When you enable **Specify Destination Address**, enter the IP address of the remote LIS client. We recommend that you disable this option and let the 2210 or 2216 learn the IP address of the other end dynamically. This, however, requires InATMARP support at the other end. InATMARP is supported on the 2210 and 2216.

12.9.3.1 Defining PVCs on the ATM Switch

Figure 177 on page 330 shows the set pvc command used to define a PVC between two devices, port 16.01 and port 1.01. The PVC is verified using the show pvc command.

The same VPI but different VCI numbers are used at the ends of the PVC. In this case we use one device attached to port 16.01 on an IBM 8260 and the other device attached to port 1.01 on an IBM 8285. The 8260 is hub number 1 in our network and the 8285 is hub number 3. These values may be replaced with those relevant for your configuration.

Define the PVC:

```
8260ATM1>set pvc
Enter local port: 16
Enter local port: 1
Enter PVC id: 50
Enter remote port: 1
Enter remote port: 1
Enter remote hub number: 3
Enter call type: channel
Enter local VPI: 0.
Enter local VCI: 200
Enter remote VPI: 0.
Enter remote VCI: 100
Enter quality of service: best_effort
PVC set and started.
8260ATM1>
```

Figure 177. PVC Definitions on an ATM Switch

Verify PVC definition:

```
8260ATM1> show pvc
Enter port: 16.
Enter port: 1
Enter pvc id: 50

       Local end point       ! Remote end point  !
----------------------------+-------------------+
 Port   id   type   Vpi/Vci  ! Port Vpi/Vci   HNb!   role  !QOS! Status
----------------------------+-------------------+---------+---+---------
16.01    50 PTP-PVC   0/200  ! 1.01   0/100     3! Primary ! BE!Active
8260ATM1>
```

Figure 178. PVC Definitions on an ATM Switch

Note: PVC identifier 50 has been assigned to the PVC definition.

12.9.4 LIS Client Using Static SVCs

The IBM 2216 and the IBM 2210 provide an interesting option of being able to configure LIS clients that are using SVCs for their LIS-to-LIS client connections but do not require the presence of an ARP server. Similar to using PVCs, this approach has the advantage that no ARP server is needed. In addition, because the LIS-to-LIS client connections are established using SVCs, no ATM switch definitions are required to enable the VCCs.

Note: Static SVCs can be used in conjunction with dynamic SVCs and PVCs.

12.9.4.1 Active and Passive LIS Client

Predefined SVCs require that, for each client-to-client connection, one client's ATM address is defined on the partner client. This results in definitions that are not symmetrical; one (active) client defines the ATM address of the other end and is responsible for VCC establishment and one (passive) client awaits VCC establishment. After the connection has been established, full-duplex IP transport between both clients is possible.

Note: If the SVC has been defined on both ends, depending on timing, two VCCs can be established which are each used for traffic in one direction.

12.9.4.2 Definitions Required

Defining a static SVC to a remote LIS client requires two things:

- Definition of a LIS client
- Definition of an SVC

The LIS client definitions have been overviewed in 12.9.1, “LIS Client Using Dynamic SVCs” on page 322 and are not repeated. They are required at both ends of the SVC. The LIS client definitions define the throughput characteristics of the VCCs.

The SVC definitions need to be entered on one end only. This end is referred to as the active LIS client because it is responsible for VCC establishment. Definitions are added during the definition of the LIS client. You can define multiple static SVCs per LIS client (identified by its IP address).

The parameters that can be entered become available after selecting **ARP Entries** during the configuration of Classical IP over ATM. Figure 179 results.

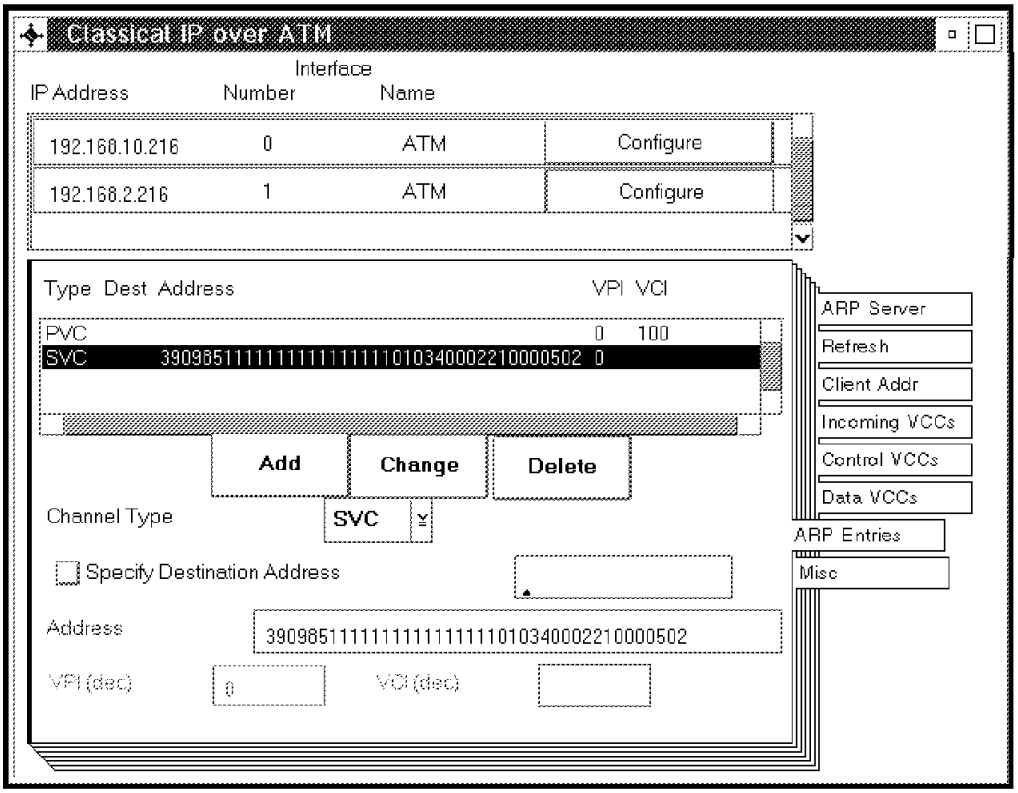


Figure 179. Static SVC Definition

When **Specify Destination Address** has been enabled, the IP address of the remote LIS client needs to be entered. We recommend that you disable this option and let the 2210 or 2216 learn the IP address of the other end dynamically. This, however, requires InATMARP support at the other end. InATMARP is supported on the 2210 and 2216.

The Address field must match the ATM address of the remote LIS client. To make sure that the ATM address of the passive LIS client is fixed, we recommend that you specify a locally administered ESI and a preconfigured

selector during its configuration. During the definition of the active LIS client you can specify the use of a run-time selector.

Using the point-to-point (PtP) concept, more complex network structures can be built. Therefore, be aware that within each LIS:

- Every LIS client requires only a single IP address and a single LIS client definition.
- For each PtP connection, at least one end must be assigned as the active client. This active client is responsible for VCC establishment and requires an ARP entry.
- Clients can be active for one PtP connection, while being passive for another.

Chapter 13. Routing and Bridging Support over ATM

This chapter outlines the support provided on the IBM 2210 and the IBM 2216 for routing and bridging over ATM RFC 1483 connections and ATM LAN emulation interfaces. Reading this chapter will help you understand the functions that are provided and how the routing and bridging is performed over ATM. Examples of configuring these functions can be found in 14.3, “Implementing Scenario 3” on page 386.

13.1 RFC 1483 Support

RFC 1483 specifies encapsulation methods for carrying bridged and routed protocols over AAL-5 ATM connections. Both Classical IP and the IPX support in the 2210 and 2216 use the LLC SNAP format for routed protocols as defined in this RFC. This is important to keep in mind as you read about the IP and IPX routing and the bridging support in the following sections.

13.2 Routing Support

The routing overview presented in this section is short due to the simple relationships between LAN emulation, Classical IP and the supported routing protocols.

The key to understanding the support provided for both routing and bridging over ATM is the fact that a LAN emulation client and an RFC 1483 connection appear to the routing and bridging software as just another interface.

For example, in LAN emulation, when a LEC is created, it is assigned a unique interface number. The interface number may then be used to configure the desired routing protocols. The protocols then treat the emulated LAN interface exactly the same as a real Ethernet and token-ring interfaces.

13.2.1 IP Routing

Figure 180 depicts the IP routing support provided by the 2210 and 2216.

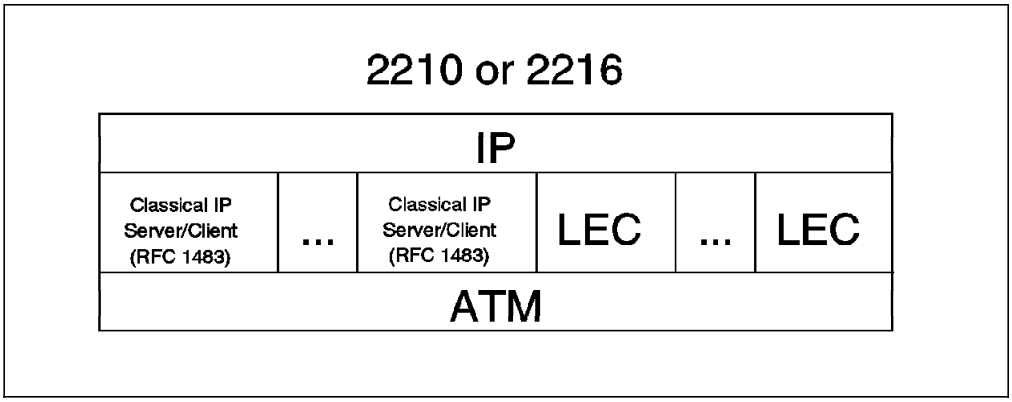


Figure 180. IP Routing in the 2210 and 2216

As can be seen in the figure, IP routing is supported between any combination of CIP, LANE, or legacy interfaces on the router. This support includes OSPF,

multicast support and classless addressing in addition to basic IP support such as ICMP, UDP, TCP and ARP.

13.2.2 IP Routing Protocols

The IBM 2210 and the IBM 2216 support both RIP and OSPF over ATM LAN emulation. RIP is only supported over LAN emulation. It is not supported over Classical IP. More detail on IP routing protocols can be found in *Description and Configuration Scenarios Volume I*. Examples of configuring RIP and OSPF can be seen in 14.2, “Implementing Scenario 2” on page 358 and 14.3, “Implementing Scenario 3” on page 386 respectively.

13.2.2.1 Using RIP

As stated earlier, RIP is only supported on LAN emulation. In Classical IP networks OSPF, BGP or static routes can be used instead.

RIP is a very robust protocol and there is a very high probability that implementations from different vendors will interoperate together without difficulty. However, due to the limitations of RIP, it is not recommended that you use it as the major routing protocol for new network designs. Instead, RIP should be used in situations where it is necessary to interoperate with an existing network already using it.

13.2.2.2 Using OSPF

OSPF is a relatively new routing protocol and, for that reason, does not have the installed base of RIP. However, most large internal networks either currently in design or being implemented use OSPF as the major routing protocol. This is because OSPF overcomes many of the limitations of RIP.

OSPF can be implemented on both LAN emulation and Classical IP subnets using the 2210 and 2216. On Classical IP networks, neighboring routers must be defined to each other. In this regard, it works in much the same way as for frame relay networks.

If the 2210 or 2216 is attaching to more than one LIS, the routing protocol needs to be enabled for each IP address on the ATM interface.

13.2.3 IPX Routing

Figure 181 depicts the support for IPX routing. As can be seen in the figure, IPX routing is supported over emulated LAN interfaces and RFC 1483 connections to other routers.

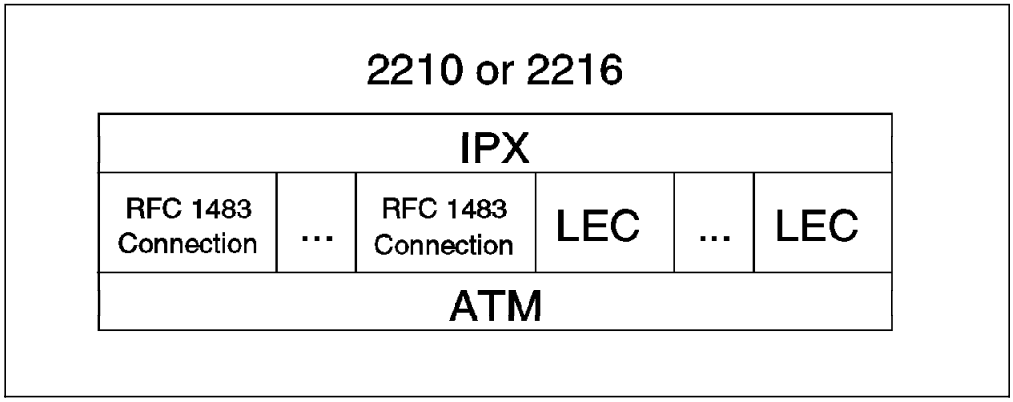


Figure 181. IPX Routing in the 2210 and 2216

The 2210 and 2216 IPX routing support complies with the IPX router specification from Novell. IPX is fully supported over emulated LANs and the steps to configure IPX routing over an emulated LAN interface are exactly the same as for a legacy LAN interface.

IPX routing is also supported between routers attached via RFC 1483 connections. This is briefly discussed below.

13.2.3.1 Routing IPX over RFC 1483 Connections

IPX routers use the Routing Information Protocol (RIP) and the Server Advertisement Protocol (SAP) to propagate routing and server information tables. These protocols use broadcast frames to propagate information to interested parties. The 2210 and 2216 will propagate these broadcasts to all other adjacent routers over RFC 1483 connections.

These connections must be configured so that a permanent connection will exist while the network is operational. Both PVCs and configured SVCs are supported.

Note: The configuration of a PVC or SVC for IPX uses the same procedure as configuring them for Classical IP. For information on configuring static SVCs or PVCs see 12.9.4, “LIS Client Using Static SVCs” on page 330 or 12.9.3, “LIS Client Using PVCs” on page 328 respectively.

Currently, only one IPX network may be configured per ATM interface. That is, there can be connections to multiple routers on one ATM interface, but all of the routers must use the same IPX network number.

RFC 1483 VCCs to IPX routers may not be shared with other protocols such as IP. As with Classical IP, Quality of Service characteristics can be specified by configuring VCC traffic parameters, such as Peak and Sustained Rates.

ATM Addresses: IPX ATM addresses must be unique among all components using RFC 1483 encapsulation, which includes Classical IP components. The ESI and selector portions of the ATM address are configured in the same manner as Classical IP ATM addresses and the rules are also the same. For example, if you are using static SVCs for the RFC 1483 connections, then you will need to provide ATM addresses when configuring the SVCs. In this case, you should use a manually assigned selector and a locally administered ESI so that you can provide a fixed address that can be configured at the calling routers.

Protocol Addresses: IPX protocol addresses have two parts:

- A 4-byte network number
- A 6-byte host number, also known as the host ID

Network numbers must be unique within IPX routing domains and host numbers must be unique within an IPX network.

Destination IPX host numbers may be specified during VCC configuration or learned dynamically via an InATMARP. IPX host numbers of destination routers that do not support InATMARP must be configured. When the destination host number is configured, the associated routing table entry is permanent and not aged out. Conversely, when the destination host number is not configured the associated routing table is aged. An InATMARP is used to periodically refresh the 2210s′ or 2216s′ knowledge of the partner routers IPX host number.

The host number portion of a local IPX address is automatically set to the ESI component of the associated ATM address. This value will be the burned-in address of the ATM interface hardware, unless an ESI has been configured for the ATM interface. We recommend that you use a locally administered ESI for ease of management.

13.2.4 Configuring IPX to Use RFC 1483 Support

Configuring IPX routing is easy in the 2210 and 2216. The only parameters that need to be configured are the IPX network number and the desired connections to adjacent routers across the ATM network. The following section shows these configuration steps. While the 2216 configuration program has been used in our example, the screens for the 2210 program are identical. (Examples of configuring IPX using the command line can be found in 14.3, “Implementing Scenario 3” on page 386.)

Before configuring IPX over RFC 1483 connections, the following steps must be performed:

1. For the 2216, the ATM adapter has to be added to the configuration.

   This procedure is done under slots in the Navigation Window and is shown in 11.7.1, “Configuring an ATM Interface” on page 305.

2. Configure the ATM interface.

   This procedure is done under Interfaces in the Navigation Window and is described in detail in 11.7.1, “Configuring an ATM Interface” on page 305.

To configure IPX routing, from the configuration program main notebook page, select **General** from under the IPX line. Figure 182 is displayed.

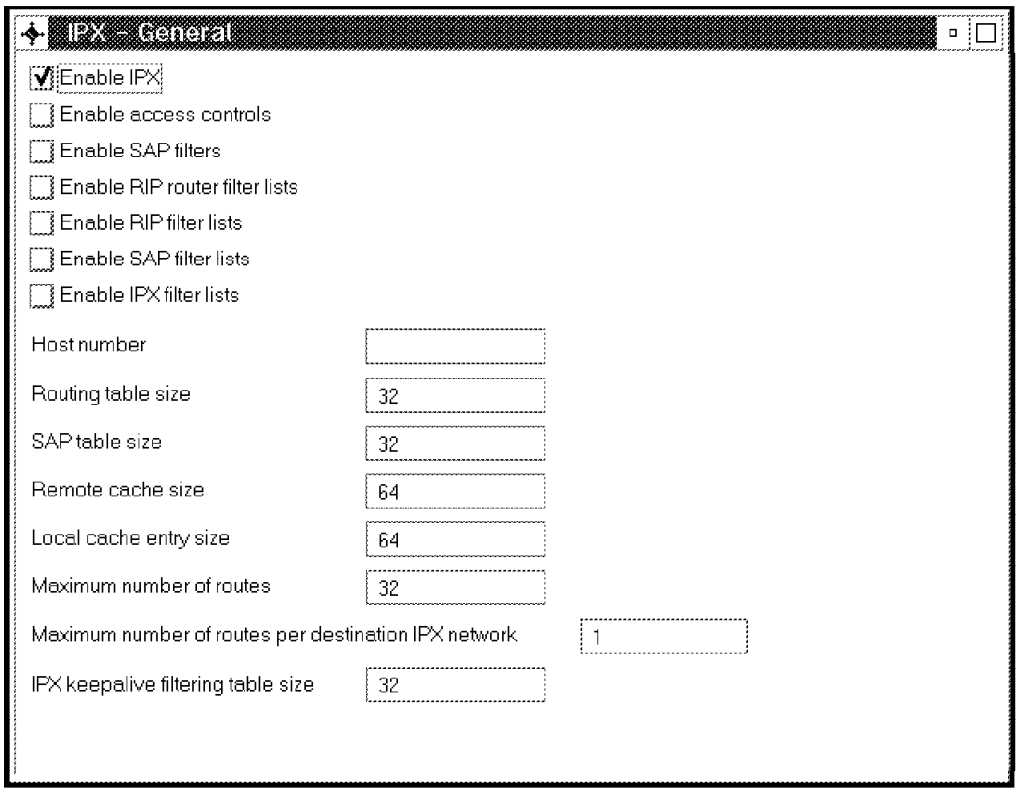


Figure 182. Enabling IPX on the Router

Check the **Enable IPX** box to enable IPX routing on the router as a whole.

Once IPX has been enabled, select **Interfaces** from the Navigation Window. Figure 183 will appear allowing IPX to be configured on an interface.

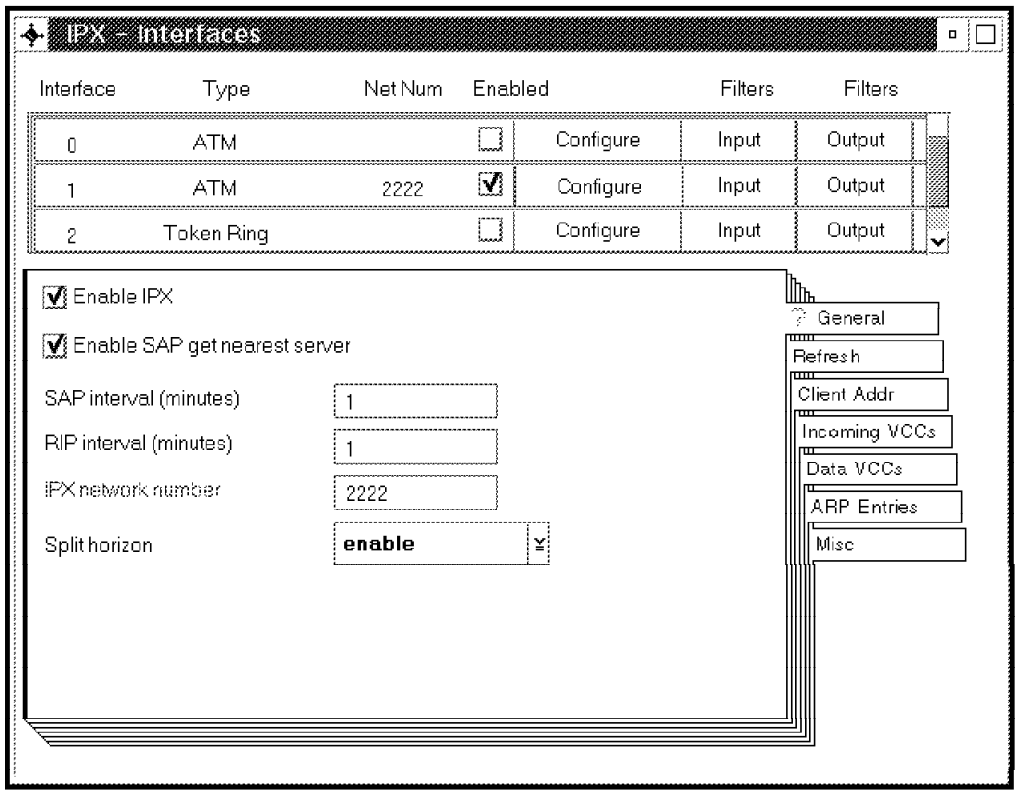


Figure 183. Enabling IPX on the ATM Interface

Select **ATM** from the list of interfaces at the top of the screen. Then, enter the IPX network number and check the **Enable IPX** box in order to enable IPX on this interface.

Note: The IPX split horizon option should be disabled when the 2210 or 2216 is going to perform intermediate routing between a set of adjacent routers that are reached through the same interface and there is not a fully meshed connection between all of the routers. Split horizon need not be disabled when the IPX router interconnection is a full mesh.

Next, select the **Client Addr** tab. Figure 184 on page 338 is displayed. From here, you can choose an ESI from the drop-down list. This list of ESIs was created when the ATM interface was created. We recommend using locally administered ESIs for ease of management.

As discussed previously, It is not necessary to assign a selector if you use a PVC connection to the other routers across the ATM network. If a static SVC is used, a selector must be assigned so that the full destination ATM address is known. This ATM address will be specified when configuring the SVC at the calling router.

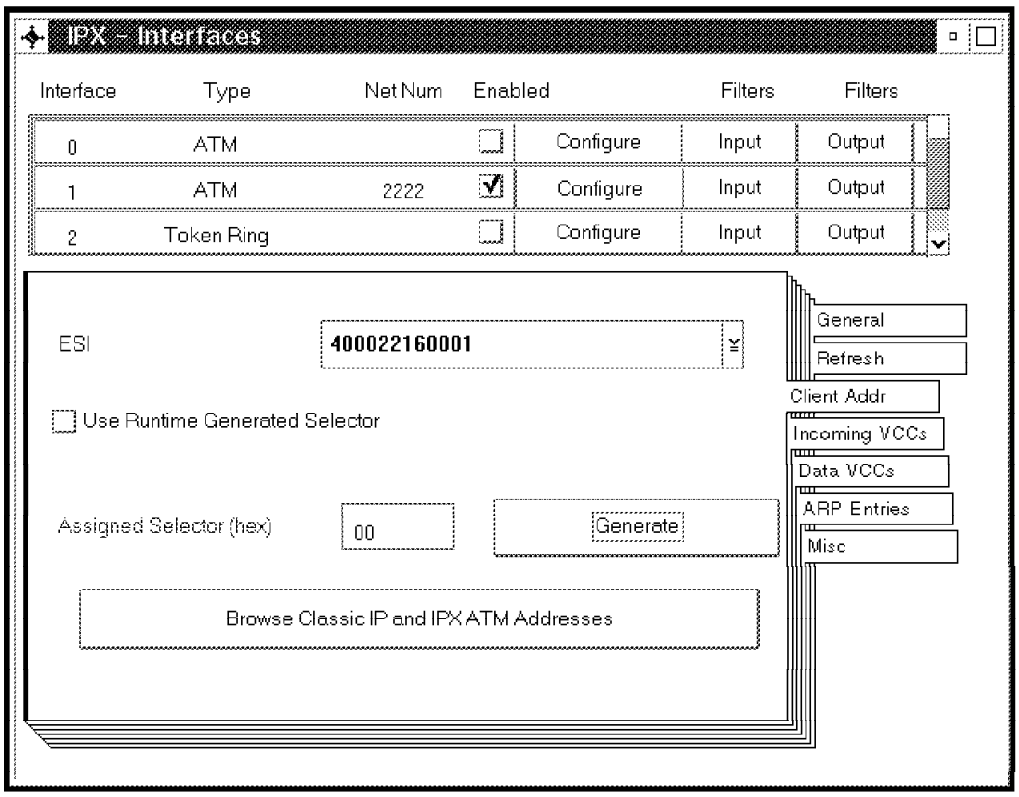


Figure 184. ESI and Selector Configuration

The next step required to configure IPX over ATM is to define the PVC and SVC connections to neighboring routers. These are implemented the same as for Classical IP and are shown in Figure 185 on page 339. More details on configuring PVCs and SVCs can be found in 12.9.3, “LIS Client Using PVCs” on page 328 or 12.9.4, “LIS Client Using Static SVCs” on page 330 respectively.

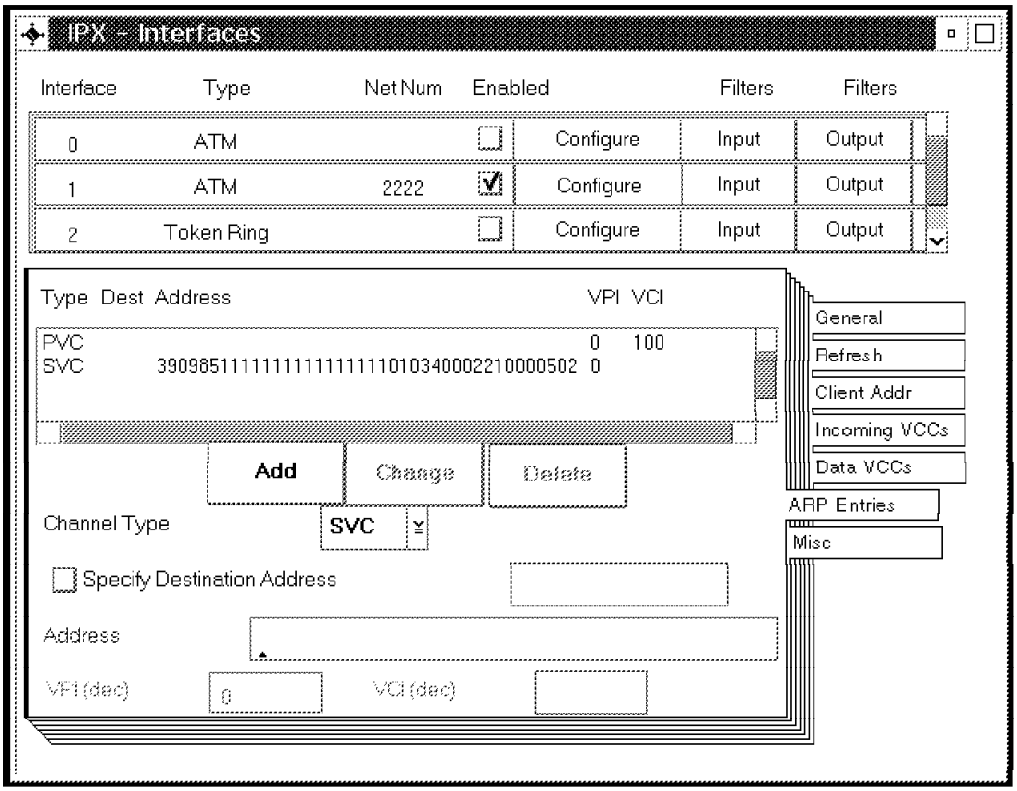


Figure 185. Configuring PVCs and SVCs

This completes the configuration of IPX over ATM, as default values can be taken for the remaining screens.

13.2.4.1 Configuring IPX over LAN Emulation

To configure IPX over LAN emulation, select the LEC to be configured from the list of interfaces at the top of the notebook page. For example, if a token-ring LEC is selected for configuration, Figure 186 on page 340 will appear.

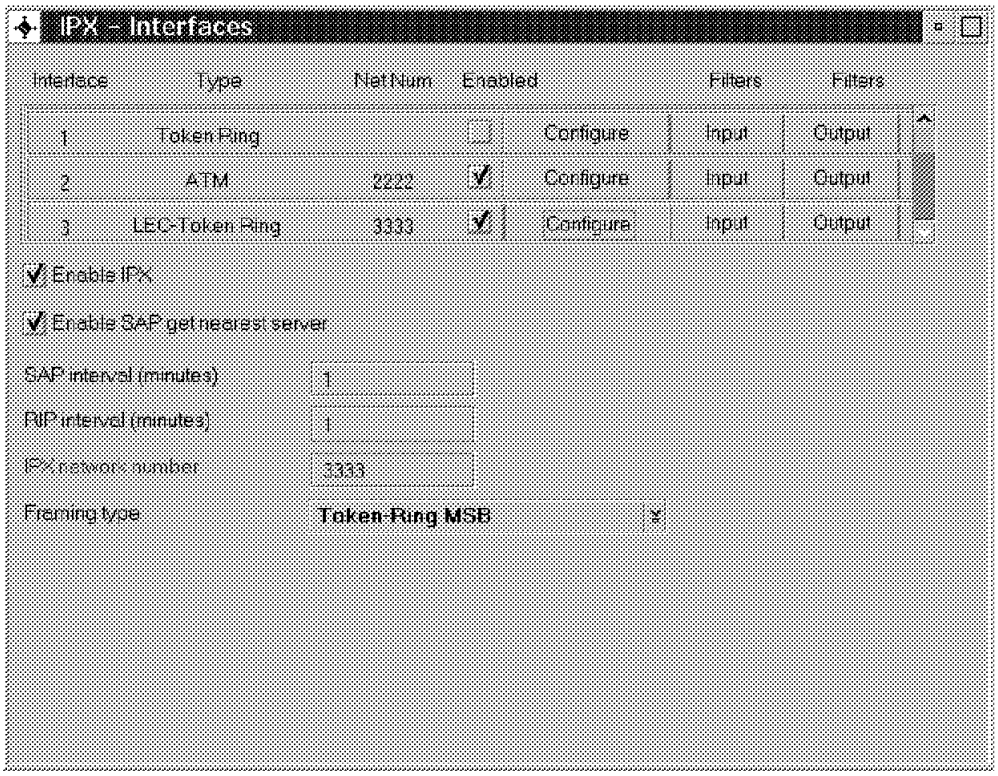


Figure 186. IPX Configuration for LAN Emulation

From here, it is very simple. Check the **Enable IPX** check box to enable IPX on this interface. Then enter the IPX Network Number and select the desired Framing Type from the drop-down list.

13.2.5 APPN Routing

Figure 187 depicts the APPN routing support in Nways MRS and Nways MAS V1.0.

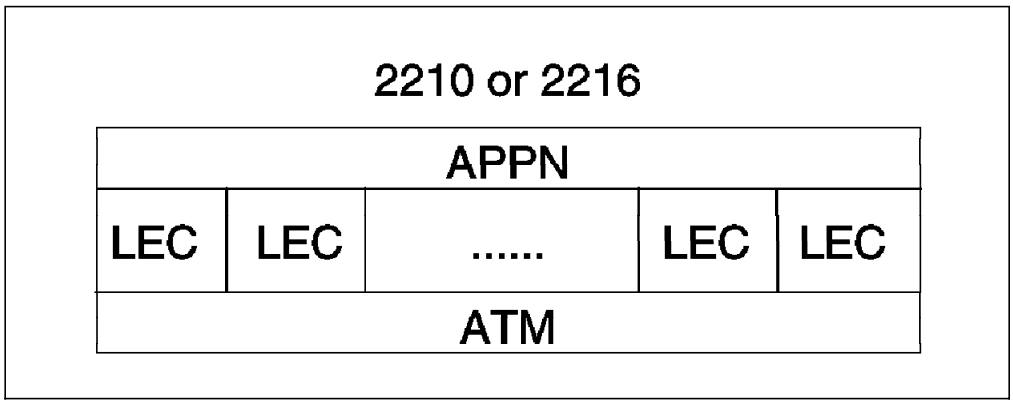


Figure 187. APPN Routing in the 2210 and 2216

In Version 1.0, APPN routing is only supported over LAN emulation. If SNA over RFC 1483 connections becomes supported in future releases, then APPN will also be routable over these connections as well.

Today, if SNA traffic needs to be carried over ATM without LAN emulation, then DLSw can be used. DLSw uses IP encapsulation and as mentioned, IP is supported over ATM. APPN routing is only supported over LAN emulation.

13.3 Bridging Overview

This section details the bridging support provided by the 2210 and 2216 on LAN emulation. The technique for configuring bridging over ATM is the same as for legacy LANs and therefore isn't outlined in this section. More detail on the bridging function provided and how to configure it is given in *Description and Configuration Scenarios Volume I*.

The 2210 and 2216 support bridging over emulated Ethernet and token-ring interfaces, as illustrated in Figure 188. The operational characteristics of bridging over these interfaces are identical to those over real interfaces. Emulated interfaces have interface numbers and bridge port numbers. Each bridge port will have a particular behavior and the bridge will have an overall behavior.

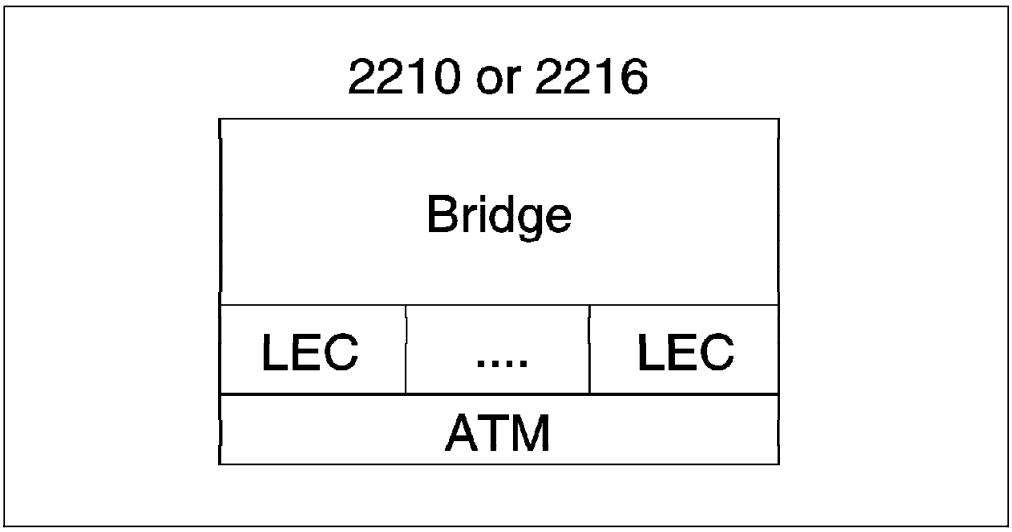


Figure 188. Bridging over Emulated LAN Interfaces

Three port-level bridging modes are available:

- Transparent Bridging (TB)
- Source Route Bridging (SRB)
- Source Route Transparent Bridging (SRT) which supports both SR and TB bridging simultaneously

Emulated Ethernet ports only support TB. Emulated token-ring ports support all three modes.

There are six box-level bridging behaviors:

- Pure TB

  This behavior is activated when all bridge ports are in TB mode. In pure TB mode, the 2210 or 2216 only acts as a transparent bridge and the IEEE 802.1d Spanning Tree algorithm is used.

- Pure SR

This behavior is activated when all bridge ports are in SR mode. In pure SR mode the 2210 or 2216 only acts as a source route bridge and the IBM Source Route Bridging Spanning Tree algorithm is used.

- SR and TB

  SR and TB behavior is activated when at least one bridge port is in SR mode, at least one bridge port is in TB mode, no bridge ports are in SRT mode and SR-TB translation is disabled. In SR and TB mode, the 2210 or 2216 acts as both a transparent bridge and a source route bridge simultaneously, but the two types of bridges don't work together and are, thus, isolated from each other. The IEEE 802.1d and IBM Source Route Spanning Tree algorithms are used independently in SRB and TB mode.

- SR-TB

  The SR-TB bridging mode differs from SR and TB in that SR-TB translation is enabled. In SR-TB mode, the bridges are no longer independent and frames are translated between the two bridges. SR-TB translation is only supported for SNA and NetBIOS protocols.

- SRT

  SRT behavior is activated when at least one bridge port is in SRT mode and SR-TB translation is not enabled. In SRT mode, the bridges are independent, as in SR and TB mode, but only the IEEE 802.1d Spanning Tree algorithm is used.

- Adaptive SRT (ASRT)

  The ASRT bridging mode differs from SRT in that SR-TB translation is enabled. Given the port behaviors, only one additional configuration parameter for enabling or disabling SR-TB translation is required to determine the box-level bridging function.

When a LEC is acting as a bridge port it joins the ELAN as a proxy and registers its MAC address, regardless of the bridging mode. If the port-level bridging mode is SR or SRT, a route descriptor is also registered with the LES. The LEC will always answer LE_ARP_REQUESTs for LAN destinations that it has registered. Additionally, if transparent bridging is enabled on the port, the LEC will respond to LE_ARP_REQUESTs when the target MAC address is in the TB database.

Chapter 14. ATM Scenarios

This section shows examples of configuring the required parameters on the IBM 2216 and the IBM 2210 for routing and bridging across ATM using LAN emulation clients (LECs) and Classical IP clients (CIPs) in the routers. Step-by-step configuration procedures are presented for three commonly expected scenarios:

1. Routing and bridging between emulated token-ring and Ethernet segments to legacy LAN segments, both directly attached and over leased line connections (see 14.1, “Implementing Scenario 1”).
2. Routing between emulated token-ring and Ethernet LAN segments over a frame relay connection (see 14.2, “Implementing Scenario 2” on page 358).
3. Routing between legacy LAN segments over an ATM backbone using both ATM Forum-compliant LAN Emulation and Classical IP (see 14.3, “Implementing Scenario 3” on page 386).

These scenarios are implemented using a variety of IBM 2210 and IBM 2216 configurations.

14.1 Implementing Scenario 1

Scenario 1 is shown in Figure 189. It uses the ATM LEC function of the 2216 to route between token-ring and Ethernet ELANs as well as legacy token-ring segments. It also includes routing and bridging over a PPP connection to a legacy LAN segment on an IBM 2210.

We purposely do not use an MSS to emphasize that the 2210/16 can route between ELANs like the MSS. The 2216 and 2210 are set up to route IP and IPX. In this scenario, OSPF is used as the routing protocol for IP.

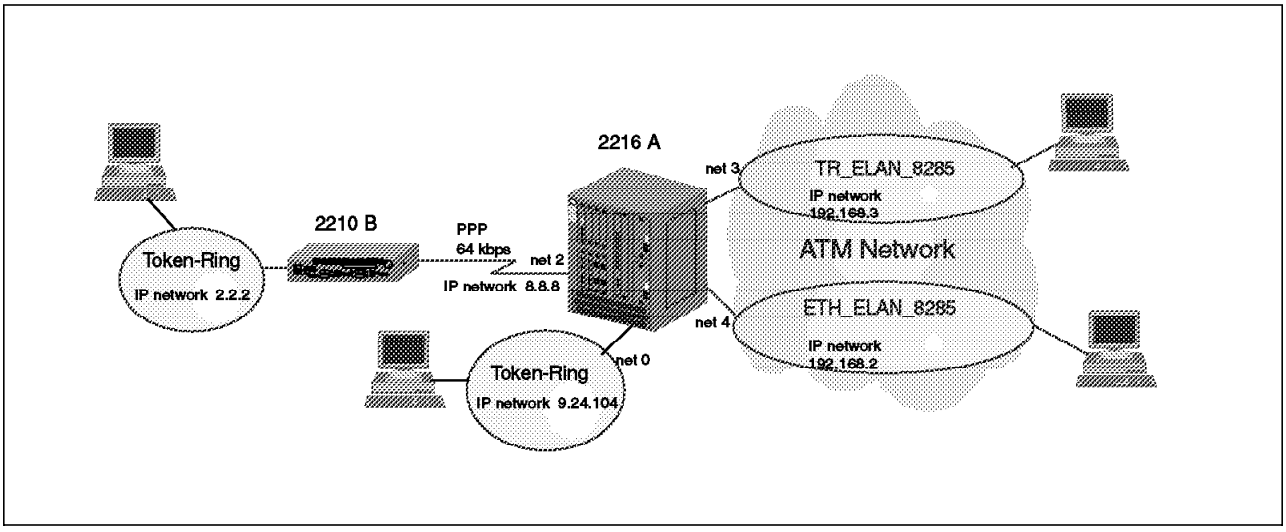


Figure 189. Scenario 1

The steps necessary for configuring the 2216 for scenario 1 are presented in the sections below. The outline of the process is as follows:

1. Add the hardware interfaces
2. Configure the hardware interfaces
3. Configure the protocols
4. Save the configuration and restart the router

Please refer to Figure 189 on page 343 as you perform these steps.

Note: The steps necessary to configure the 2210 for this scenario are not shown here because there is nothing relative to ATM to configure.

14.1.1 Adding the Hardware Interfaces

Note: The order of adding the following interfaces is arbitrary. You do not have to use the same order. However, if you use a different order, the network numbers for your interfaces will be different from those shown in these examples.

First add the interface for the legacy token-ring LAN segment that the 2216 attaches to. The basic configuration sequence for this scenario is shown in Figure 190. For more information on configuring token-ring, please see the *Nways Multiprotocol Access Services Software User's Guide*. These steps are performed from the talk 6 menu at the 2216 console.

```
Config (only)>add dev tok
Device Slot #(1-8) [1]? 1
Device Port #(1-2) [1]? 1
Adding token-ring device in slot 1  port 1 as interface #0
Use "net 0" to configure token-ring parameters
```

Figure 190. Adding a Legacy Token-Ring Interface

Next, add the ATM device itself. The configuration sequence is shown in Figure 191.

```
Config (only)>add dev atm
Device Slot #(1-8) [1]? 4
Adding CHARM ATM device in slot 4  port 1 as interface #1
Use "net 1" to configure CHARM ATM parameters
```

Figure 191. Adding an ATM Adapter

Next add the serial interface for the V.24 connection. The basic configuration sequence for this scenario is shown in Figure 192 on page 345. For more information on configuring serial interfaces, please see the *Nways Multiprotocol Access Services Software User's Guide*.

```
Config (only)>add dev eia
Device Slot #(1-8) [1]? 8
Device Port #(0-7) [0]? 0
Defaulting Data-link protocol to PPP
Adding EIA-232E/V.24 PPP device in slot 8  port 0 as interface #2
Use "set data-link" command to change the data-link protocol
Use "net 2" to configure EIA-232E/V.24 PPP parameters
```

Figure 192. Adding a Serial Interface

If you have performed these steps correctly, you will be able to list the devices and they will appear similar to those shown in Figure 193. Your slot and port numbers may be different, depending on where you installed the adapters in the 2216.

```
Config (only)>list dev
Ifc 0 Token Ring                    Slot: 1  Port: 1
Ifc 1 CHARM ATM                     Slot: 4  Port: 1
Ifc 2 EIA-232E/V.24 PPP             Slot: 8  Port: 0
```

Figure 193. Listing the Installed Devices

14.1.2 Configuring the Interfaces

In this step, you will configure the interface parameters associated with devices installed above. These steps are also performed from the talk 6 menu.

First configure the token-ring interface (net0). Depending upon your desired configuration, the default parameters may be adequate. This is the case in implementing this example scenario. The defaults are shown in Figure 194. For more information on configuring token-ring, please see the *Nways Multiprotocol Access Services Software User's Guide*.

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

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Shielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
IPX interface configuration record missing

TKR config>exit
```

Figure 194. Configuring the Token-Ring Interface Parameters

Next, configure the serial interface between the two routers. In this scenario, the default parameters are acceptable. These are shown in Figure 195 on page 346.

Note: The configuration of this serial PPP link is totally transparent to the fact that traffic passing through it came from an ATM network.

```
Config (only)>net 2
Point-to-Point user configuration
PPP Config>list all
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Speed (bps): 19200

Transmit Delay Counter: 0
Lower DTR: Disabled


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

LCP Options
-----------
Max Receive Unit:           2048   Magic Number:                   Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):   No   Addr/Cntl Field Comp(ACFC):        No
```

Figure 195. Listing the Default Parameters for the Serial Interface

The next screen is shown in Figure 196.

```
Authentication Options
        ----------------------
Authenticate remote using:  none
        Identify self as:   ibm


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


CCP Options
        -----------
        Data Compression disabled
        Algorithm list: none


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

Figure 196. Listing the Default Parameters for the Serial Interface

Next, configure the ATM interface. The configuration sequence is shown in Figure 197 on page 347.

The ESI added here is used for both LEC and CIP clients. The LEC and CIP clients use the network prefix from the switch and the ESI defined here along with a unique selector byte as their ATM address.

Note: There is no command when configuring the LEC and CIP clients to add another ESI. That can only be done while configuring the ATM interface. Therefore it is important that you have decided on your ATM network structure and addressing before you begin configuring the ATM interface.

The command set uni auto sets the UNI version to auto-detection. For information on the ILMI process and how the UNI version is chosen during initialization see 11.5.1, “Overview of ILMI Functions” on page 294.

```
Config (only)>net 1
ATM user configuration
ATM Config>interface
ATM interface configuration
ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? 40.00.22.16.00.01
ATM Interface Config>set uni auto
```

Figure 197. Configuring the ATM Interface

If you have performed these steps correctly, you should be able to list the ATM configuration and see a screen similar to the one in Figure 198. Note that you need to do both a list conf and a list esi to verify all of the parameters you just entered.

```
ATM Interface Config>list conf

                         ATM Configuration


  Interface (net) number =    1
  Maximum VCC data rate Mbps   =     155
  Maximum frame size     = 9234
  Maximum number of callers =  209
  Maximum number of calls = 1024
  Maximum number of parties to a multipoint call =  512
  Maximum number of Selectors that can be configured  =  200
  UNI Version = AUTO
  Packet trace = OFF
ATM Interface Config>list esi

          ESI         Enabled
  -----------------   -------
  40.00.22.16.00.01       YES

ATM Interface Config>exit
```

Figure 198. Listing the ATM Interface

Now, add the logical interfaces for the two emulated LANs connecting to the 2216. In our scenario, we have both a token-ring and an Ethernet emulated LAN. It is necessary to add an interface for each. Note that the router gives each a unique interface number even though the traffic for both will cross the same ATM interface. In effect, these logical interfaces look and act just like two separate hardware interfaces. The sequence for adding the LECs is shown in Figure 199.

```
ATM Config>le-client
ATM LAN Emulation Clients configuration
LE Client config>add tok
Added Emulated LAN as interface 3
LE Client config>add eth
Added Emulated LAN as interface 4
```

Figure 199. Adding Logical Interfaces for the Emulated LANs

Next, configure the LAN emulation clients for each of the logical interfaces that you just defined. The sequence for the token-ring LEC interface is shown in Figure 200 on page 349.

Please note the following when configuring the LECs:

Notes:

1. The set esi address is used to select an already defined End System Identifier (ESI) to be used for this interface. The definition was done in the previous step when the ATM interface was defined.
2. For this scenario, you need to have the ATM address of the LAN Emulation Server (LES) for the ELAN that the LEC will join before proceeding. Since we are not using an MSS server and its associated LAN Emulation Configuration Server (LECS), it is necessary to hard code the address of the LES into the LEC configuration. This way, when the LEC is ready to join the ELAN, it will already know what the address of its LES is and will not need to use the LECS to find it.
3. You must set the LECS auto configuration to no before you can configure the ATM address of the LES.
4. Setting the ELAN name is not necessary *for this scenario* but it is shown as an example. If you are using a LECS in your system that is using an ELAN name policy and has more than one token-ring LES defined, then you will need to set the ELAN name. In this case, setting the ELAN name allows you to attach to a specific ELAN. Otherwise, a LEC going through the ILMI procedure may be assigned to any of the token-ring LESs, which might not be the desired ELAN.
5. The ELAN name is case sensitive. If not typed in correctly, the interface will not come up to an operational state.

```
LE Client config>conf 3
ATM LAN Emulation Client configuration
Token-Ring Forum-Compliant LEC Config>set elan
Assign emulated LAN name []? TR_ELAN_8285

Token-Ring Forum-Compliant LEC Config>set esi
Select ESI
   (1) Use burned in ESI
   (2) 40.00.22.16.00.01

Enter selection [1]? 2
Token-Ring Forum-Compliant LEC Config>set auto
Do LECS auto configuration? [Yes]: no
Token-Ring Forum-Compliant LEC Config>set les
LES ATM address in 00.00.00.00.00.00:... form []?
39.09.85.11.11.11.11.11.11.11.11.01.03.40.00.00.82.85.a1.03

Token-Ring Forum-Compliant LEC Config>set mac
Use adapter address for MAC? [Yes]: n
MAC address [00.00.00.00.00.00]? 40.00.22.16.00.03
```

Figure 200. Configuring the LEC on the Emulated Token-Ring

The sequence for the Ethernet interface is shown in Figure 201. Note that you must set the LECS auto configuration to no before you can configure the ATM address of the LES. Otherwise, the order of the set statements is not significant.

```
LE Client config>conf 4
ATM LAN Emulation Client configuration
Ethernet Forum Compliant LEC Config>set auto
Do LECS auto configuration? [Yes]: no
Ethernet Forum Compliant LEC Config>set les
LES ATM address in 00.00.00.00.00.00:... form []?
39.09.85.11.11.11.11.11.11.11.11.01.03.40.00.00.82.85.a1.02
Ethernet Forum Compliant LEC Config>set elan
Assign emulated LAN name []? ETH_ELAN_8285
Ethernet Forum Compliant LEC Config>set esi
Select ESI
   (1) Use burned in ESI
   (2) 40.00.22.16.00.01

Enter selection [1]? 2
Ethernet Forum Compliant LEC Config>set mac
Use adapter address for MAC? [Yes]: n
MAC address [00.00.00.00.00.00]? 40.00.22.16.00.04
```

Figure 201. Configuring the LEC on the Emulated Ethernet

One other option for the Ethernet LEC that is not shown but is worth mentioning is the IP-Encapsulation format. This parameter sets the Ethernet frame type for IP encapsulation. The two options are Ethernet DIX or IEEE 802.3 and it should be set to the frame type used by the rest of your Ethernet network. For example, if the other LE clients on the ELAN are using IEEE 802.3 frame format, you will need to set the LEC frame format to IEEE 802.3 or the router will be unable to recognize the frames. The default setting for a LEC on the 2210 or 2216 is Ethernet DIX.

If you have performed these steps correctly, you should be able to list the LEC configuration and see a screen similar to the one shown in Figure 202 on page 350 which shows the configuration for the Ethernet LAN emulation client.

```
 Ethernet Forum Compliant LEC Config>list

                  ATM LEC Configuration

    ATM interface number             = 1
    LEC interface number             = 4
    LECS auto configuration          = No

    C1: Primary ATM address
           ESI address               = 40.00.22.16.00.01
           Selector byte             = 0x2
    C2: Emulated LAN type            = Ethernet
    C3: Maximum frame size           = 1516
    C5: Emulated LAN name            = ETH_ELAN_8285
    C6: LE Client MAC address        = 40.00.22.16.00.04
    C7: Control timeout              = 30
    C9: LE Server ATM address        = 39.09.85.11.11.11.11.11.11.11.11.
01.01.40.00.00.82.85.a1.02
   C10: Maximum unknown count        = 1
   C11: Maximum unknown time         = 1
   C12: VCC timeout period           = 1200
   C13: Maximum retry count          = 1
   C17: Aging time                   = 300
   C18: Forward delay time           = 15
   C20: LE ARP response time         = 1
   C21: Flush timeout                = 4
   C22: Path switch delay            = 6
   C24: Multicast send VCC type      = Best-Effort
   C25: Multicast send VCC avg rate  = 25000
   C26: Multicast send VCC peak rate = 25000
   C28: Connection completion timer  = 4

    LE ARP queue depth               = 5
    LE ARP cache size                = 10
    Best effort peak rate            = 25000
    Maximum config retries           = 3
    Packet trace                     = No
    No IPX interface configuration
    IP Encapsulation                 = ETHER
 Ethernet Forum Compliant LEC Config>exit
```

Figure 202. Listing the Ethernet LEC

Now, list the LEC configuration. You should have both an Ethernet and a token-ring ELAN and they should look like those in Figure 203 on page 351.

```
LE Client config>list

   ATM Forum Compliant Emulated LANs
-------------------------------------------------------
  Physical ATM interface number = 1
  LEC interface number = 3
  Emulated LAN type    = Token-Ring Forum-Compliant
  Emulated LAN name    = TR_ELAN_8285
-------------------------------------------------------
  Physical ATM interface number = 1
  LEC interface number = 4
  Emulated LAN type    = Ethernet Forum Compliant
  Emulated LAN name    = ETH_ELAN_8285
LE Client config>exit
ATM Config>exit
```

Figure 203. Listing the Configured LECs on the ATM Interface

This completes the configuration of the physical and logical interfaces.

14.1.3 Configuring the Protocols

The next step is to configure the IP, IPX, and SNA protocols. These steps are performed from the talk 6 menu at the 2216 console. Please refer to Figure 189 on page 343 as you perform these steps.

Note

The configuration of the protocols is the same whether you're on an ELAN or a legacy LAN segment. We show the configuration here for scenario 1 just for completeness.

First, configure IP. The basic configuration sequence for this scenario is shown in Figure 204 on page 352. For more information on configuring IP, please see the 2216 Protocol Configuration and Monitoring Reference, Volume 1. The router ID is needed as OSPF is used as the routing protocol. This is explained further in the *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume I*, SG24-4957.

```
Config (only)>protocol ip
Internet protocol user configuration
IP config>add addr
Which net is this address for [0]?
New address [0.0.0.0]? 9.24.104.202
Address mask [255.0.0.0]? 255.255.255.0
IP config>add addr
Which net is this address for [0]? 2
New address [0.0.0.0]? 8.8.8.216
Address mask [255.0.0.0]? 255.255.255.0
IP config>add addr 3
New address [0.0.0.0]? 192.168.3.216
Address mask [255.255.255.0]?
IP config>add addr 4
New address [0.0.0.0]? 192.168.2.216
Address mask [255.255.255.0]?
IP config>set router-id
Router-ID [0.0.0.0]? 10.10.10.216
```

Figure 204. Adding IP Addresses to Physical Interfaces

If you have performed these steps correctly, you will be able to list the IP addresses and you will see a result similar to that depicted in Figure 205.

```
IP config>list addr
IP addresses for each interface:
 intf  0   9.24.104.202     255.255.255.0  Local wire broadcast, fill 1
 intf  2   8.8.8.216        255.255.255.0  Local wire broadcast, fill 1
 intf  3   192.168.3.216    255.255.255.0  Local wire broadcast, fill 1
 intf  4   192.168.2.216    255.255.255.0  Local wire broadcast, fill 1
IP config>exit
```

Figure 205. Listing the IP Addresses for Each Configured Interface

This completes the configuration of IP for this scenario.

Next, enable OSPF as the routing protocol for the 2216. This sequence is shown in Figure 206.

```
Config (only)>p ospf
Open SPF-Based Routing Protocol configuration console

OSPF Config>enab ospf
Estimated # external routes [0]? 1000
Estimated # OSPF routers [0]? 40
```

Figure 206. Enabling OSPF on the 2216

Next, configure OSPF for each interface. The configuration sequence for the legacy token-ring segment is shown in Figure 207 on page 353. Note that for this scenario, the default parameters are usable. The only OSPF parameter to set is the IP address associated for this interface. For more information on

configuring OSPF, please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
OSPF Config>set int 0
Interface IP address [0.0.0.0]? 9.24.104.203
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
OSPF Config>exit
```

Figure 207. Configuring OSPF for an IP Interface

Complete the OSPF configuration for the other interfaces, taking care to specify the correct IP address for each interface.

This completes the OSPF configuration.

Next, configure IPX. The first step is to enable IPX on the router globally, followed by enabling it on each of the interfaces that we want to route IPX over. This step includes assigning the IPX network number to each interface. The configuration sequence is shown in Figure 208.

```
Config>protocol ipx
IPX protocol user configuration
IPX config>enable ipx

IPX config>enable interface 0
Configure an IPX network number for this interface.
Network number in hex [1]? 9
IPX config>enable interface 2
Configure an IPX network number for this interface.
Network number in hex [1]? 8888
IPX config>enable interface 3
Configure an IPX network number for this interface.
Network number in hex [1]? 3333
IPX config>enable interface 4
Configure an IPX network number for this interface.
Network number in hex [1]? 2222
```

Figure 208. Enabling IPX and Assigning IPX Network Numbers

The next step is to set a host number for the serial link. IPX routing is based on a network number and a MAC address. Since serial interfaces do not have a MAC address, the host number is used to completely specify the correct interface to route to.

The configuration sequence is shown in Figure 209 on page 354.

```
IPX config>set host-number
Host number for serial lines (in hex)[]? 400022160002
IPX config>set max ser
New Service table size [32]? 64
IPX config>set max net
New Network table size [32]? 64
```

Figure 209. Setting an IPX Host Number for a Serial Link

Important

When IPX is enabled on the LEC interfaces, default NetWare IPX frame types are added to the LEC configuration. The default values are:

- Ethernet 802.3 for the Ethernet LEC.
- Token-Ring MSB for the token-ring LEC.

If you want to change these default values you need to go back to the LEC configuration prompt and use the `frame` command to specify the correct frame type.

In our testing, we encountered a problem where we intermittently could not route IPX over all ports. We discovered that we had more IPX services on our network than could be held in the router's table. The router parameter `maximum services` is the one that controls this and it defaults to a value of 32. In our lab environment, we had more than 32 IPX servers. Every time we tried to reach a server that was not in the table, we were unsuccessful because the server was not in the router's services table. When we increased the `maximum services` value from 32 to 64, the problems disappeared.

You can check this from the talk 5 menus with the following commands:

```
protocol ipx
slist
```

14.1.4 Saving the Configuration and Restarting the Router

When all configuration steps have been completed, save your configuration and then restart the router. The procedure to do this is shown in Figure 210.

```
Config (only)>write
Config Save: Using bank A and config number 2
Config (only)>reload
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 210. Saving the Configuration and Restarting the Router

14.1.5 Monitoring the Router Activity

After the router restarts with the new configuration, you should use the talk 5 menus to check that the interfaces are working properly. Figure 211 shows a configuration listing. You can use the +conf command to see the details of any interface and to see what interfaces are up or down.

```
+conf

Multiprotocol Access Services
5765-B87 Feature 2802 V1 R1.0 PTF 0 RPQ 0 MAS.A01 cc1_11b

Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
7   IPX   NetWare IPX
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol

Num Name  Feature
2   MCF   MAC Filtering

5 Networks:
Net Interface  MAC/Data-Link         Hardware                    State
0   TKR/0      Token-Ring/802.5      Token-Ring                  Up
1   ATM/0      ATM                   CHARM ATM                   Up
2   PPP/0      Point to Point        EIA-232E/V.24               Up
3   TKR/1      Token-Ring/802.5      CHARM ATM                   Up
4   Eth/0      Ethernet/IEEE 802.3   CHARM ATM                   Up
```

Figure 211. Viewing the Status of the Interfaces

Figure 212 shows an IPX dump. You can use the +p ipx and dump commands to list the IPX networks that the router knows about. This list includes the networks directly attached and ones learned using the RIP protocol.

```
+p ipx
IPX>dump

10 route entries used out of 32
10 net entries used out of 32

Type     Dest net Hops Delay  Age(M:S)   via Router
 Dir       3333    0     1      0: 0       3333/400022160003 3-TKR/1
 Dir       2222    0     1      0: 0       2222/400022160004 4-Eth/0
 Dir          9    0     1      0: 0          9/08005AFE0188 0-TKR/0
 Dir       8888    0     5      0: 0       8888/400022160002 2-PPP/0
 RIP         10    1     2      0:50          9/08005ACE6D99
 RIP   30AA0F92    1     2      0:45          9/400052005240
 RIP   31ECF1DD    1     2      0:35          9/08005A0D2860
 RIP   325521DE    1     2      0: 5       2222/08005A998151
 Old   857A7D6D   16     2      3:45          9/08005AB96860
 RIP   D6CA61D7    1     2      0:55          9/08005ACE6D99
```

Figure 212. Displaying an IPX Dump

Figure 213 on page 356 shows an IPX SLIST. The list shows the NetWare services that the 2216 is aware of, in this case 26. In this scenario, with the maximum services parameter set to 64, there is space for 38 more entries.

```
*talk 5
+protocol ipx
IPX>slist
State Typ Service Name                Hops Age     Net  /   Host     /Sock
 SAP 0278 DIRECTORY_TREE_______________ 2  0:40 325521DE/000000000001/4006
 SAP 026B DIRECTORY_TREE_______________ 2  0:40 325521DE/000000000001/0005
 SAP 0004 NW_MSS                       2  0:40 325521DE/000000000001/0451
 SAP 0751 If_changing_conf._please_tel 1  0:10        9/0001CB92FE09/4004
 SAP 0107 MANSERV1                     1  0:20 30AA0F92/000000000001/8104
 SAP 0004 MANSERV1                     1  0:20 30AA0F92/000000000001/0451
 SAP 004B BSER4.00-6.10_30AA0F92000000 1  0:20 30AA0F92/000000000001/8059
 SAP 0102 ISMANSERV11841501800000020   1  0:20 30AA0F92/000000000001/400D
 SAP 0102 IVMANSERV11841501800000020   1  0:20 30AA0F92/000000000001/400F
 SAP 0102 LANPROTECT18415018920FAA3010 1  0:20 30AA0F92/000000000001/4010
 SAP 026B SYSMAN_______________________ 1  0:20 30AA0F92/000000000001/0005
 SAP 0751 IBM8235_A2470E               1  0:25        9/0001CBA2470E/4004
 SAP 0751 IBM8235_32C00A               1  0:35        9/0001CB32C00A/4004
 SAP 0278 SYSMAN_______________________ 1  0:20 30AA0F92/000000000001/4006
 SAP 0640 TME10-SRV1                   1  0:30        9/08005A0D2861/E885
 SAP 064E TME10-SRV1!!!!!A5569B20ABE51 1  0:30        9/08005A0D2861/4070
 SAP 064E CSNTSRV2!!!!!!!A5569B20ABE51 1  0:10        9/400052005138/4000
 SAP 064E WTR05285!!!!!!!A5569B20ABE51 1  0:10        9/400052005285/4000
 SAP 026B FERGUS_NW41_TREE_____________ 1  0: 5 31ECF1DD/000000000001/0005
 SAP 0107 FERGUS_NW41                  1  0: 5 31ECF1DD/000000000001/8104
 SAP 0004 FERGUS_NW41                  1  0: 5 31ECF1DD/000000000001/0451
 SAP 0278 FERGUS_NW41_TREE_____________ 1  0: 5 31ECF1DD/000000000001/4006
 SAP 0130 FERGUS_NW41                  1  0: 5 31ECF1DD/000000000001/1F80
 SAP 0115 FERGUS_NW41__________________ 1  0: 5 31ECF1DD/000000000001/1F80
 SAP 012B FERGUS_NW41__________________ 1  0: 5 31ECF1DD/000000000001/1F80
 SAP 05B3 FERGUS_NW41                  1  0: 5 31ECF1DD/000000000001/0000

26 entries used out of 64
```

Figure 213. Displaying the Entries in the Services Table

Figure 214 on page 357 shows an IP dump. You can use the +p ip and dump commands to list the IP networks that the router knows about. This list includes the networks directly attached and ones learned using an IP routing protocol. In this case the routing protocol used was OSPF.

```
+p ip
IP>dump
Type   Dest net         Mask      Cost     Age       Next hop(s)

Sbnt   8.0.0.0          FF000000  1        4127      None
 Dir*  8.8.8.0          FFFFFF00  1        4147      PPP/0
 SPF   8.8.8.210        FFFFFFFF  1        4147      8.8.8.210
 SPF   8.8.8.216        FFFFFFFF  2        4055      PPP/0
Sbnt   9.0.0.0          FF000000  1        4607      None
 SPF*  9.24.104.0       FFFFFF00  1        4612      TKR/0
 SPF*  192.168.2.0      FFFFFF00  1        4622      Eth/0
 SPF*  192.168.3.0      FFFFFF00  1        4626      TKR/1

Routing table size: 768 nets (49152 bytes), 8 nets known
IP>exit
```

Figure 214. Displaying an IP Dump

This completes the configuration steps necessary for implementing scenario 1.

14.2 Implementing Scenario 2

Scenario 2 is shown in Figure 215. It shows how to route between ELANs over a frame relay wide area connection. As in the first scenario, we purposely do not use an MSS to emphasize that the 2210 and 2216 can route and bridge between ELANs and legacy LANs.

The 2216 and 2210 are set up to route IP and IPX and bridge DLSw. RIP was used as the routing protocol for IP.

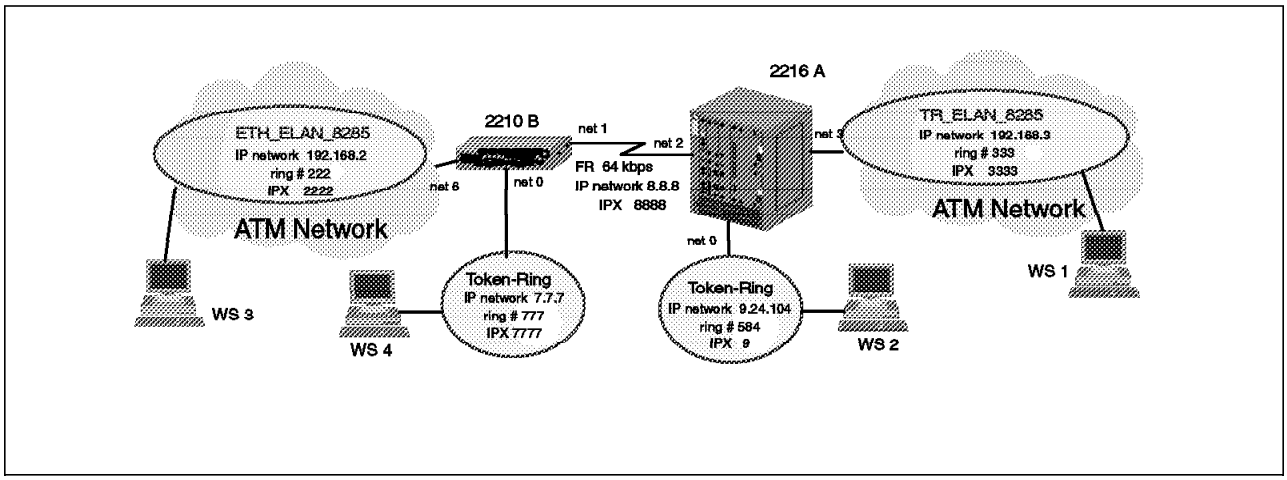


Figure 215. Scenario 2

The steps necessary for configuring the routers for scenario 2 are presented in the following sections. The outline of the process is as follows:

1. Configure the hardware interfaces
2. Configure the protocols
3. Save the configuration and restart the router

Note: In the case of the 2216, you have the additional step of adding the hardware interfaces.

We show the 2210 configuration first. Then the configuration of the 2216 is presented. Please refer to Figure 215 as you perform these steps.

14.2.1 Configuring the 2210 Hardware Interfaces

First, set the DLC for the serial port to frame relay. Then, configure the necessary frame relay parameters. The basic configuration sequence for this scenario is shown in Figure 216 on page 359. For more information on configuring frame relay, please see the *Nways Multiprotocol Routing Services Software User's Guide*.

```
Config>set data fra
Interface Number [0]? 1
Config>net 1
Frame Relay user configuration
FR Config>dis lmi
FR Config>add per
Circuit number [16]?
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []?
Is circuit required for interface operation [N]?
FR Config>set clock int
Must also set the line speed to a valid value
Line speed (2400 to 2048000) [0]? 64000
FR Config>set cable rs dce
FR Config>list hdlc

                        Frame Relay HDLC Configuration


  Encoding      = NRZ               IDLE                    = Flag
  Clocking      = Internal
  Cable type    = RS-232 DCE
  Line speed (bps)       = 64000    Interface MTU in bytes   = 2048
  Transmit delay         = 0
  Lower DTR              = Disabled
FR Config>exit
```

Figure 216. Configuring Frame Relay

Next, configure the token-ring interface. The basic configuration sequence for this scenario is shown in Figure 217. For more information on configuring a token-ring interface, please see the *Nways Multiprotocol Routing Services Software User's Guide*.

```
Config>net 0
Token-Ring interface configuration
TKR config>speed 4
TKR config>set phy 400022100000
TKR config>media sh
```

Figure 217. Configuring the Token-Ring Interface

If you have performed these steps correctly, you should be able to list the token-ring configuration and see a screen similar to the one in Figure 218 on page 360.

```
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Shielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              400022100000
IPX interface configuration record missing
TKR config>exit
```

Figure 218. Listing the Token-Ring Configuration

Note: In the figure above, notice that the IPX frame type has not been configured for the interface yet. When IPX is configured on the interface a default frame type of Token-Ring MSB is assigned. If you want to change the default value you will need to return to this token-ring interface configuration and change it, after IPX has been configured. You cannot change it at this stage, as IPX hasn't been configured yet. In this scenario we want to use the default so we don't go back and change the frame type.

Next, configure the ATM interface. The configuration sequence is shown in Figure 219.

The ESI added here is used for both LEC and CIP clients. The LEC and CIP clients use the network prefix from the switch and the ESI defined here along with a unique selector byte as their ATM address.

Note: There is no command when configuring the LEC and CIP clients to add another ESI. That can only be done while configuring the ATM interface. Therefore it is important that you have decided on your ATM network structure and addressing before you begin configuring the ATM interface.

The command set uni auto sets the UNI version to auto-detection. For information on the ILMI process and how the UNI version is chosen during initialization see 11.5.1, "Overview of ILMI Functions" on page 294.

```
Config>net 5
ATM user configuration
ATM Config>int
ATM interface configuration
ATM Interface Config>set uni auto
ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? 40.00.22.10.00.05
```

Figure 219. Configuring the ATM Interface

If you have performed these steps correctly, you should be able to list the ATM configuration and see a screen similar to the one in Figure 220 on page 361. Note that you need to do both a list conf and a list esi to verify all of the parameters you just entered.

```
ATM Interface Config>list con

                        ATM Configuration


  Interface (net) number =    5
  Maximum VCC data rate Mbps   =      25
  Maximum frame size     = 9234
  Maximum number of callers =  209
  Maximum number of calls = 1024
  Maximum number of parties to a multipoint call =  512
  Maximum number of Selectors that can be configured  =  200
  UNI Version = AUTO
  Packet trace = OFF
ATM Interface Config>list esi

          ESI         Enabled
  -----------------   -------
  40.00.22.10.00.05       YES

ATM Interface Config>exit
```

Figure 220. Listing the ATM Configuration

Next, add the LEC for the Ethernet ELAN and configure it. The configuration sequence is shown in Figure 221 on page 362.

Please note the following when configuring the LEC:

Notes:

1. The set esi address is used to select an already defined End System Identifier (ESI) to be used for this interface. The definition was done in the previous step when the ATM interface was defined.
2. For this scenario, you need to have the ATM address of the LAN Emulation Server (LES) for the ELAN that the LEC will join before proceeding. Since we are not using an MSS server and its associated LAN Emulation Configuration Server (LECS), it is necessary to hard code the address of the LES into the LEC configuration. This way, when the LEC is ready to join the ELAN, it will already know what the address of its LES is and will not need to use the LECS to find it.
3. You must set the LECS auto configuration to no before you can configure the ATM address of the LES.
4. Setting the ELAN name is not necessary *for this scenario* but it is shown as an example. If you are using a LECS in your system that is using an ELAN name policy and has more than one token-ring LES defined, then you will need to set the ELAN name. In this case, setting the ELAN name allows you to attach to a specific ELAN. Otherwise, a LEC going through the ILMI procedure may be assigned to any of the token-ring LESs, which might not be the desired ELAN.
5. The ELAN name is case sensitive. If not typed in correctly, the interface will not come up to an operational state.

```
ATM Config>le-c
ATM LAN Emulation Clients configuration
LE Client config>add eth
Added Emulated LAN as interface 6
LE Client config>conf 6
ATM LAN Emulation Client configuration
Ethernet Forum Compliant LEC Config>set auto
Do LECS auto configuration? [Yes]: no
Ethernet Forum Compliant LEC Config>set les
LES ATM address in 00.00.00.00.00.00:... form []? 39.09.85.11.11.11.11.11.11.11.
11.01.03.40.00.00.82.85.a1.02
Ethernet Forum Compliant LEC Config>set esi
Select ESI
   (1) Use burned in ESI
   (2) 40.00.22.10.00.05

Enter selection [1]? 2
Ethernet Forum Compliant LEC Config>set mac
Use adapter address for MAC? [Yes]: n
MAC address [00.00.00.00.00.00]? 40.00.22.10.00.06
```

Figure 221. Configuring the LEC

If you have performed these steps correctly, you should be able to list the configuration of the Ethernet LEC and see a screen similar to the one in Figure 222 on page 363.

```
Ethernet Forum Compliant LEC Config>list

                ATM LEC Configuration

   ATM interface number             = 5
   LEC interface number             = 6
   LECS auto configuration          = No

   C1: Primary ATM address
          ESI address               = 40.00.22.10.00.05
          Selector byte             = 0x2
   C2: Emulated LAN type            = Ethernet
   C3: Maximum frame size           = 1516
   C5: Emulated LAN name            =
   C6: LE Client MAC address        = 40.00.22.10.00.06
   C7: Control timeout              = 30
   C9: LE Server ATM address        = 39.09.85.11.11.11.11.11.11.11.11.01.03.40.
                                      00.00.82.85.A1.02
  C10: Maximum unknown count        = 1
  C11: Maximum unknown time         = 1
  C12: VCC timeout period           = 1200
  C13: Maximum retry count          = 1
  C17: Aging time                   = 300
  C18: Forward delay time           = 15
  C20: LE ARP response time         = 1
  C21: Flush timeout                = 4
  C22: Path switch delay            = 6
  C24: Multicast send VCC type      = Best-Effort
  C25: Multicast send VCC avg rate  = 25000
  C26: Multicast send VCC peak rate = 25000
  C28: Connection completion timer  = 4

   LE ARP queue depth               = 5
   LE ARP cache size                = 10
   Best effort peak rate            = 25000
   Maximum config retries           = 3
   Packet trace                     = No
   No IPX interface configuration
   IP Encapsulation                 = ETHER

Ethernet Forum Compliant LEC Config>set elan
Assign emulated LAN name []? ETH_ELAN_8285
Ethernet Forum Compliant LEC Config>ip ieee
Ethernet Forum Compliant LEC Config>exit
```

Figure 222. Listing the Ethernet LEC

Now, from the LE Client Config> prompt, issue the **List** command to list the LEC configuration for the machine. This shows you all the defined LECs for the router (in this case one). The LEC configuration should look similar to the one in Figure 223 on page 364.

```
LE Client config>list

   ATM Forum Compliant Emulated LANs
-------------------------------------------------------
  ATM interface number = 5
  LEC interface number = 6
  Emulated LAN type    = Ethernet Forum Compliant
  Emulated LAN name    = ETH_ELAN_8285
LE Client config>exit
ATM Config>exit
```

Figure 223. Listing the Router LEC Configuration

This completes the configuration of the physical interfaces.

14.2.2 Configuring the 2210 Protocols

Start by configuring IP. The basic configuration sequence for this scenario is shown in Figure 224. For more information on configuring IP, please see the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p ip
Internet protocol user configuration
IP config>add add 1
New address [0.0.0.0]? 8.8.8.210
Address mask [255.0.0.0]? 255.255.255.0
IP config>add add 0
New address [0.0.0.0]? 7.7.7.210
Address mask [255.0.0.0]? 255.255.255.0
IP config>add add 6
New address [0.0.0.0]? 192.168.2.210
Address mask [255.255.255.0]?
IP config>set int
Internal IP address [0.0.0.0]? 8.8.8.210
IP config>enable rip
IP config>exit
```

Figure 224. Configuring IP

Note: The internal IP address of the router must be set to the same address as one of the interfaces and is used for data link switching.

Next, configure IPX. This is done with the p ipx command. For this scenario, it simply means defining an IPX network address to each interface and then enabling the IPX protocol for each interface. The basic configuration sequence for this scenario is shown in Figure 225 on page 365. For more information on configuring IPX, please see the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p ipx
IPX protocol user configuration
IPX config>set net
Which interface [0]?
Network number in hex [1]? 7777
IPX config>set net
Which interface [0]? 1
Network number in hex [1]? 8888
IPX config>set net
Which interface [0]? 6
Network number in hex [1]? 2222
IPX config>en int
Which interface [0]?
IPX config>en int
Which interface [0]? 1
IPX config>en int 6
IPX config>set host
Host number for serial lines (in hex) []? 400022100000
IPX config>set max ser
New Service table size [32]? 64
IPX config>set max netw
New Network table size [32]? 64
```

Figure 225. Configuring IPX

If you have performed these steps correctly, you should be able to list the IPX configuration and see a screen similar to the one in Figure 226 on page 366.

```
IPX config>list

IPX globally                enabled
Host number (serial line)   400022100000
Router Name (IPXWAN)
NodeID (IPXWAN)             00000000
Maximum networks                 64
Maximum total route entries      32
Maximum routes per dest. network 1
Maximum services                 64
Maximum Network Cache entries    64
Maximum Local Cache entries      64

List of configured interfaces:
               Frame                    SAP nearest  Split
Ifc  IPX net #  Encapsulation          server reply Horizon      IPXWAN
  0       7777  TOKEN-RING        MSB   Enabled      Enabled      N/A
  1       8888  N/A                     Enabled      Enabled      N/A
  6       2222  ETHERNET_802.3          Enabled      Enabled      N/A


RIP/SAP Timer Intervals and Pacing:
               SAP Interval  RIP Interval
Ifc  IPX net #   (Minutes)     (Minutes)    Pacing
  0       7777          1             1     Disabled
  1       8888          1             1     Disabled
  6       2222          1             1     Disabled
IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.

IPX Keepalive Filtering/Proxy Reply is not enabled on any interface.
IPX config>exit
```

Figure 226. Listing the IPX Configuration

Next, configure the bridging function in the router. The basic configuration sequence for this scenario is shown in Figure 227 on page 367. Note that source route to translational (SR-TB) conversion has been configured. This is so that a station on the Ethernet ELAN can communicate with a station on the token-ring. For more information on configuring the bridge, please see the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable brid
ASRT config>dis tr
Port Number [1]?
ASRT config>en sou
Port Number [1]?
Segment Number for the port in hex(1 - FFF) [  1]? 7
Bridge number in hex (0 - 9, A - F) [0]?
ASRT config>enab dls
ASRT config>ena sr-tb
TB-Domain Segment Number in hex(1-FFF) [1]? feb
TB-Domain's MTU [1470]?
Bridge Virtual Segment Number in hex(1-FFF) [1]? aaa
```

Figure 227. Configuring the Bridge Function

If you have performed these steps correctly, you should be able to list the ASRT configuration and see a screen similar to the one in Figure 228 on page 368.

```
ASRT config>list br

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

Bridge:                 Enabled                 Bridge Behavior: SR<->TB SRB
                  +-----------------------------+
------------------| SOURCE ROUTING INFORMATION |------------------------------
                  +-----------------------------+
Bridge Number:          00                      Segments:          1
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1:N SRB:                Active                  Internal Segment:  0xAAA
LF-bit interpret:       Extended
                  +-------------------+
------------------| SR-TB INFORMATION |--------------------------------------
                  +-------------------+
SR-TB Conversion:       Enabled
TB-Virtual Segment:     0xFEB                   MTU of TB-Domain:  1470
                  +----------------------------------+
------------------| SPANNING TREE PROTOCOL INFORMATION |----------------------
                  +----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IEEE802.1d on TB ports only, IBM-SRB proprietary on SR
ports
                  +-------------------------+
------------------| TRANSLATION INFORMATION |---------------------------------
                  +-------------------------+
FA<=>GA Conversion:     Enabled  UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                  +------------------+
------------------| PORT INFORMATION |--------------------------------------
                  +------------------+
Number of ports added: 2
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled
Port:   2      Interface:       6      Behavior:    STB Only   STP:  Enabled

ASRT config>exit
```

Figure 228. Listing the Bridge Configuration

Next, configure Data Link Switching (DLSw). The basic configuration sequence for this scenario is shown in Figure 229 on page 369. For more information on configuring DLSw, please see the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p dls
DLSw protocol user configuration
DLSw config>enable dls
DLSw config>set srb
Enter segment number in hex (1-FFF) [000]? FAB
DLSw config>open
Interface # [0]?
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 0
DLSw config>open 6
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 6
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 8.8.8.216
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]? e
Neighbor Priority (H/M/L) [M]?
DLSw config>exit
```

Figure 229. Configuring Data Link Switching

14.2.3 Saving the Configuration and Restarting the Router

When all configuration steps have been completed, restart the router. This will activate your configuration and is shown in Figure 230.

```
*restart
Are you sure you want to restart the gateway? (Yes or
[No]): y

Copyright Notices:

Licensed Materials - Property of IBM
Multiprotocol Routing Services
(C) Copyright IBM Corp. 1996
All Rights Reserved. US Gov. Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.

MOS Operator Control

*
```

Figure 230. Restarting the Router

14.2.4 Monitoring the 2210 Activity

After the router restarts with the new configuration, you should use the talk 5 menus to check that the configuration is correct. Use the configure command to check that all the interfaces are up and running. An example is shown in Figure 231.

```
+conf

Multiprotocol Routing Services

5765-B86 Feature 5105 V1 R1.0 PTF 0 RPQ 0 MRS.A7C

Boot ROM version  V2.20    Watchdog timer enabled    Auto-boot enabled
Time: 15:39:08    Thursday, June 28, 2012    Temp: 53C (127F)
Console Baud Rate: 9600    Auxiliary Baud Rate 9600

Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
7   IPX   NetWare IPX
11  SNMP  Simple Network Management Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
26  DLS   Data Link Switching

Num Name  Feature
2   MCF   MAC Filtering

7 Networks:
Net Interface  MAC/Data-Link         Hardware                    State
0   TKR/0      Token-Ring/802.5      IBM Token-Ring              Up
1   FR/0       Frame Relay           SCC Serial Line             Up
2   PPP/0      Point to Point        SCC Serial Line             Down
3   PPP/1      Point to Point        SCC Serial Line             Down
4   PPP/2      Point to Point        SCC Serial Line             Down
5   ATM/0      ATM                   CHARM ATM                   Up
6   Eth/0      Ethernet/IEEE 802.3   CHARM ATM                   Up
```

Figure 231. Checking the Router Configuration

14.2.5 Adding the 2216 Hardware Interfaces

First, add the devices to the configuration. We start with token-ring and then add the ATM adapter and the serial port. The configuration sequence is shown in Figure 232 on page 371.

```
ra2216a  Config>add dev tok
Device Slot #(1-8) [1]?
Device Port #(1-2) [1]?
Adding Token Ring device in slot 1  port 1 as interface #0
Use "net 0" to configure Token Ring parameters
ra2216a  Config>add dev atm
Device Slot #(1-8) [1]? 4
Adding CHARM ATM device in slot 4  port 1 as interface #1
Use "net 1" to configure CHARM ATM parameters
ra2216a  Config>add dev eia
Device Slot #(1-8) [1]? 8
Device Port #(0-7) [0]?
Defaulting Data-link protocol to PPP
Adding EIA-232E/V.24 PPP device in slot 8  port 0 as interface #2
Use "set data-link" command to change the data-link protocol
Use "net 2" to configure EIA-232E/V.24 PPP parameters
```

Figure 232. Adding the Hardware Interfaces

Next, set the serial port DLC to frame relay. The configuration sequence is shown in Figure 233.

```
ra2216a  Config>set da fr
Interface Number [0]? 2
```

Figure 233. Setting the DLC for the Serial Interface

If you have performed these steps correctly, you should be able to list the devices and see a screen similar to the one in Figure 234.

```
ra2216a  Config>list dev
Ifc 0 Token Ring                    Slot: 1  Port: 1
Ifc 1 CHARM ATM                     Slot: 4  Port: 1
Ifc 2 EIA-232E/V.24 Frame Relay     Slot: 8  Port: 0
```

Figure 234. Listing the Devices in the Router

14.2.6 Configuring the 2216 Interfaces

Start with frame relay. You should be able to list the frame relay config and see a screen similar to the one in Figure 235 on page 372. This shows the default parameters for frame relay.

```
ra2216a  Config>net 2
Frame Relay user configuration
ra2216a  FR Config>list all

                        Frame Relay HDLC Configuration


  Encoding      = NRZ               IDLE                     = Flag
  Clocking      = External
  Cable type    = RS-232 DTE
  Line speed (bps)       = 19200    Interface MTU in bytes   = 2048
  Transmit delay         = 0
  Lower DTR              = Disabled

                        Frame Relay Configuration


  LMI enabled            =     Yes  LMI DLCI                       =    0
  LMI type               =    ANSI  LMI Orphans OK                 =  Yes

  Protocol broadcast     =     Yes  Congestion monitoring          =  Yes
  Emulate multicast      =     Yes  CIR monitoring                 =   No

  PVCs P1 allowed        =      64  Interface down if no PVCs      =   No
  Timer T1 seconds       =      10  Counter N1 increments          =    6
  LMI N2 error threshold =       3  LMI N3 error threshold window =    4
  MIR % of CIR           =      25  IR % Increment                 =   12
  IR % Decrement         =      25  DECnet length field            =   No

No PVCs configured
No required PVC groups have been defined

No address translations configured
```

Figure 235. Listing the Frame Relay DLC Configuration

For this scenario, the defaults are OK with the exception of the setting for LMI. We need to disable LMI because we are using a back-to-back V.24 connection between the two routers. LMI is only used when connecting to a frame relay network. Also, we need to add a PVC to the frame relay interface for the connection to the 2210. These steps are shown in Figure 236.

```
ra2216a  FR Config>dis lmi
ra2216a  FR Config>add per
Circuit number [16]?
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []?
Is circuit required for interface operation [N]?
ra2216a  FR Config>ex
```

Figure 236. Configuring Frame Relay for Scenario 2

Next, configure the token-ring interface. The basic configuration sequence for this scenario is shown in Figure 237 on page 373. For more information on configuring token-ring, please see the *Nways Multiprotocol Access Services Software User's Guide*.

```
ra2216a  Config>net 0
Token-Ring interface configuration
ra2216a  TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Shielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
IPX interface configuration record missing

ra2216a  TKR config>set phy 40:00:22:16:00:00
ra2216a  TKR config>med ?
SHIELDED twisted pair
UNSHIELDED twisted pair
ra2216a  TKR config>ex
```

Figure 237. Configuring the Token-Ring Interface

Next, configure ATM. The configuration sequence is shown in Figure 238. The process is identical to that in configuring the ATM interface on the 2210 and the same notes apply. These notes are presented again here for your convenience.

The ESI added here is used for both LEC and CIP clients. The LEC and CIP clients use the network prefix from the switch and the ESI defined here along with a unique selector byte as their ATM address.

Note: There is no command when configuring the LEC and CIP clients to add another ESI. That can only be done while configuring the ATM interface. Therefore it is important that you have decided on your ATM network structure and addressing before you begin configuring the ATM interface.

The command set uni auto sets the UNI version to auto-detection. For information on the ILMI process and how the UNI version is chosen during initialization see 11.5.1, “Overview of ILMI Functions” on page 294.

```
ra2216a  Config>net 1
ATM user configuration
ra2216a  ATM Config>int
ATM interface configuration
ra2216a  ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? 40.00.22.16.00.01
ra2216a  ATM Interface Config>set uni auto
ra2216a  ATM Interface Config>exit
```

Figure 238. Configuring the ATM Interface

Next, configure the LEC. The configuration sequence is shown in Figure 239 on page 374. The process is identical to that in configuring the LEC on the 2210 except that we are adding an emulated token-ring interface to the 2216 while we added an emulated Ethernet interface to the 2210. The same notes apply, namely:

Notes:

1. The set esi address is used to select an already defined End System Identifier (ESI) to be used for this interface. The definition was done in the previous step when the ATM interface was defined.
2. For this scenario, you need to have the ATM address of the LAN Emulation Server (LES) for the ELAN that the LEC will join before proceeding. Since we are not using an MSS server and its associated LAN Emulation Configuration Server (LECS), it is necessary to hard code the address of the LES into the LEC configuration. This way, when the LEC is ready to join the ELAN, it will already know what the address of its LES is and will not need to use the LECS to find it.
3. You must set the LECS auto configuration to no before you can configure the ATM address of the LES.
4. Setting the ELAN name is not necessary *for this scenario* but it is shown as an example. If you are using a LECS in your system that is using an ELAN name policy and has more than one token-ring LES defined, then you will need to set the ELAN name. In this case, setting the ELAN name allows you to attach to a specific ELAN. Otherwise, a LEC going through the ILMI procedure may be assigned to any of the token-ring LESs, which might not be the desired ELAN.
5. The ELAN name is case sensitive. If not typed in correctly, the interface will not come up to an operational state.

```
ra2216a  ATM Config>le-c
ATM LAN Emulation Clients configuration
ra2216a  LE Client config>add tok
Added Emulated LAN as interface 3
ra2216a  LE Client config>conf 3
ATM LAN Emulation Client configuration
ra2216a  Token Ring Forum Compliant LEC Config>set esi
Select ESI
   (1) Use burned in ESI
   (2) 40.00.22.16.00.01

Enter selection [1]? 2
ra2216a  Token Ring Forum Compliant LEC Config>set mac
Use adapter address for MAC? [Yes]: n
MAC address [00.00.00.00.00.00]? 40.00.22.16.00.03
ra2216a  Token Ring Forum Compliant LEC Config>set elan
Assign emulated LAN name []? TR_ELAN_8285
ra2216a  Token Ring Forum Compliant LEC Config>set auto
Do LECS auto configuration? [Yes]: n
ra2216a  Token Ring Forum Compliant LEC Config>set les
LES ATM address in 00.00.00.00.00.00:... form []? 39.09.85.11.11.11.11.11.11.11.
11.01.03.40.00.00.82.85.a1.03
```

Figure 239. Configuring the LEC for the Token-Ring ELAN

If you have performed these steps correctly, you should be able to list the configuration for the token-ring LEC and see a screen similar to the one in Figure 240 on page 375.

```
ra2216a  Token Ring Forum Compliant LEC Config>list

                 ATM LEC Configuration

   Physical ATM interface number    = 1
   LEC interface number             = 3
   LECS auto configuration          = No

   C1: Primary ATM address
          ESI address               = 40.00.22.16.00.01
          Selector byte             = 0x2
   C2: Emulated LAN type            = Token Ring
   C3: Maximum frame size           = 4544
   C5: Emulated LAN name            = TR_ELAN_8285
   C6: LE Client MAC address        = 40.00.22.16.00.03
   C7: Control timeout              = 30
   C9: LE Server ATM address        = 39.09.85.11.11.11.11.11.11.11.11.01.03.40.
00.00.82.85.A1.03
  C10: Maximum unknown count        = 10
  C11: Maximum unknown time         = 1
  C12: VCC timeout period           = 1200
  C13: Maximum retry count          = 1
  C17: Aging time                   = 300
  C18: Forward delay time           = 15
  C20: LE ARP response time         = 1
  C21: Flush timeout                = 4
  C22: Path switch delay            = 6
  C24: Multicast send VCC type      = Best-Effort
  C25: Multicast send VCC avg rate  = 155000
  C26: Multicast send VCC peak rate = 155000
  C28: Connection completion timer  = 4

   LE ARP queue depth               = 5
   LE ARP cache size                = 10
   Best effort peak rate            = 155000
   Maximum config retries           = 3
   Packet trace                     = No
   RIF Aging Timer                  = 120
   Source Routing                   = Enabled
   IPX interface configuration record missing

ra2216a  Token Ring Forum Compliant LEC Config>ex
ra2216a  LE Client config>ex
ra2216a  ATM Config>ex
```

Figure 240. Listing the LEC Configuration

14.2.7 Configuring the 2216 Protocols

Start with IP. The basic configuration sequence for this scenario is shown in Figure 241 on page 376. For more information on configuring the IP protocol, please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
ra2216a  Config>p ip
Internet protocol user configuration
ra2216a  IP config>add add
Which net is this address for [0]?
New address [0.0.0.0]? 9.24.104.203
Address mask [255.0.0.0]? 255.255.255.0
ra2216a  IP config>add add
Which net is this address for [0]? 2
New address [0.0.0.0]? 8.8.8.216
Address mask [255.0.0.0]? 255.255.255.0
ra2216a  IP config>add add 3
New address [0.0.0.0]? 192.168.3.216
Address mask [255.255.255.0]?
```

Figure 241. Configuring IP

Now, list the IP configuration to ensure that you entered the addresses correctly. You should see a screen similar to the one in Figure 242.

```
ra2216a  IP config>list all
Interface addresses
IP addresses for each interface:
   intf  0   9.24.104.203     255.255.255.0    Local wire broadcast, fill 1
   intf  1                                     IP disabled on this interface
   intf  2   8.8.8.216        255.255.255.0    Local wire broadcast, fill 1
   intf  3   192.168.3.216    255.255.255.0    Local wire broadcast, fill 1

Routing

Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: disabled
BGP: disabled
RIP: disabled
```

Figure 242. Listing the IP Configuration

Next, enable RIP on the box and give it an internal IP address. The configuration sequence is shown in Figure 243.

```
ra2216a  IP config>enable rip
ra2216a  IP config>set internal
Router-ID [0.0.0.0]? 8.8.8.216
ra2216a  IP config>exit
```

Figure 243. Enabling RIP

Next, configure IPX. The configuration sequence is shown in Figure 244 on page 377.

```
ra2216a  Config>p ipx
IPX protocol user configuration
ra2216a  IPX config>enable ipx
ra2216a  IPX config>enab int 0
Configure an IPX network number for this interface.
Network number in hex [1]? 9
ra2216a  IPX config>en int 3
Configure an IPX network number for this interface.
Network number in hex [1]? 3333
ra2216a  IPX config>en int 2
Configure an IPX network number for this interface.
Network number in hex [1]? 8888
ra2216a  IPX config>set max net
New Network table size [32]? 64
ra2216a  IPX config>set max ser
New Service table size [32]? 64
ra2216a  IPX config>set host
Host number for serial lines (in hex) []? 400022160002
```

Figure 244. Configuring IPX

If you have performed these steps correctly, you should see a screen similar to the one in Figure 245 on page 378.

```
ra2216a  IPX config>list
IPX globally                enabled
Host number (serial line)   400022160002
Router Name (IPXWAN)
NodeID (IPXWAN)             0
Maximum networks                  64
Maximum total route entries       32
Maximum routes per dest. network  1
Maximum services                  64
Maximum Network Cache entries     64
Maximum Local Cache entries       64

List of configured interfaces:
                Frame                     SAP nearest  Split
Ifc  IPX net #  Encapsulation           server reply Horizon      IPXWAN
  0          9  TOKEN-RING        MSB   Enabled      Enabled      N/A
  2       8888  N/A                     Enabled      Enabled      N/A
  3       3333  TOKEN-RING        MSB   Enabled      Enabled      N/A


RIP/SAP Timer Intervals and Pacing:
                SAP Interval  RIP Interval
Ifc  IPX net #   (Minutes)     (Minutes)    Pacing
  0          9          1             1     Disabled
  2       8888          1             1     Disabled
  3       3333          1             1     Disabled
IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.

IPX Keepalive Filtering/Proxy Reply is not enabled on any interface.
ra2216a  IPX config>ex
```

Figure 245. Listing the IPX Configuration

Now that IPX has been configured, you can go back and set the frame types for the token ring LEC. In this scenario, the default of TOKEN-RING MSB was used. If you need support for other frame types, go back and add them now.
Regardless, if you list the LEC configuration again now, you will see that the NetWare IPX encapsulation has been assigned. (See Figure 246 on page 379.)

```
ra2216a  Config>net 3
ATM LAN Emulation Client configuration
ra2216a  Token Ring Forum Compliant LEC Config>list

                ATM LEC Configuration

   Physical ATM interface number             = 1
   LEC interface number             = 3
   LECS auto configuration          = No

   C1: Primary ATM address
          ESI address               = 40.00.22.16.00.01
          Selector byte             = 0x2
   C2: Emulated LAN type            = Token Ring
   C3: Maximum frame size           = 4544
   C5: Emulated LAN name            = TR_ELAN_8285
   C6: LE Client MAC address        = 40.00.22.16.00.03
   C7: Control timeout              = 30
   C9: LE Server ATM address        = 39.09.85.11.11.11.11.11.11.11.11.01.03.40.
00.00.82.85.A1.03
  C10: Maximum unknown count        = 10
  C11: Maximum unknown time         = 1
  C12: VCC timeout period           = 1200
  C13: Maximum retry count          = 1
  C17: Aging time                   = 300
  C18: Forward delay time           = 15
  C20: LE ARP response time         = 1
  C21: Flush timeout                = 4
  C22: Path switch delay            = 6
  C24: Multicast send VCC type      = Best-Effort
  C25: Multicast send VCC avg rate  = 155000
  C26: Multicast send VCC peak rate = 155000
  C28: Connection completion timer  = 4

   LE ARP queue depth               = 5
   LE ARP cache size                = 10
   Best effort peak rate            = 155000
   Maximum config retries           = 3
   Packet trace                     = No
   RIF Aging Timer                  = 120
   Source Routing                   = Enabled
   NetWare IPX encapsulation        = TOKEN-RING MSB
ra2216a  Token Ring Forum Compliant LEC Config>ex
```

Figure 246. Listing the LEC Configuration

Now configure the bridge function. The basic configuration sequence for this scenario is shown in Figure 247 on page 380. Note that since the 2216 only has token-ring segments attached, it is not necessary to enable translational bridging. For more information on configuring bridging, please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
ra2216a  Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
ra2216a  ASRT config>enabl bridg
ra2216a  ASRT config>enab dls
ra2216a  ASRT config>dis tra
Port Number [1]?
ra2216a  ASRT config>list port
Port ID (dec)    : 128:01, (hex): 80-01
Port State       : Enabled
STP Participation: Enabled
Port Supports    : No Bridging
Assoc Interface  : 0
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port ID (dec)    : 128:02, (hex): 80-02
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 3
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
ra2216a  ASRT config>dis tran
Port Number [1]? 2
ra2216a  ASRT config>en sour
Port Number [1]?
Segment Number for the port in hex(1 - FFF) [001]? 584
Bridge number in hex (0 - 9, A - F) [0]?
ra2216a  ASRT config>en sour
Port Number [1]? 2
Segment Number for the port in hex(1 - FFF) [001]? 333
Bridge Virtual Segment Number in hex(1 - FFF) [1]? 216
```

Figure 247. Configuring the Bridging Function

If you have performed these steps correctly, you should be able to list the bridging configuration and see a screen similar to the one in Figure 248 on page 381.

```
ra2216a  ASRT config>list br

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

Bridge:                 Enabled                 Bridge Behavior: SRB
                   +----------------------------+
------------------ | SOURCE ROUTING INFORMATION |------------------------------
                   +----------------------------+
Bridge Number:          00                      Segments:          2
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1:N SRB:                Active                  Internal Segment:  0x216
LF-bit interpret:       Extended
                   +-------------------+
------------------ | SR-TB INFORMATION |-------------------------------------
                   +-------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
                   +-----------------------------------+
------------------ | SPANNING TREE PROTOCOL INFORMATION |----------------------
                   +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IBM-SRB proprietary
                   +-------------------------+
------------------ | TRANSLATION INFORMATION |---------------------------------
                   +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                   +------------------+
------------------ | PORT INFORMATION |-------------------------------------
                   +------------------+
Number of ports added: 2
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled
Port:   2      Interface:       3      Behavior:    SRB Only   STP:  Enabled

ra2216a  ASRT config>exit
```

Figure 248. Listing the Bridge Configuration

Now configure Data Link Switching (DLSw). The basic configuration sequence for this scenario is shown in Figure 249 on page 382. For more information on configuring DLSw, please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
ra2216a  Config>p dlsw
DLSw protocol user configuration
ra2216a  DLSw config>enab dls
ra2216a  DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 8.8.8.210
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]? e
Neighbor Priority (H/M/L) [M]?
ra2216a  DLSw config>open
Interface # [0]?
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 0
ra2216a  DLSw config>open
Interface # [0]? 3
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 3
ra2216a  DLSw config>set srb
Enter segment number in hex (1-FFF) [000]? FAB
ra2216a  DLSw config>exit
```

Figure 249. Configuring Data Link Switching

14.2.8 Saving the Configuration and Restarting the Router

When all configuration steps have been completed, save your configuration and then restart the router. The procedure to do this is shown in Figure 250.

```
Config (only)>write
Config Save: Using bank A and config number 2
Config (only)>reload
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 250. Saving the Configuration and Restarting the Router

14.2.9 Monitoring Activity on the 2216

After the router restarts with the new configuration, you should use the talk 5 menus to check that the interfaces are working properly. Figure 251 on page 383 shows a listing of the configuration for scenario 2.

```
*t 5

CGW Operator Console

+config

Multiprotocol Access Services

5765-B87 Feature 2802 V1 R1.0 PTF 0 RPQ 0 MAS.A01 cc1_11b


Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
7   IPX   NetWare IPX
11  SNMP  Simple Network Management Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
26  DLS   Data Link Switching

Num Name  Feature
2   MCF   MAC Filtering

4 Networks:
Net Interface  MAC/Data-Link         Hardware                    State
0   TKR/0      Token-Ring/802.5      Token-Ring                  Up
1   ATM/0      ATM                   CHARM ATM                   Up
2   FR/0       Frame Relay           EIA-232E/V.24               Up
3   TKR/1      Token-Ring/802.5      CHARM ATM                   Up
```

Figure 251. Listing the Router Configuration

Figure 252 shows an IP dump. You can use this to see the IP networks that the router knows about. This list includes the networks directly attached and ones learned using the RIP protocol.

```
+p ip
IP>dump
Type   Dest net         Mask      Cost     Age       Next hop(s)

 RIP   7.0.0.0          FF000000  2        20        8.8.8.210
Sbnt   8.0.0.0          FF000000  1        13        None
 Dir*  8.8.8.0          FFFFFF00  1        38        FR/0
Sbnt   9.0.0.0          FF000000  1        13        None
 Dir*  9.24.104.0       FFFFFF00  1        21        TKR/0
 RIP   9.24.105.0       FFFFFF00  2        10        9.24.104.74
 RIP   192.168.2.0      FFFFFF00  2        20        8.8.8.210
 Dir*  192.168.3.0      FFFFFF00  1        33        TKR/1
 RIP   192.168.109.0    FFFFFF00  2        10        9.24.104.74
 RIP   192.168.253.0    FFFFFF00  2        10        9.24.104.126
 RIP   192.168.254.0    FFFFFF00  2        10        9.24.104.126

Routing table size: 768 nets (49152 bytes), 11 nets known
```

Figure 252. Listing the IP Configuration

Now use the IP ping command to check that IP is working properly. In Figure 253 on page 384, we show pinging a station attached to the ELAN named

ETH_ELAN_8285 from the 2216. The frames are going across the frame relay connection through the 2210 and out the 2210 ATM interface onto the campus ATM backbone to the workstation.

```
IP>ping 192.168.2.89
PING 8.8.8.216 -> 192.168.2.89: 56 data bytes, ttl=64, every 1 sec.

----192.168.2.89 PING Statistics----
3 packets transmitted, 0 packets received, 100% packet loss
IP>ping 192.168.2.210
PING 8.8.8.216 -> 192.168.2.210: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.168.2.210: icmp_seq=0. ttl=64. time=20. ms
56 data bytes from 192.168.2.210: icmp_seq=1. ttl=64. time=20. ms
56 data bytes from 192.168.2.210: icmp_seq=2. ttl=64. time=20. ms
56 data bytes from 192.168.2.210: icmp_seq=3. ttl=64. time=20. ms

----192.168.2.210 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 20/20/20 ms
```

Figure 253. Using the Ping Command to Check IP

Figure 254 shows an IPX dump. You can use this to list the IPX networks that the router knows about. This list includes the networks directly attached and ones learned using the RIP protocol.

```
+protocol ipx
IPX>dump

10 route entries used out of 64
10 net entries used out of 64

Type     Dest net Hops Delay  Age(M:S)   via Router
 Dir       8888    0     5      0: 0       8888/400022160002 2-FR/0
 Dir       3333    0     1      0: 0       3333/400022160003 3-TKR/1
 Dir          9    0     1      0: 0          9/400022160000 0-TKR/0
 RIP         10    1     2      0:50          9/08005AB96860
 RIP       2222    1     2      0:35       8888/400022100000
 RIP   30AA0F92    1     2      0:55          9/400052005240
 RIP   31ECF1DD    1     2      0:10          9/08005A0D2860
 RIP   325521DE    2     3      0:35       8888/400022100000
 RIP   857A7D6D    1     2      0:50          9/08005AB96860
 RIP   D6CA61D7    1     2      0:35          9/08005ACE6D99

IPX>exit
```

Figure 254. Displaying an IPX Dump

The DLSw TCP/IP sessions are listed in Figure 255 on page 385. This shows that the 2216 has a TCP/IP session with a neighboring router of address 8.8.8.210 and that the connection is established. There are no active sessions across the link at present.

```
+protocol dlsw
Data Link Switching Console
DLSw>list tcp sess all

  Group/Mcast@    IP Address      Conn State     CST Version  ActSes SesCreates
  --------------- --------------- -------------- --- -------- ------ ----------
1                 8.8.8.210       ESTABLISHED     a  AIW V1RO      0          0

DLSw>ex
+
```

Figure 255. Displaying the DLSw TCP/IP Sessions

This completes the configuration of scenario 2.

14.3 Implementing Scenario 3

This scenario is shown in Figure 256. In this scenario the 2216 and 2210 route between legacy LANs over an ATM network. The routers are configured to route IP and IPX while bridging SNA via DLSw. OSPF is used as the routing protocol for IP.

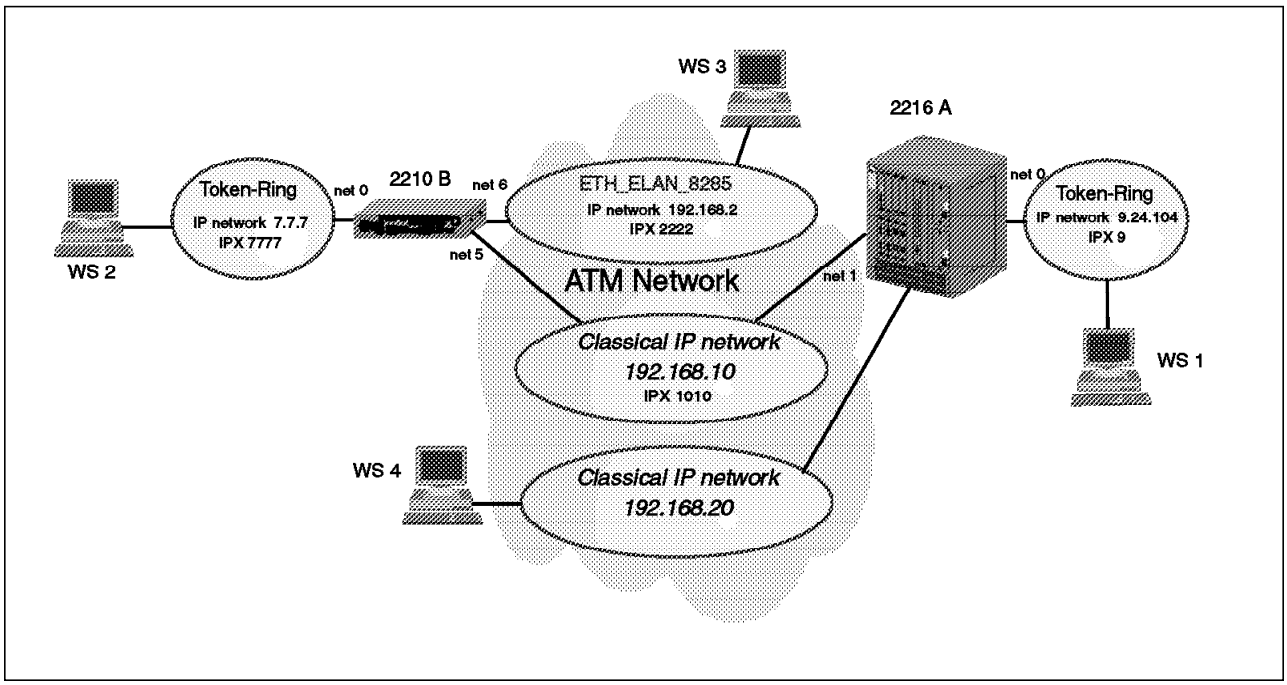


Figure 256. Scenario 3

The steps necessary for configuring the 2216 for scenario 3 are presented below. We first show the steps for configuring the hardware interfaces. We then explain the steps for configuring the protocols. Please refer to Figure 256 as you perform these steps.

14.3.1 Adding the Hardware Interfaces

First, add the hardware interfaces. The configuration sequence we used for this scenario is shown in Figure 257.

```
Config>add dev tok
Device Slot #(1-8) [1]?
Device Port #(1-2) [1]?
Adding Token Ring device in slot 1  port 1 as interface #0
Use "net 0" to configure Token Ring parameters
Config>add dev atm
Device Slot #(1-8) [1]? 4
Adding CHARM ATM device in slot 4  port 1 as interface #1
Use "net 1" to configure CHARM ATM parameters
Config>exit
```

Figure 257. Adding the Hardware Interfaces

14.3.2 Configuring the Hardware Interfaces

The next step is to configure the hardware interfaces. Start with the token-ring adapter. The basic configuration sequence for this scenario is shown in Figure 258. For more information on configuring token-ring, please see the *Nways Multiprotocol Access Services Software User's Guide*.

```
Config>net 0
Token-Ring interface configuration
TKR config>speed 4
TKR config>media unsh
TKR config>set phys
MAC address in 00:00:00:00:00:00 form []? 40:00:22:16:00:00
```

Figure 258. Configuring the Token-Ring Interface

If you have performed these steps correctly, you should be able to list the token-ring configuration and see something very similar to that shown in Figure 259.

```
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Unshielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              400022160000
IPX interface configuration record missing
TKR config>exit
```

Figure 259. Listing the Token-Ring Configuration

Next, configure the ATM interface. The configuration sequence is shown in Figure 260 on page 388.

The ESI added here is used for both LEC and CIP clients. The LEC and CIP clients use the network prefix from the switch and the ESI defined here along with a unique selector byte as their ATM address.

Note: There is no command when configuring the LEC and CIP clients to add another ESI. That can only be done while configuring the ATM interface. Therefore it is important that you have decided on your ATM network structure and addressing before you begin configuring the ATM interface.

The command `set uni auto` sets the UNI version to auto-detection. For information on the ILMI process and how the UNI version is chosen during initialization see 11.5.1, “Overview of ILMI Functions” on page 294.

```
Config>net 1
ATM user configuration
ATM Config>int
ATM interface configuration
ATM Interface Config>set uni auto
ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? 400 .00.22.1.  16.00.01
ATM Interface Config>exit
ATM Config>exit
```

Figure 260. Configuring the ATM Interface

14.3.3 Configuring the Protocols

First, configure IP. The basic configuration sequence for this scenario is shown in Figure 261. For more information on configuring IP, please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p ip
Internet protocol user configuration
IP config>add address 0
New address [0.0.0.0]? 9.24.104.203
Address mask [255.0.0.0]? 255.255.255.0
IP config>add address 1
New address [0.0.0.0]? 192.168.10.216
Address mask [255.255.255.0]?
IP config>set router-id
Router-ID [9.24.104.203]? 10.10.10.216
IP config>add add
Which net is this address for [0]? 1
New address [0.0.0.0]? 192.168.20.216
Address mask [255.255.255.0]?
IP config>set internal
Internal IP address [0.0.0.0]? 10.10.10.216
```

Figure 261. Configuring the IP Protocol

If you performed these steps correctly, you should be able to list the IP configuration and see something very similar to that shown in Figure 262 on page 389.

```
IP config>list add
IP addresses for each interface:
   intf  0   9.24.104.203     255.255.255.0    Local wire broadcast, fill 1
   intf  1   192.168.10.216   255.255.255.0    Local wire broadcast, fill 1
             192.168.20.216   255.255.255.0    Local wire broadcast, fill 1
   intf  2                                     IP disabled on this interface
   intf  3                                     IP disabled on this interface
   intf  4                                     IP disabled on this interface
   intf  5                                     IP disabled on this interface
   intf  6                                     IP disabled on this interface
Router-ID: 10.10.10.216
Internal IP address: 10.10.10.216
IP config>exit
```

Figure 262. Listing Defined IP Addresses

Next, configure IPX. The basic configuration sequence for this scenario is shown in Figure 263. For more information on configuring IPX, please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p ipx
IPX protocol user configuration
IPX config>ena ipx
IPX config>ena int 0
Configure an IPX network number for this interface.
Network number in hex [1]? 9
IPX config>ena int 1
Configure an IPX network number for this interface.
Network number in hex [1]? 1010
IPX config>set max ser 64
```

Figure 263. Configuring IPX

Now, list the the IPX configuration. You should see something very similar to that shown in Figure 264 on page 390.

```
IPX config>list

IPX globally                enabled
Host number (serial line)   000000000000
Router Name (IPXWAN)
NodeID (IPXWAN)             0
Maximum networks                  32
Maximum total route entries       32
Maximum routes per dest. network  1
Maximum services                  64
Maximum Network Cache entries     64
Maximum Local Cache entries       64

List of configured interfaces:
                Frame                    SAP nearest  Split
Ifc  IPX net #  Encapsulation           server reply Horizon      IPXWAN
  0          9  TOKEN-RING        MSB   Enabled      Enabled      N/A
  1       1010  N/A                      Enabled      Enabled      N/A


RIP/SAP Timer Intervals and Pacing:
                SAP Interval  RIP Interval
Ifc  IPX net #   (Minutes)     (Minutes)    Pacing
  0          9          1             1     Disabled
  1       1010          1             1     Disabled
IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.

IPX Keepalive Filtering/Proxy Reply is not enabled on any interface.
IPX config>exit
```

Figure 264. Listing the IPX Configuration

Now, configure Classical IP and IPX over ATM. The configuration sequences are shown in Figure 265 on page 391 and Figure 266 on page 392. Please note the following about this configuration:

Notes:

1. We added two clients for IP and one for IPX on the ATM interface. The reason three clients were added is that each LIS must have a client and if there are to be IPX connections across ATM, an IPX client is needed.
2. There can only be one IPX client added as only one IPX network is supported on each ATM interface.
3. Up to 32 CIP clients can be added to each ATM interface.
4. As the two IP clients configured are to be servers, they must have a selector explicitly defined. That way their ATM addresses can be configured at workstations that use them as servers.
5. Be careful that you specify the correct interface. In this case we used ATM interface #1.

```
Config>p arp
ARP user configuration
ARP config>add atm 1
Protocol [IP]?
Client IP Address [0.0.0.0]? 192.168.10.216
This client is also a server? [No]: yes
Refresh timeout (in minutes) [20]?
Enable auto-refresh? [Yes]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 400022160001
Select ESI [1]? 2
Use internally assigned selector? [Yes]: no
Selector Only, Range 00..FF [00]? AA
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Service for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Service for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
ARP config>add atm 1
Protocol [IP]?
Client IP Address [0.0.0.0]? 192.168.20.216
This client is also a server? [No]: yes
Refresh timeout (in minutes) [20]?
Enable auto-refresh? [Yes]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 400022160001
Select ESI [1]? 2
Use internally assigned selector? [Yes]: no
Selector Only, Range 00..FF [00]? 02
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Service for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Service for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
```

Figure 265. Configuring Classical IP Clients

```
ARP config>add atm 1
Protocol [IP]? ipx
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [Yes]:
  (  1) Use burned in ESI
  (  2) 400022160001
Select ESI [1]? 2
Use internally assigned selector? [Yes]:
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Service for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
```

Figure 266. Configuring an IPX Client

If you performed these steps correctly, you should be able to list the configuration and see something very similar to that shown in Figure 267.

```
ARP config>list atm

ATM Arp Clients:
-------------------------------------------------
If: 1  Prot: 0  Addr: 192.168.10.216   ESI: 40.00.22.16.00.01  Sel: AA
Server: yes  Refresh T/O: 20   AutoRefr: yes   By InArp: yes  Validate PCR: no
Use Best Effort: yes/yes  (Control/Data)   Max B/W(kbps):      0
Cell Rate(kbps):  Peak:      0/     0      Sustained:      0/     0
Max SDU(bytes):   9188
-------------------------------------------------
If: 1  Prot: 7                         ESI: 40.00.22.16.00.01  Sel: auto
Refresh T/O: 5    AutoRefr: yes   By InArp: yes  Validate PCR: no
Use Best Effort: yes  (Data)              Max B/W(kbps):      0
Cell Rate(kbps):  Peak:      0            Sustained:      0
Max SDU(bytes):   9188
-------------------------------------------------
If: 1  Prot: 0  Addr: 192.168.20.216   ESI: 40.00.22.16.00.01  Sel: 02
Server: yes  Refresh T/O: 20   AutoRefr: yes   By InArp: yes  Validate PCR: no
Use Best Effort: yes/yes  (Control/Data)   Max B/W(kbps):     0
Cell Rate(kbps):  Peak:      0/     0      Sustained:      0/     0
Max SDU(bytes):   9188
```

Figure 267. Listing the Classical IP Configuration

Now you need to configure a PVC connection to the router across the ATM network. This is used for IPX traffic and is needed as IPX over ATM has no method for resolving IPX addresses to ATM addresses. Therefore either a static SVC or a PVC is needed. If a PVC is used, the PVC must also be defined in the ATM switch that one of the routers connects to (see Figure 273 on page 397). The configuration sequence is shown in Figure 268 on page 393.

```
ARP config>add pvc
Interface Number [0]? 1
Protocol [IP]? ipx
Specify destination protocol address? (Yes or [No]): No
Permanent Virtual Circuit VPI, Range 0..255 [0]? 0
Permanent Virtual Circuit VCI, Range 0..65535 [0]? 200
ARP config>list pvc

ATM Arp Permanent Virtual Circuit Definitions
No. IF# Prot# P/S     Protocol     -> VPI / VCI    (Client Address)
1    1    7    P 00.00.00.00.00.00 ->   0 / 200
ARP config>exit
```

Figure 268. Defining a PVC

Next, configure OSPF. The basic configuration sequence for this scenario is shown in Figure 269 on page 394. For more information on configuring OSPF, please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*.

Note: The field IP Address of Neighbor is the IP address of the neighboring router across the ATM network. You must issue the add neighbor command to specify this address. This is required because Classical IP is a non-broadcast network and the only way a connection to the neighboring router can be made is if its IP address is known. Once the IP address is known, an ATMARP request can be sent to the ARP server to obtain the ATM address.

```
Config>p ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>ena ospf
Estimated # external routes [0]? 1000
Estimated # OSPF routers [0]? 40
OSPF Config>set int
Interface IP address [0.0.0.0]? 9.24.104.203
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
OSPF Config>set int
Interface IP address [0.0.0.0]? 192.168.10.216
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
OSPF Config>add neighbor
Interface IP address [0.0.0.0]? 192.168.10.216
IP Address of Neighbor [0.0.0.0]? 192.168.10.210
Can that router become Designated Router on this net? [No]:
OSPF Config>exit
```

Figure 269. Configuring OSPF

Next configure ASRT. The basic configuration sequence for this scenario is shown in Figure 270. For more information on configuring ASRT, please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>ena brid
ASRT config>dis tran
Port Number [1]? 1
ASRT config>ena sour
Port Number [1]? 1
Segment Number for the port in hex(1 - FFF) [001]? 584
Bridge number in hex (0 - 9, A - F) [0]? 0
```

Figure 270. Configuring ASRT

If you have performed these steps correctly, you should be able to list the configuration and see something very similar to that shown in Figure 271 on page 395.

```
ASRT config>list bridg

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

Bridge:                 Enabled                 Bridge Behavior: SRB
                  +-----------------------------+
------------------| SOURCE ROUTING INFORMATION |------------------------------
                  +-----------------------------+
Bridge Number:          00                      Segments:          1
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1:N SRB:                Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
                  +-------------------+
------------------| SR-TB INFORMATION |--------------------------------------
                  +-------------------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
                  +-----------------------------------+
------------------| SPANNING TREE PROTOCOL INFORMATION |----------------------
                  +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IBM-SRB proprietary
                  +-------------------------+
------------------| TRANSLATION INFORMATION |---------------------------------
                  +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Disabled
                  +------------------+
------------------| PORT INFORMATION |--------------------------------------
                  +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled

ASRT config>ena dls
ASRT config>exit

Config>p dls
DLSw protocol user configuration
DLSw config>ena dls
DLSw config>open sap
Interface # [0]? 0
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 0
```

Figure 271. Listing the Bridge Configuration

If you performed these steps correctly, you should be able to list the configuration and see something very similar to that shown in Figure 272 on page 396.

```
DLSw config>list
Command not fully specified
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 10.10.10.210
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]? e
Neighbor Priority (H/M/L) [M]?
DLSw config>set ?
CACHE       - MAC <-> IP cache size
DYNAMIC-TCP - Dynamic Neighbor TCP parameters
LLC2        - LLC2 tunable parameters
MAXIMUM     - Maximum DLSw Sessions
MEMORY      - Memory limits
PRIORITY    - Protocol priority
SRB         - SRB segment
TIMERS      - DLSw timer values
DLSw config>set srb
Enter segment number in hex (1-FFF) [000]? fab
DLSw config>exit
```

Figure 272. Listing the DLSw Configuration

14.3.4 Configuring the ATM Switch

For your convenience, we present below the relevant 8260 configuration sequence for defining a PVC. For more information on configuring the 8260, please see the redbook *IBM 8260 As a Campus ATM Switch*, SG24-5003. The configuration sequence is shown in Figure 273 on page 397.

```
8260ATM1>SET PVC 16.01 50
Enter remote port: 1.01
Enter remote hub number: 03
Enter call type: channel
Enter local VPI: 0.
Enter local VCI: 200
Enter remote VPI: 0.
Enter remote VCI: 100
Enter quality of service: best_effort
PVC set and started.
8260ATM1>show pvc all

       Local end point       ! Remote end point  !
----------------------------+-------------------+
 Port   id   type   Vpi/Vci  ! Port Vpi/Vci   HNb!   role  !QOS! Status
----------------------------+-------------------+---------+---+---------
 6.01   100 PTP-PVC   0/35   ! 8.01   0/33      2! Primary ! BE!Failed
14.01    56 PTP-PVC   0/99   !16.01   0/99      1! Primary ! BE!Failed
14.01    57 PTP-PVC   0/98   !16.01   0/98      1! Primary ! RB!Failed
16.01    50 PTP-PVC   0/200  ! 1.01   0/100     3! Primary ! BE!Active
8260ATM1>save all
8260ATM1>logout
Bye
```

Figure 273. Configuring the ATM Switch

14.3.5 Configuring the 2210

The steps necessary for configuring the 2210 for scenario 3 are presented below. We first present the steps for configuring the hardware interfaces. We then present the steps for configuring the protocols. Please refer to Figure 256 on page 386 as you perform these steps.

14.3.6 Configuring the Hardware Interfaces

First, configure the token-ring adapter. The basic configuration sequence for this scenario is shown in Figure 274. For more information on configuring token-ring, please see the *Nways Multiprotocol Routing Services Software User's Guide*.

```
Config>net 0
Token-Ring interface configuration
TKR config>speed 4
TKR config>media shielded
TKR config>set physical
MAC address in 00:00:00:00:00:00 form []? 40:00:22:10:00:00
```

Figure 274. Configuring the Token-Ring Interface

If you performed these steps correctly, you should be able to list the configuration and see something very similar to that shown in Figure 275 on page 398.

```
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Shielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              400022100000
IPX interface configuration record missing

TKR config>exit
```

Figure 275. Displaying the Token-Ring Interface Configuration

Next, configure the ATM interface. The configuration sequence is shown in Figure 276.

The ESI added here is used for both LEC and CIP clients. The LEC and CIP clients use the network prefix from the switch and the ESI defined here along with the a unique selector byte as their ATM address.

There is no command when configuring the LEC and CIP clients to add another ESI. That can only be done while configuring the ATM interface. Therefore it is important that you have decided on your ATM network structure and addressing before you begin configuring the ATM interface.

The command set uni auto sets the UNI version to auto-detection. For information on the ILMI process and how the UNI version is chosen during initialization see 11.5.1, “Overview of ILMI Functions” on page 294.

```
Config>net 5
ATM user configuration
ATM Config>interface
ATM interface configuration
ATM Interface Config>set uni auto
ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? 40.00.22.10.00.05
```

Figure 276. Configuring the ATM Interface

If you have performed these steps correctly, you should be able to list the configuration and see something very similar to that shown in Figure 277 on page 399.

```
ATM Interface Config>list con

                        ATM Configuration


  Interface (net) number =    5
  Maximum VCC data rate Mbps   =      25
  Maximum frame size     = 9234
  Maximum number of callers =  209
  Maximum number of calls = 1024
  Maximum number of parties to a multipoint call =  512
  Maximum number of Selectors that can be configured  =  200
  UNI Version = AUTO
  Packet trace = OFF
ATM Interface Config>list esi

          ESI         Enabled
  -----------------   -------
  40.00.22.10.00.05       YES

ATM Interface Config>exit
```

Figure 277. Displaying the ATM Interface Configuration

Next, add the Ethernet LEC and then configure it. The configuration sequence is shown in Figure 278 on page 400. Please note the following when configuring the LEC:

Notes:

1. The `set esi` address is used to select an already defined End System Identifier (ESI) to be used for this interface. The definition was done in the previous step when the ATM interface was defined.
2. For this scenario, you need to have the ATM address of the LAN Emulation Server (LES) for the ELAN that the LEC will join before proceeding. Since we are not using an MSS server and its associated LAN Emulation Configuration Server (LECS), it is necessary to hard code the address of the LES into the LEC configuration. This way, when the LEC is ready to join the ELAN, it will already know what the address of its LES is and will not need to use the LECS to find it.
3. You must set the LECS auto configuration to `no` before you can configure the ATM address of the LES.
4. Setting the ELAN name is not necessary *for this scenario* but it is shown as an example. If you are using a LECS in your system that is using an ELAN name policy and has more than one token-ring LES defined, then you will need to set the ELAN name. In this case, setting the ELAN name allows you to attach to a specific ELAN. Otherwise, a LEC going through the ILMI procedure may be assigned to any of the token-ring LESs, which might not be the desired ELAN.
5. The ELAN name is case sensitive. If not typed in correctly, the interface will not come up to an operational state.

```
ATM Config>le-client
ATM LAN Emulation Clients configuration
LE Client config>add eth
Added Emulated LAN as interface 6
LE Client config>conf 6
ATM LAN Emulation Client configuration
Ethernet Forum Compliant LEC Config>set auto
Do LECS auto configuration? [Yes]: no
Ethernet Forum Compliant LEC Config>set les
LES ATM address in 00.00.00.00.00.00:.... form []?
      39.09.85.11.11.11.11.11.11.11.11.01.03.82.85.40.00.00.82.85.a1.02
Ethernet Forum Compliant LEC Config>set elan
Assign emulated LAN name []? ETH_ELAN_8285
Ethernet Forum Compliant LEC Config>set esi
Select ESI
   (1) Use burned in ESI
   (2) 40.00.22.10.00.05

Enter selection [1]? 2
Ethernet Forum Compliant LEC Config>set mac
Use adapter address for MAC? [Yes]: no
MAC address [00.00.00.00.00.00]? 40.00.22.10.00.06
Ethernet Forum Compliant LEC Config>ip ieee-802.3
```

Figure 278. Configuring the Ethernet LAN Emulation Client

If you performed these steps correctly, you should be able to list the configuration and see something very similar to that shown in Figure 279 on page 401.

```
Ethernet Forum Compliant LEC Config>list all

                ATM LEC Configuration

   ATM interface number             = 5
   LEC interface number             = 6
   LECS auto configuration          = No

   C1: Primary ATM address
          ESI address               = 40.00.22.10.00.05
          Selector byte             = 0x2
   C2: Emulated LAN type            = Ethernet
   C3: Maximum frame size           = 1516
   C5: Emulated LAN name            = ETH_ELAN_8285
   C6: LE Client MAC address        = 40.00.22.10.00.06
   C7: Control timeout              = 30
   C9: LE Server ATM address        = 39.09.85.11.11.11.11.11.11.11.
                                      11.01.03.40.00.00.82.85.A1.02
  C10: Maximum unknown count        = 1
  C11: Maximum unknown time         = 1
  C12: VCC timeout period           = 1200
  C13: Maximum retry count          = 1
  C17: Aging time                   = 300
  C18: Forward delay time           = 15
  C20: LE ARP response time         = 1
  C21: Flush timeout                = 4
  C22: Path switch delay            = 6
  C24: Multicast send VCC type      = Best-Effort
  C25: Multicast send VCC avg rate  = 25000
  C26: Multicast send VCC peak rate = 25000
  C28: Connection completion timer  = 4

   LE ARP queue depth               = 5
   LE ARP cache size                = 10
   Best effort peak rate            = 25000
   Maximum config retries           = 3
   Packet trace                     = No
   No IPX interface configuration
   IP Encapsulation                 = IEEE-802.3

Ethernet Forum Compliant LEC Config>exit
LE Client config>exit
ATM Config>exit
```

Figure 279. Displaying the LEC Configuration

14.3.7 Configuring the Protocols

First, configure IP. The basic configuration sequence for this scenario is shown in Figure 280 on page 402. For more information on configuring IP, please see the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p ip
Internet protocol user configuration
IP config>add address 0
New address [0.0.0.0]? 7.7.7.210
Address mask [255.0.0.0]? 255.255.255.0
IP config>add add 5
New address [0.0.0.0]? 192.168.10.210
Address mask [255.255.255.0]?
IP config>add add 6
New address [0.0.0.0]? 192.168.2.210
Address mask [255.255.255.0]?
IP config>list add
IP addresses for each interface:
   intf  0   7.7.7.210        255.255.255.0    Local wire broadcast, fill 1
   intf  1                                     IP disabled on this interface
   intf  2                                     IP disabled on this interface
   intf  3                                     IP disabled on this interface
   intf  4                                     IP disabled on this interface
   intf  5   192.168.10.210   255.255.255.0    Local wire broadcast, fill 1
   intf  6   192.168.2.210    255.255.255.0    Local wire broadcast, fill 1
IP config>set router-id
Router-ID [0.0.0.0]? 10.10.10.210
IP config>set internal
Internal IP address [0.0.0.0]? 10.10.10.210
IP config>exit
```

Figure 280. Configuring IP

Now, configure Classical IP and IPX over ATM. The configuration sequence is shown in Figure 281 on page 403. Please note the following about this configuration:

Notes:

1. We added one client for IP and one for IPX on the ATM interface. The reason two clients were added is that each LIS must have a client and if there are to be IPX connections across ATM, an IPX client is needed.
2. There can only be one IPX client added as only one IPX network is supported on each ATM interface.
3. Up to 32 CIP clients can be added to each ATM interface.
4. As the IP client configured is not going to be a server, an internally assigned selector is used.
5. Be careful that you specify the correct interface. In this case we used ATM interface #5.

```
Config>p arp
ARP user configuration
ARP config>add atm
Interface Number [0]? 5
Protocol [IP]?
Client IP Address [0.0.0.0]? 192.168.10.210
This client is also a server? [No]:
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [No]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 400022100005
Select ESI [1]? 2
Use internally assigned selector? [Yes]:
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Service for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Service for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?

ARP config>add atm
Interface Number [0]? 5
Protocol [IP]? ipx
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [Yes]:
  (  1) Use burned in ESI
  (  2) 400022100005
Select ESI [1]? 2
Use internally assigned selector? [Yes]:
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Service for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
```

Figure 281. Configuring Classical IP

If you performed these steps correctly, you should be able to list the configuration and see something very similar to that shown in Figure 282 on page 404.

```
ARP config>list atm

ATM Arp Clients:
-------------------------------------------------
If: 5  Prot: 0  Addr: 192.168.10.210   ESI: 40.00.22.10.00.05  Sel: auto
Server: no   Refresh T/O: 5    AutoRefr: no    By InArp: yes  Validate PCR: no
Use Best Effort: yes/yes  (Control/Data)   Max B/W(kbps):      0
Cell Rate(kbps):  Peak:      0/     0      Sustained:      0/     0
Max SDU(bytes):   9188
-------------------------------------------------
If: 5  Prot: 7                          ESI: 40.00.22.10.00.05  Sel: auto
Refresh T/O: 5    AutoRefr: yes   By InArp: yes  Validate PCR: no
Use Best Effort: yes  (Data)              Max B/W(kbps):      0
Cell Rate(kbps):  Peak:      0            Sustained:      0
Max SDU(bytes):   9188
```

Figure 282. Displaying the ATM Configuration

Next, we define a PVC and an ARP server. The PVC is used as an IPX connection to the neighboring router (2216) across the ATM network. This is necessary as ATM is a non-broadcast network and therefore there is no means of resolving IPX addresses to ATM addresses.

The ARP server is needed as the CIP client is not a server. Therefore it needs a way of resolving IP addresses to ATM addresses and this function is provided by the ARP server.

The PVC and ARP records are listed after they have been configured. This is shown in Figure 283.

```
ARP config>add pvc
Interface Number [0]? 5
Protocol [IP]? ipx
Specify destination protocol address? (Yes or [No]): no
Permanent Virtual Circuit VPI, Range 0..255 [0]?
Permanent Virtual Circuit VCI, Range 0..65535 [0]? 100
ARP config>list pvc
ATM Arp Permanent Virtual Circuit Definitions
No. IF# Prot# P/S     Protocol     -> VPI / VCI    (Client Address)
1    5    7    P 00.00.00.00.00.00 ->   0 / 100
ARP config>add arp pri
Local Client IP Address [0.0.0.0]? 192.168.10.210
Private NSAP Address: Specify 40 digits
ATM Address []? 39098511111111111111110101400022160001AA
ARP config>list arp

ATM Arp Remote Server List:
   IP Address      Address / Sub Address
 192.168.10.210  39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.22.16.00.01.AA
ARP config>exit
```

Figure 283. Defining the PVC and the ARP Server

Next, configure IPX. The basic configuration sequence for this scenario is shown in Figure 284 on page 405. For more information on configuring IPX, please see

the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p ipx
IPX protocol user configuration
IPX config>enable ipx
IPX config>ena int 0
Configure an IPX network number for this interface.
Network number in hex [1]? 7777
IPX config>ena int 6
Configure an IPX network number for this interface.
Network number in hex [1]? 2222
IPX config>ena int 5
Configure an IPX network number for this interface.
Network number in hex [1]? 1010
```

Figure 284. Configuring IPX

If you have performed these steps correctly, you should be able to list the IPX configuration and see something very similar to that shown in Figure 285 on page 406.

```
IPX config>list all

IPX globally                enabled
Host number (serial line)   000000000000
Router Name (IPXWAN)
NodeID (IPXWAN)             0
Maximum networks                  32
Maximum total route entries       32
Maximum routes per dest. network  1
Maximum services                  32
Maximum Network Cache entries     64
Maximum Local Cache entries       64

List of configured interfaces:
                Frame                    SAP nearest  Split
Ifc  IPX net #  Encapsulation           server reply Horizon      IPXWAN
  0       7777  TOKEN-RING        MSB   Enabled      Enabled      N/A
  5       1010  N/A                     Enabled      Enabled      N/A
  6       2222  ETHERNET_802.3          Enabled      Enabled      N/A


RIP/SAP Timer Intervals and Pacing:
                SAP Interval  RIP Interval
Ifc  IPX net #   (Minutes)     (Minutes)    Pacing
  0       7777          1             1     Disabled
  5       1010          1             1     Disabled
  6       2222          1             1     Disabled
IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.

IPX Keepalive Filtering/Proxy Reply is not enabled on any interface.

IPX config>set max ser
New Service table size [32]? 64
IPX config>set max net
New Network table size [32]? 64
IPX config>exit
```

Figure 285. Displaying the IPX Configuration

Next, configure OSPF. The basic configuration sequence for this scenario is shown in Figure 286 on page 407. For more information on configuring OSPF, please see the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>enable ospf
Estimated # external routes [0]? 1000
Estimated # OSPF routers [0]? 40
OSPF Config>set inter
Interface IP address [0.0.0.0]? 192.168.2.210
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
OSPF Config>set int
Interface IP address [0.0.0.0]? 7.7.7.210
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
OSPF Config>set int
Interface IP address [0.0.0.0]? 192.168.10.210
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
OSPF Config>add neig
Interface IP address [0.0.0.0]? 192.168.10.210
IP Address of Neighbor [0.0.0.0]? 192.168.10.216
Can that router become Designated Router on this net [Yes]?
```

Figure 286. Configuring OSPF

If you performed these steps correctly, you should be able to list the OSPF configuration and see something very similar to that shown in Figure 287 on page 408.

```
OSPF Config>list all

                        --Global configuration--
                OSPF Protocol:          Enabled
                # AS ext. routes:       1000
                Estimated # routers:    40
                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
192.168.2.210     0.0.0.0              1      5       1     1     10     40
7.7.7.210         0.0.0.0              1      5       1     1     10     40
192.168.10.210    0.0.0.0              1      5       1     1     10     40

                        --Neighbor configuration--
                Neighbor Addr     Interface Address   DR eligible?
                192.168.10.216    192.168.10.210      yes
OSPF Config>exit
```

Figure 287. Displaying the OSPF Configuration

Next, configure the bridging function in the router. The basic configuration sequence for this scenario is shown in Figure 288. For more information on configuring the bridge, please see the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>ena brid
ASRT config>dis transp
Port Number [1]? 1
ASRT config>ena sour
Port Number [1]? 1
Segment Number for the port in hex(1 - FFF) [001]?
Bridge number in hex (0 - 9, A - F) [0]? 0
ASRT config>ena sr-tb
TB-Domain Segment Number in hex(1-FFF) [1]? feb
TB-Domain's MTU [1470]?
Bridge Virtual Segment Number in hex(1-FFF) [1]? aaa
ASRT config>enable dls
```

Figure 288. Configuring the Bridge Function

If you have performed these steps correctly, you should be able to list the ASRT configuration and see a screen similar to the one in Figure 289 on page 409.

```
ASRT config>list bridge

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

Bridge:                 Enabled                 Bridge Behavior: SR<->TB
                  +-----------------------------+
------------------| SOURCE ROUTING INFORMATION |------------------------------
                  +-----------------------------+
Bridge Number:          00                      Segments:          1
Max ARE Hop Cnt:        14                      Max STE Hop cnt:   14
1:N SRB:                Active                  Internal Segment:  0xAAA
LF-bit interpret:       Extended
                  +-------------------+
------------------| SR-TB INFORMATION |--------------------------------------
                  +-------------------+
SR-TB Conversion:       Enabled
TB-Virtual Segment:     0xFEB                   MTU of TB-Domain:  1470
                  +-----------------------------------+
------------------| SPANNING TREE PROTOCOL INFORMATION |----------------------
                  +-----------------------------------+
Bridge Address:         Default                 Bridge Priority:   32768/0x8000
STP Participation:      IEEE802.1d on TB ports, IBM-8209 and IBM-SRB Proprietar
y on SR ports
                  +-------------------------+
------------------| TRANSLATION INFORMATION |----------------------------------
                  +-------------------------+
FA<=>GA Conversion:     Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                  +------------------+
------------------| PORT INFORMATION |--------------------------------------
                  +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP:  Enabled
Port:   2      Interface        6      Behavior:    STB Only   STP:  Enabled

ASRT config>exit
```

Figure 289. Listing the Bridge Configuration

Next, configure Data Link Switching (DLSw). The basic configuration sequence for this scenario is shown in Figure 290 on page 410. For more information on configuring DLSw, please see the *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*.

```
Config>p dls
DLSw protocol user configuration
DLSw config>ena dls
DLSw config>open sap
Interface # [0]? 0
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 0
DLSw config>open sap
Interface # [0]? 6
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM' [4]? sna
SAPs 0 4 8 C opened on interface 6
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 10.10.10.216
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]? e
Neighbor Priority (H/M/L) [M]?
DLSw config>set srb
Enter segment number in hex (1-FFF) [000]? fab
DLSw config>exit
```

Figure 290. Configuring Data Link Switching

14.3.8 Saving the Configuration and Restarting the Router

When all configuration steps have been completed, restart the router. This will activate your configuration and is shown in Figure 291.

```
*restart
Are you sure you want to restart the gateway? (Yes or
[No]): y

Copyright Notices:

Licensed Materials - Property of IBM
Multiprotocol Routing Services
(C) Copyright IBM Corp. 1996
All Rights Reserved. US Gov. Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.

MOS Operator Control

*
```

Figure 291. Restarting the Router

14.3.9 Monitoring the Activity on the 2210

After the router restarts with the new configuration, you should use the talk 5 menus to check that the interfaces are working properly.

Figure 292 shows a configuration listing. You can use this command to see the details of any interface and to see what interfaces are up or down.

```
*t 5
+conf

Multiprotocol Routing Services

5765-B86 Feature 5105 V1 R1.0 PTF 0 RPQ 0 MRS.A7C

Boot ROM version  V2.20    Watchdog timer enabled    Auto-boot enabled
Time: 11:56:11    Saturday, June 30, 2012    Temp: 52C (125F)
Console Baud Rate: 9600    Auxiliary Baud Rate 9600

Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
7   IPX   NetWare IPX
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
26  DLS   Data Link Switching

Num Name  Feature
2   MCF   MAC Filtering

7 Networks:
Net Interface  MAC/Data-Link         Hardware                      State
0   TKR/0      Token-Ring/802.5      IBM Token-Ring                Up
1   PPP/0      Point to Point        SCC Serial Line               Down
2   PPP/1      Point to Point        SCC Serial Line               Down
3   PPP/2      Point to Point        SCC Serial Line               Down
4   PPP/3      Point to Point        SCC Serial Line               Down
5   ATM/0      ATM                   CHARM ATM                     Up
6   Eth/0      Ethernet/IEEE 802.3   CHARM ATM                     Up
```

Figure 292. Viewing the Status of the Interfaces

Figure 293 on page 412 shows an example of the stat command. This command shows you statistics for each interface.

```
+stat
Nt Interface   Unicast  Multicast      Bytes    Packets      Bytes
             Pkts Rcv   Pkts Rcv   Received      Trans      Trans
0  TKR/0          2676       8302     966146      46940    2036676
1  PPP/0             0          0          0          0          0
2  PPP/1             0          0          0          0          0
3  PPP/2             0          0          0          0          0
4  PPP/3             0          0          0          0          0
5  ATM/0        107928          0    9962916     112319    9731403
6  Eth/0         46645      41320    7879747      54353    4157878
```

Figure 293. Viewing the Status of the Interfaces

Figure 294 shows how to display the status of an individual interface, in this case, the emulated Ethernet LAN segment.

```
+int 6
                              Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
6  6   Eth/0            0    0          1          2            0

  Ethernet/IEEE 802.3 MAC/data-link on CHARM ATM interface

          LEC Statistics

   In Octets.high     = 0
   In Octets.low      = 7359818
   In Discards        = 0
   In Errors          = 0
   In Unknown Protos  = 0
   Out Octets.high    = 0
   Out Octets.low     = 1665099
   Out Discards       = 3382
   Out Errors         = 0

   In Frames          = 46711
   Out Frames         = 54411
   In Bytes           = 7890559
   Out Bytes          = 4161500
```

Figure 294. Viewing the Status of an ELAN

Figure 295 on page 413 shows an IP dump. You can use this to list the IP networks that the router knows about. This list includes the networks directly attached and ones learned using an IP routing protocol (in this case, OSPF).

```
+p ip
IP>dump
Type   Dest net         Mask      Cost     Age       Next hop(s)

Sbnt   7.0.0.0          FF000000  1        2467      None
 SPF*  7.7.7.0          FFFFFF00  1        2489      TKR/0
Sbnt   9.0.0.0          FF000000  1        2467      None
 SPF   9.24.104.0       FFFFFF00  2        2477      192.168.10.216
Sbnt   10.0.0.0         FF000000  1        2467      None
 SPF   10.10.10.210     FFFFFFFF  0        2497      SINK/0
 SPF   10.10.10.216     FFFFFFFF  1        2477      192.168.10.216
 SPF*  192.168.2.0      FFFFFF00  1        2484      Eth/0
 Dir*  192.168.10.0     FFFFFF00  1        2467      ATM/0
 SPF   192.168.10.210   FFFFFFFF  0        2497      ATM/0
 SPF   192.168.10.216   FFFFFFFF  1        2477      192.168.10.216

Routing table size: 768 nets (49152 bytes), 11 nets known
```

Figure 295. Displaying an IP Dump

Figure 296 shows an example of using the IP ping command to ping from the 2210 across the CIP segment through the 2216 to the legacy token-ring port on the 2216.

```
IP>ping 9.24.104.203
PING 192.168.10.210 -> 9.24.104.203: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 9.24.104.203: icmp_seq=0. ttl=64. time=0. ms
56 data bytes from 9.24.104.203: icmp_seq=1. ttl=64. time=0. ms

----9.24.104.203 PING Statistics----
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
IP>exit
```

Figure 296. Using the IP Ping Command to Test IP Routing

Figure 297 on page 414 shows an IPX dump. You can use this to list the IPX networks that the router knows about. This list includes the networks directly attached and ones learned using the RIP protocol.

```
+p ipx
IPX>dump

8 route entries used out of 32
8 net entries used out of 32

Type     Dest net Hops Delay  Age(M:S)   via Router
 Dir       1010    0     1      0: 0       1010/400022100005 5-ATM/0
 Dir       7777    0     1      0: 0       7777/400022100000 0-TKR/0
 Dir       2222    0     1      0: 0       2222/400022100006 6-Eth/0
 RIP          9    1     2      0:10       1010/400022160001
 RIP   30AA0F92    2     3      0:10       1010/400022160001
 RIP   31ECF1DD    2     3      0:10       1010/400022160001
 RIP   325521DE    1     2      0:10       2222/08005A998151
 RIP   53914BBA    2     3      0:10       1010/400022160001
```

Figure 297. Displaying an IPX Dump

Figure 298 shows an example of using the IPX ping command to ping from the 2210 across the CIP segment through the 2216 ATM interface to the legacy token-ring adapter in the 2216.

```
IPX>ping
Destination network number [1]? 9
Destination node number []? 400022160000
IPXPING 9/400022160000: 56 data bytes
56 data bytes from 9/400022160000: hops=1 time=0 ms
56 data bytes from 9/400022160000: hops=1 time=0 ms
56 data bytes from 9/400022160000: hops=1 time=0 ms
56 data bytes from 9/400022160000: hops=1 time=0 ms
56 data bytes from 9/400022160000: hops=1 time=0 ms

----9/400022160000 IPXPING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/ave/max = 0/0/0
IPX>exit
```

Figure 298. Using the IPX Ping Command to Test IPX Routing

Figure 299 on page 415 shows how to display the active TCP and DLSw sessions. Note that the SNA traffic is being encapsulated on the TCP session that connects the two routers.

```
+p dls
Data Link Switching Console
DLSw>list tcp sess all
   Group   IP Address      Conn State     CST  Version  Active Sess Sess Creates
   ------- --------------- -------------- ---  -------- ----------- ------------
1          10.10.10.216    ESTABLISHED     a   AIW V2R0      1           6
DLSw>list dls ses all
         Source         Destination      State     Flags    Dest IP Addr    Id
     --------------  --------------  ---------  -------  --------------  ----
   1 4000FFFF0000 04  400052005215 04  CONNECTED           10.10.10.216       5
DLSw>ex
```

Figure 299. Displaying Active DLS Sessions

Figure 300 shows an example of how to display the VCCs in this case for the emulated Ethernet segment.

```
+net 6
ATM Emulated LAN Console
LEC+list vcc

                 LEC VCC Table

   Handle  VPI     VCI   Type     Status
   -------------------------------------
       8     0     375   Cntrl    Ready
       9     0     376   Cntrl    Ready
      10     0     377   Mcast    Ready
      11     0     378   Mcast    Ready
      13     0     380   Data     Ready
      16     0     383   Data     Ready
      17     0     384   Data     Ready

LEC+exit
```

Figure 300. Displaying VCCs in the LAN Emulation Client

Figure 301 on page 416 shows an example of how to display all the VCCs for the ATM interface.

```
+net 5
ATM Console
ATM+inter
ATM Interface Console
ATM Interface+lis vcc

 Conn    Conn                          Sap   Frames       Frames     Bytes        Bytes
 Handle  Type  VPI  VCI    FrameSap     Type  Transmitted  Received   Transmitted  Received
 ------ -----  ---  ----  ----------  ----  -----------  ---------  -----------  ----------
     17     P-P    0   384    3154A8C0  Buff         765         404       62778       25124
     16     P-P    0   383    3154A8C0  Buff        5284        3015      489500      345806
     14     P-P    0   381    31B1C8F4  Buff       11519       12084      918959     1351234
     13     P-P    0   380    3154A8C0  Buff         539         542       33418       33828
     11    P-MP    0   378    3154A8C0  Buff           0       41912           0     2999300
     10     P-P    0   377    3154A8C0  Buff       41454           0     2935836           0
      9    P-MP    0   376    3154A8C0  Buff           0       41249           0     4454892
      8     P-P    0   375    3154A8C0  Buff       41062          14     4434696        1512
      1    SAAL    0     5           0   N/A        1413        1413       14960       14808
 0     N/A    0   100    31B1E014  Buff         935        2752       78004      482773
      2    ILMI    0    16           0   N/A        4110        4110      219415      265003
ATM Interface+exit
ATM+exit
```

Figure 301. Displaying Active VCCs

14.3.10 Monitoring the Activity on the 2216

Now, perform some checks of the configuration on the 2216 side. From the talk 5 menus, check that the interfaces are working properly.

Figure 302 shows an example of listing the machine configuration to see which interfaces are active.

```
+conf

Multiprotocol Access Services

5765-B87 Feature 2802 V1 R1.0 PTF 0 RPQ 0 MAS.A01 cc1_11b


Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
7   IPX   NetWare IPX
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol

Num Name  Feature
2   MCF   MAC Filtering

3 Networks:
Net Interface  MAC/Data-Link         Hardware                      State
0   TKR/0      Token-Ring/802.5      Token-Ring                    Up
1   ATM/0      ATM                   CHARM ATM                     Up
```

Figure 302. Displaying the 2216 Interface Status

Figure 303 on page 417 shows an example of how to display the active VCCs on the ATM interface.

```
+net 1
ATM Console
ATM+int
ATM Interface Console
ATM Interface+list vcc

 Conn     Conn                          Sap   Frames        Frames     Bytes        Bytes
 Handle   Type   VPI  VCI    FrameSap   Type  Transmitted   Received   Transmitted  Received
 ------ -------  ---  ----  ----------  ----  -----------  ----------  -----------  ----------
     5      P-P    0   168     1440FE8  Buff          10           9          496         452
     4      P-P    0   167     1441180  Buff          20          18         1520        1416
     1     SAAL    0     5     13375B4  Buff          24          24          304         480
     0      N/A    0   200     14428A0  Buff          39           3         5693         164
     2     ILMI    0    16     13375B4  Buff          49          49         2540        2966

ATM Interface+list users

 UserHandle  AdapFrSap   BufFrSap    ATM Address
 ----------  ----------  ----------  ------------------------------------------------------------
    1442888           0     14428A0  39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.22.16.00.01.C8
    1441168           0     1441180  39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.22.16.00.01.AA
    1440FD0           0     1440FE8  39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.22.16.00.01.02

ATM Interface+exit
ATM+exit
```

Figure 303. Displaying ATM Connections

Figure 304 shows an example of using the IP ping command to ping from the 2216 across the CIP segment through the 2210 to a PC attached to the Ethernet emulated LAN.

```
+p ip
IP>ping 192.168.2.89
PING 192.168.10.216 -> 192.168.2.89: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.168.2.89: icmp_seq=0. ttl=254. time=0. ms
56 data bytes from 192.168.2.89: icmp_seq=1. ttl=254. time=0. ms
56 data bytes from 192.168.2.89: icmp_seq=2. ttl=254. time=0. ms

----192.168.2.89 PING Statistics----
3  packets transmitted, 3  packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
IP>exit
```

Figure 304. Using the IP Ping Command to Test IP Routing

Figure 305 on page 418 shows an IPX dump. You can use this to list the IPX networks that the router knows about. This list includes the networks directly attached and ones learned using the RIP protocol.

```
+p ipx
IPX>dump

8 route entries used out of 32
8 net entries used out of 32

Type     Dest net Hops Delay  Age(M:S)   via Router
 Dir       1010    0     1      0: 0       1010/400022160001 1-ATM/0
 Dir          9    0     1      0: 0          9/400022160000 0-TKR/0
 RIP       2222    1     2      0:35       1010/400022100005
 RIP       7777    1     2      0:35       1010/400022100005
 RIP   30AA0F92    1     2      0:55          9/400052005240
 RIP   31ECF1DD    1     2      0:35          9/08005A0D2860
 RIP   325521DE    2     3      0:35       1010/400022100005
 RIP   E46366AE    1    24      0: 0          9/0001CB32C00A
IPX>exit
```

Figure 305. Displaying an IPX Dump

Figure 306 shows how to display active DLSw sessions. Note that the first attempt shows that the circuit is being established and by the time the command is issued again, the status changes to connected.

```
+p dls
Data Link Switching Console

DLSw>list dls sess all
         Source         Destination      State     Flags    Dest IP Addr    Id
     --------------  --------------  ---------  -------  --------------  ----
   1 400001240000 04  4000FFFF0000 04  CIRC_EST           10.10.10.210      10
DLSw>list dls sess all
         Source         Destination      State     Flags    Dest IP Addr    Id
     --------------  --------------  ---------  -------  --------------  ----
   1 400001240000 04  4000FFFF0000 04  CONNECTED          10.10.10.210      10
```

Figure 306. Displaying DLSw Sessions

This completes the configuration steps required for scenario 3.

Chapter 15. Problem Determination and System Monitoring

This chapter describes the function provided on the IBM 2210 and IBM 2216 for monitoring ATM traffic. It will help in problem determination and is shown here to give an idea of what type of monitoring is available for ATM. The actual output from the monitor isn't explained in this chapter, as it is detailed in the *Event Logging System Messages Guide, SC30-3682-04*.

15.1 Event Logging System

There are two ways event logging can be enabled for the 2210 or 2216. Event logging can be enabled from the configuration prompt on the command line under talk 6. If this is done the 2210 or 2216 will start monitoring the traffic immediately upon a reload, or a restart in the case of the 2210. Event logging can also be enabled under talk 5 on the command line. If it is enabled this way the 2210 or 2216 will start monitoring traffic instantly. It will continue to monitor the traffic until the event logging is disabled or the router is reloaded, or restarted in the case of the 2210. If you are trying to monitor the traffic during connection to the ATM network then the best way would be by enabling monitoring under talk 6. This way you won't miss the traffic that is sent and received while you are trying to enable event logging.

To enable and then disable event logging the following steps need to be performed:

1. Enter the event logging system under talk 5 or talk 6.
2. Enable the subsystem(s) that you want displayed.
3. To view the logging output you need to enter the monitoring console using the command:

   ```
   talk 2
   ```

4. To disable event logging you need to re-enter the event logging system and disable the subsystem(s).

Note: If you want to clear all the monitored traffic that has been stored, you can use the command:

```
flush 2
```

An example of this is shown in Figure 307 on page 420.

15.1.1 Using the Event Logging System

This section shows the commands for enabling and disabling event logging. There are also examples of typical output produced using the event logging system.

There are a number of different subsystems that can be monitored for ATM. You will need to enable different subsystems depending on the type of problem that you are experiencing. The subsystems available for monitoring ATM traffic are:

- ARP
- ATM
- LEC

- LECS
- LES
- ILMI
- SAAL
- SVC

A number of these subsystems may need monitoring depending on the problem. The only two of no use are the LES and LECS subsystems. The 2210 and 2216 don't support a LES/BUS or a LECS, therefore these subsystems will not produce any output.

Figure 307 shows the process of enabling the ARP subsystem. Initially the event logging system is entered and the ARP subsystem is enabled. Before entering the monitoring system, using the command:

```
talk 2
```

Any messages that are stored are cleared by using the command:

```
flush 2
```

Once the messages have been cleared you can monitor any ARP messages that are being produced by entering the monitoring system as shown in Figure 307. From the produced messages it can be seen that some ATM_ARP frames are being received. There are also some IP ARP packets being received that aren't destined for this router.

```
*talk 5
+event
Event Logging System user console
ELS>display subsystem arp all
ELS>exit
+
*flush 2
*talk 2

 ARP.051: ATM CIP atmArpRcvFrame: (prot = 806) nt 3 int ATM/0
 ARP.051: ATM CIP atmArpRcvFrame: (prot = 800) nt 3 int ATM/0
 ARP.051: ATM CIP atmArpRcvFrame: (prot = 800) nt 3 int ATM/0
 ARP.002: Pkt in 1 6 800 nt 0 int TKR/0
 ARP.016: unkn dst prot ad nt 0 int TKR/0
 ARP.051: ATM CIP atmArpRcvFrame: (prot = 800) nt 3 int ATM/0
 ARP.002: Pkt in 1 6 800 nt 0 int TKR/0
 ARP.016: unkn dst prot ad nt 0 int TKR/0
 ARP.002: Pkt in 1 6 800 nt 0 int TKR/0
 ARP.016: unkn dst prot ad nt 0 int TKR/0
```

Figure 307. Enabling and Viewing Event Logging of the ARP Subsystem

In the example shown in Figure 308 on page 421, it can be seen that you need to first disable the subsystem already being displayed. In this case the command:

```
nodisplay subsystem arp all
```

will prevent any ARP traffic from being monitored. Then when the ATM subsystem is set to display, only ATM messages will be monitored and

displayed. The meaning of the messages can be found in the *Event Logging System Messages Guide, SC30-3682-04* as mentioned previously.

```
*talk 5
+event
Event Logging System user console
ELS>nodisplay subsystem arp all
ELS>dis sub atm all
ELS>exit
+
*flush 2
*talk 2

 ATM.154: Timer set alarm, nt 3, ndx = 15, callback = 14470C0
 ATM.155: Timer set alarm, nt 3, type = 1, element = 1375C38
 ATM.154: Timer set alarm, nt 3, ndx = 15, callback = 14470DC
 ATM.155: Timer set alarm, nt 3, type = 2, element = 1375C54
 ATM.035: Function atmPlaceCall called, nt 3 int ATM/0
 ATM.066: API, place call, nt 3 int ATM/0, addr 390985111111111111
111101014000221600030 2
 ATM.035: Function conn_mgr_200::place_call called, nt 3 int ATM/0
 ATM.123: conn_mgr place_call ntrd, nt 3 int ATM/0
```

Figure 308. Enabling and Monitoring the ATM Subsystem

Figure 309 shows the disabling of the ATM subsystem and the enabling of the LEC subsystem. The traffic is then viewed from the talk 2 monitoring system.

```
*talk 5
+event
Event Logging System user console
ELS>nodisplay subsystem atm all
ELS>dis sub lec all
ELS>exit
+
*flush 2
*talk 2

 LEC.015: nt 4 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 4 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 4 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 4 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 4 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 4 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 4 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.002: nt 4 Func entry lec_ART::alarm_rang
 LEC.002: nt 4 Func exit  lec_ART::alarm_rang
```

Figure 309. Enabling and Monitoring the LEC Subsystem

Figure 310 on page 422 shows some typical traffic generated when monitoring the SAAL subsystem. These messages were obtained using the same technique outlined for the previous subsystems.

```
 SAAL.001: nt 3 Function saal_wrapper::cpaal_tx_data_request entered
 SAAL.002: nt 3 Function saal_wrapper::cpaal_tx_data_request extd
 SAAL.001: nt 3 Function xmitr::reset_tx_pd entered
 SAAL.002: nt 3 Function sscop::alarm_rang extd
 SAAL.001: nt 3 Function sscop::cpaal_rx_data_indication entered
 SAAL.001: nt 3 Function sscop::pdu_stat entered
 SAAL.026: nt 3 recv status: 000000C1 00000046 0B00003C 00000028, len=12
 SAAL.001: nt 3 Function sscop::txdata_handler entered
 SAAL.002: nt 3 Function sscop::txdata_handler (no poll) extd
 SAAL.002: nt 3 Function sscop::pdu_stat extd
 SAAL.002: nt 3 Function sscop::cpaal_rx_data_indication extd
 SAAL.001: nt 3 Function sscop::cpaal_rx_data_indication entered
 SAAL.001: nt 3 Function sscop::pdu_poll entered
 SAAL.026: nt 3 recv poll: 000000C3 0A00003C 0200FFFF 00000028, len=8
```

Figure 310. Monitoring the SAAL Subsystem

Figure 311 shows some typical traffic generated when monitoring the SVC subsystem. These messages were obtained using the same technique outlined for the previous subsystems.

```
 SVC.015: Enter function DeleteThisCall: conn hndl,ID,state,29,6,0
 SVC.018: Exit remove_from_pend_list: ID,Flag,6,128
 SVC.002: deleting pnding call=21277856
 SVC.015: Enter function UpdateCallState: conn hndl,old state,
new state,29,0,0
 SVC.025: received data = 09030000 07058000 68598000 098400E6
 SVC.002: find_call=0
 SVC.024: Received message,  type=5
 SVC.020: Received Setup,conn hndl=30,ID=7,state=0
 SVC.015: Enter function UpdateCallState: conn hndl,old state,
new state,30,0,6
```

Figure 311. Monitoring the SVC Subsystem

The ILMI subsystem was monitored using the same method and produced the output shown in Figure 312 on page 423.

```
ILMI.020: nt3 snt Get Response
ILMI.020: nt3 snt GetNext
ILMI.008: nt3 recv Get Response
ILMI.003: nt3 ntrd func responsef, state=ILMI_PREFIX_READY
ILMI.008: nt3 recv Get
ILMI.003: nt3 ntrd func getf, state=ILMI_PREFIX_READY
ILMI.011: nt3 Snd GetRsp Vpi+Vci, state=ILMI_PREFIX_READY
ILMI.003: nt3 ntrd func BuildGetResp, state=ILMI_PREFIX_READY
ILMI.020: nt3 snt Get Response
ILMI.023: nt3 ntrd func alloc_atm_addr, addr=400022160003,sel=02
ILMI.004: nt3 ntrd func LockSelector, mac indx, sel0
ILMI.004: nt3 ntrd func FindSelector, mac indx=0
ILMI.019: nt3 Exit FindSelector,rc,sel,0,2
ILMI.019: nt3 Exit LockSelector,rc,hndl,0,2
```

Figure 312. Monitoring the ILMI Subsystem

The event logging system can be very helpful when you are experiencing a problem with your network. By enabling the correct subsystems the traffic through the router can be monitored. This should help identify the cause of the problem. It is recommended that the event logging system be used as an initial step to eliminate problems.

Part 4. Appendixes

Appendix A. Special Notices

This publication is intended to help customers and system specialists to implement networks incorporating the IBM 2210 and the IBM 2216 in their SNA or ATM environment. The information in this publication is not intended as the specification of any programming interfaces that are provided by the IBM 2210 and its MRS or the IBM 2216 and its MAS. See the PUBLICATIONS section of the IBM Programming Announcement for the IBM 2210 and its MRS and the IBM 2216 and its MAS for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

APPN
IBM
NetView
OS/2
RT
400
ESCON
MVS/ESA
Nways
OS/390
VTAM

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix B. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

B.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 431.

- *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios - Volume I*, SG24-4957-00
- *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios - Volume I*, SG24-4446-02
- *APPN Architecture and Product Implementations Tutorial*, SG24-3669
- *Campus ATM Design Guidelines*, SG24-5002-00
- *Asynchronous Transfer Mode (ATM) Technical Overview*, SG24-4625-00
- *Understanding and Using the IBM MSS Server*, SG24-4915-00
- *Internetworking over ATM: An Introduction*, SG24-4699-00

B.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042

B.3 Other Publications

These publications are also relevant as further information sources:

- *Nways Multiprotocol Routing Services Software User's Guide*, SC30-3881
- *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 1*, SC30-3680
- *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3865
- *Nways Multiprotocol Access Services Software User's Guide*, SC30-3886
- *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*, SC30-3884
- *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885

- *Nways Event Logging System Messages Guide*, SC30-3682-04
- *Configuration Program User's Guide for Nways Multiprotocol Access Services and Multiprotocol Routing Services*, GC30-3830
- *SNA APPN Archiecture Reference*, SC30-3422
- *VTAM Network Implementation Guide V4R4 for MVS/ESA*, SC31-8370
- *VTAM Resource definition Reference V4R4 for MVS/ESA*, SC31-8377

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at http://www.redbooks.ibm.com.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO: type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Web Site on the World Wide Web**

  http://w3.itso.ibm.com/redbooks

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (http://www.redbooks.ibm.com/redpieces.htm). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** — send orders to:

	IBMMAIL	**Internet**
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29570	Calgary, Alberta T2P 3N5	DK-3450 Allerød
Raleigh, NC 27626-0570	Canada	Denmark
USA		

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1)001-408-256-5422 (Outside USA)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com
- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (http://www.redbooks.ibm.com/redpieces.htm). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number
- Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

ITSO Redbook Evaluation

IBM 2210 Nways Multiprotocol Router IBM 2216 Nways Multiaccess Connector
SG24-4956-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@vnet.ibm.com

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes____ No____

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

_____

_____

_____

_____

_____

This soft copy for use by IBM employees only.

Printed in U.S.A.