IBM

International Technical Support Centers

The IBM 6611 Network Processor

GG24-3870-00

The IBM 6611 Network Processor

Document Number GG24-3870-00

September 1992

International Technical Support Center
Raleigh

Take Note!

Before using this information and the product it supports, be sure to read the general information under "Special Notices" on page xiii.

First Edition (September 1992)

This edition applies to Version 1 Release 1 of the IBM Multiprotocol Network Program (5648-016) for use with the IBM 6611 Network Processor.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

An ITSC Technical Bulletin Evaluation Form for readers' feedback appears facing Chapter 1. If this form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Center
Dept. 985, Building 657
P.O. Box 12195
Research Triangle Park, NC 27709

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Abstract

This document describes the IBM 6611 Network Processor and the IBM Multiprotocol Network Program (5648-016). It provides an introduction to the concepts, functions and use of the 6611 Network Processor and Multiprotocol Network Program in various environments.

This document is intended for network managers, network architects, systems programmers and systems engineers who need to implement networks which incorporate the 6611 Network Processor with the Multiprotocol Network Program. Some knowledge of networking architectures and protocols is assumed.

CO (291 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to help customers and systems engineers to implement networks based on the IBM 6611 Network Processor when used with the IBM Multiprotocol Network Program (5648-016). The information in this publication is not intended as the specification of any programming interfaces that are provided by the IBM 6611 Network Processor and the IBM Multiprotocol Network Program (5648-016). See the PUBLICATIONS section of the IBM Programming Announcement for the IBM 6611 Network Processor and the IBM Multiprotocol Network Program (5648-016) 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 Commercial Relations, IBM Corporation, Purchase, NY 10577.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. 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 document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

You can reproduce a page in this document as a transparency, if that page has the copyright notice on it. The copyright notice must appear on each page being reproduced.

The following terms, which are denoted by an asterisk (*) in this publication, are trademarks of the International Business Machines Corporation in the United States and/or other countries:

ACF/VTAM
AIX
AIXwindows
Enterprise System/9000
IBM
Micro Channel
MVS/ESA
NetView
NetView/6000
Operating System/2
OS/2
Personal System/2
POWER Architecture
PS/2
RISC System/6000
VM/ESA
VTAM

The following terms, which are denoted by a double asterisk (**) in this publication, are trademarks of other companies:

AppleTalk is a trademark of Apple Computer Inc.
Digital and DECnet are trademarks of Digital Equipment Corporation
Intel is a trademark of Intel Corporation
IPX, Internet Packet Exchange, NetWare and Novell are trademarks of Novell Inc.
Microsoft Windows is a trademark of Microsoft Corporation
UNIX is a trademark of Unix System Laboratories, Inc.
Xerox, Xerox Network Systems and XNS are trademarks of Xerox Corporation

Preface

This document is intended to assist customers and systems engineers implement networks based on the IBM 6611 Network Processor and its co-requisite IBM Multiprotocol Network Program (5648-016).

The document is organized as follows:

- Part 1, "About the IBM 6611"

  This section provides information that can be used to gain a greater understanding of the features, functions and roles of the 6611 Network Processor.

  - Chapter 1, "Introduction to Networks, Protocols and Internetworking"

    This chapter explains important concepts that should be well understood prior to reading subsequent chapters.

  - Chapter 2, "Overview of 6611 Hardware and Functions"

    This chapter describes the features and functions of the 6611 Network Processor.

- Part 2, "Using the IBM 6611"

  This section provides information on the use of various 6611 Network Processor functions.

  - Chapter 3, "Configuring the 6611"

    This chapter describes the use of the configuration program for the 6611 Network Processor.

  - Chapter 4, "Managing the 6611"

    This chapter describes the use of the management capabilities of the 6611 Network Processor.

- Part 3, "Example Scenarios"

  This section describes various example scenarios that have been constructed to demonstrate practical applications of the 6611 Network Processor and how they might be implemented.

  - Chapter 5, "Basic TCP/IP Example Scenario"

    This chapter describes a TCP/IP network based on the 6611 Network Processor. It also illustrates the configuration of the 6611 Network Processor management capabilities and is used as the basis for the other example scenarios.

  - Chapter 6, "Remote Source Route Bridging Example Scenario"

    This chapter illustrates the use of the 6611 Network Processor remote bridging functions.

  - Chapter 7, "Data Link Switching Example Scenario"

    This chapter illustrates the use of the 6611 Network Processor data link switching function for the transport of SNA and NetBIOS.

- Part 4, "Appendix"

  This section describes information that can be used as a reference.

- Appendix A, "TCP/IP Routing Table Maintenance Protocols"

  This appendix describes the TCP/IP routing table maintenenace protocols in general terms.

- Appendix B, "Configuration Reports for Example Scenarios"

  This appendix is a listing of the configuration reports that were generated as a result of each of the example scenarios.

Related Publications

The following publications are considered particularly suitable for a more detailed discussion of the topics covered in this document.

Prerequisite Publications

- *IBM 6611 Network Processor: Introduction and Planning Guide*, GK2T-0334
- *IBM Multiprotocol Network Program: User's Guide*, SC30-3559
- *IBM 6611 Network Processor: Installation and Service Guide*, GA27-3941
- *IBM 6611 Network Processor: Operations Pocket Guide*, GX27-3909
- *IBM 6611 Network Processor: Network Management Reference*, GC30-3567

Additional Publications

- *Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture*, SC31-6144
- *Xerox System Integration Standard: Internet Transport Protocols*, XSIS-028112, Xerox Corporation, 1981
- *Advanced NetWare, V2.0 Internet Packet Exchange Protocol with Asynchronous Event Scheduler*, Novell Inc., 1986
- *DECnet Digital Network Architecture Phase IV Routing Layer Functional Specification*, Digital Equipment Corporation
- *AppleTalk Phase 2 Protocol Specification*, Apple Computer Inc., 1990

ITSC Publication Structure - LANs

The rapid evolution of Local Area Network (LAN) products has resulted in the availability of a wide variety of documents, including the reference materials available with each product and additional technical planning and support material available from various development and support groups.

To assist users in locating appropriate, up-to-date information the International Technical Support Center is structuring its Local Area Network documentation into a library of publications.

Each publication is produced to address some technical requirements of a specific audience as described in the abstract and preface of the document. Because the ITSC publications are intended to complement, but not replace reference material available with the products themselves, each document also provides a bibliography of related publications.

The International Technical Support Center publications related to local area networks have been planned with the following structure in mind to simplify the problem of locating up-to-date information.

1. Overview manuals which provide tutorial information and cross-product conceptual and planning information.
2. Installation manuals which complement product reference material by describing the experiences of the ITSC in installing particular products within a total system. These documents do not address all installation parameters or options as do the product reference materials, but are intended to highlight those aspects of installation which have the greatest impact on successful use of the product, including the relationship between a specific product and other network or system products.
3. Network design and management manuals which describe trade-offs and considerations for managing or planning Local Area Networks.

The current library contains the following publications:

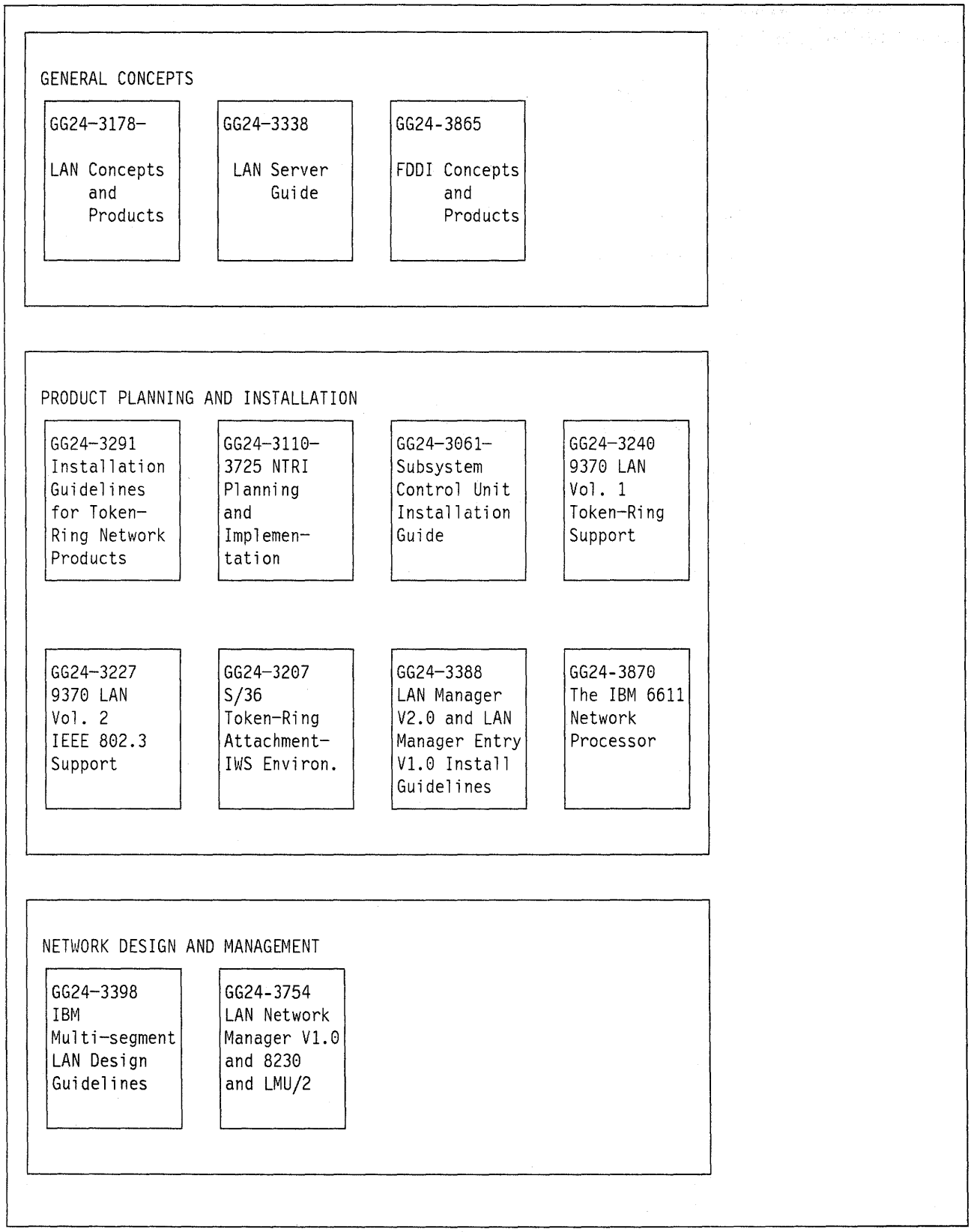


Figure 1. Existing Bulletins in ITSC LAN Bulletin Library

Acknowledgements

The advisor for this project was:

Ray Collins
International Technical Support Center, Raleigh

The authors of this document were:

Ivan Van Netelbosch
IBM Belgium

James Kelly
IBM Australia

This publication is the result of a residency conducted at the International Technical Support Center, Raleigh.

Thanks to the following people for the invaluable advice and assistance provided in the production of this document:

Rich Zick
Network RTE Systems Software Development

Part 1. About the IBM 6611

Chapter 1. Introduction to Networks, Protocols and Internetworking

This chapter provides an introduction to computer communication networks, protocols and internetworking. It defines various concepts and terminology that are used in subsequent chapters to describe the features, functions and use of the IBM* 6611 Network Processor with the IBM Multiprotocol Network Program (5648-016).

1.1 Networks

A *computer communication network* (or more simply a *network*), is the infrastructure that enables computer systems to exchange information. A typical network of the type that could be constructed using the 6611 Network Processor is illustrated in Figure 2 on page 4.

Networks consist of a combination of nodes connected by data links. Some data links are quite simple, for example the point-to-point digital data services provided by most common carriers. Other data links are quite complex and are networks in themselves, for example the CCITT X.25 services provided by many common carriers, or the local area networks provided by many vendors. These data links that are networks in themselves will be referred to as *data link networks*.

The nodes that are interconnected by data links and data link networks are either:

- *End nodes* which can exchange information with other nodes to which they are directly connected via data links and data link networks.
- *Intermediate nodes* which can forward information between different data links and data link networks, allowing end nodes which are not directly connected by a common data link or data link network to exchange information using the services of the intermediate node.

Internetworking is the function performed by intermediate nodes when they forward information between data links and data link networks on behalf of end nodes. This is described in more detail in 1.3, "Internetworking and Bridging" on page 11.

1.2 Protocols

A *computer communication network protocol* (or more simply a *protocol*), is a specification which describes how computer systems can exchange information across some form of computer communication network. In practice it is usual to define a suite of related protocols to enable effective information exchange. Examples of such protocol suites that are in wide use include:

- TCP/IP (Transmission Control Protocol/Internet Protocol) developed for the US Department of Defense
- SNA (Systems Network Architecture) developed by International Business Machines Corporation
- DECnet** developed by Digital Equipment Corporation
- XNS** (Xerox Network Systems**) developed by Xerox Corporation

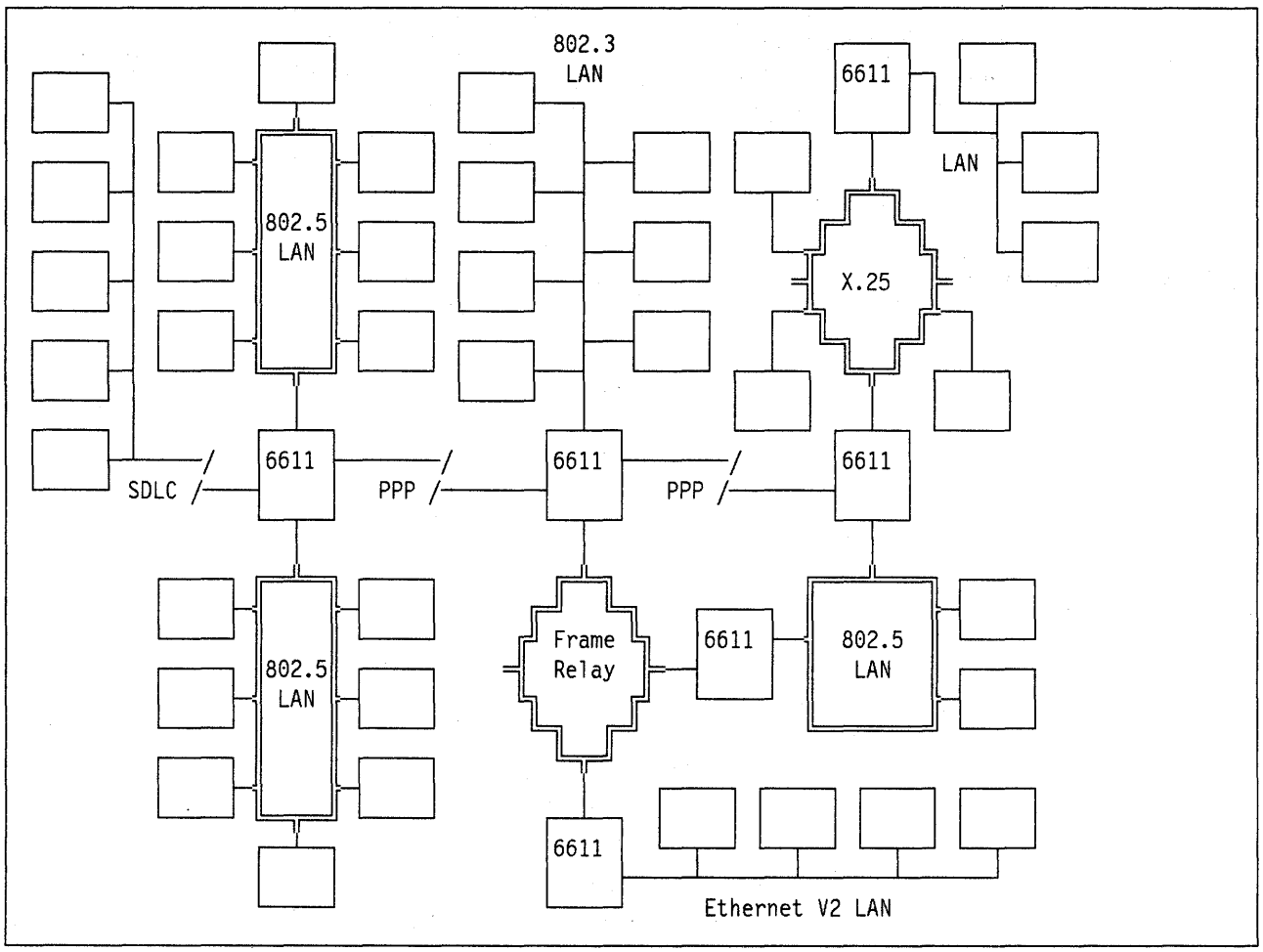


Figure 2. A Typical Network Using the 6611 Network Processor

- NetWare** developed by Novell Inc.
- AppleTalk** developed by Apple Computer Inc.
- OSI (Open Systems Interconnection) developed by the International Organization for Standardization
- NetBIOS (Network Basic Input Output System) developed by International Business Machines Corporation

Each of these protocol suites are, in general, incompatible with each other, that is a computer system that implements one protocol suite is unable to exchange information effectively with a computer system that implements a different protocol suite. Also, in many cases computer systems that implement different protocol suites have been unable to make use of a common computer communication network even if they are only required to exchange information with computer systems which implement the same protocols. This incompatibility has led many organizations to construct several distinct and unconnected computer communication networks, in other words one network for each of the protocol suites that their computer systems implement.

The IBM 6611 Network Processor when used with the IBM Multiprotocol Network Program (5648-016) provides a solution for those organizations which want to construct a single computer communications network capable of supporting computer systems that implement a wide variety of protocol suites.

The sections that follow provide a summary of protocol concepts which may be helpful in understanding the functions that the 6611 Network Processor provides, and how to implement computer communications networks based on the 6611 Network Processor that support multiple protocol suites. A more detailed discussion of the protocols supported by the 6611 Network Processor can be found in the "Understanding the Protocols" part of the *IBM 6611 Network Processor: Introduction and Planning Guide*.

1.2.1 The OSI Reference Model

When discussing computer communication network protocols it is convenient to make use of the OSI Reference Model, which is illustrated in Figure 3.

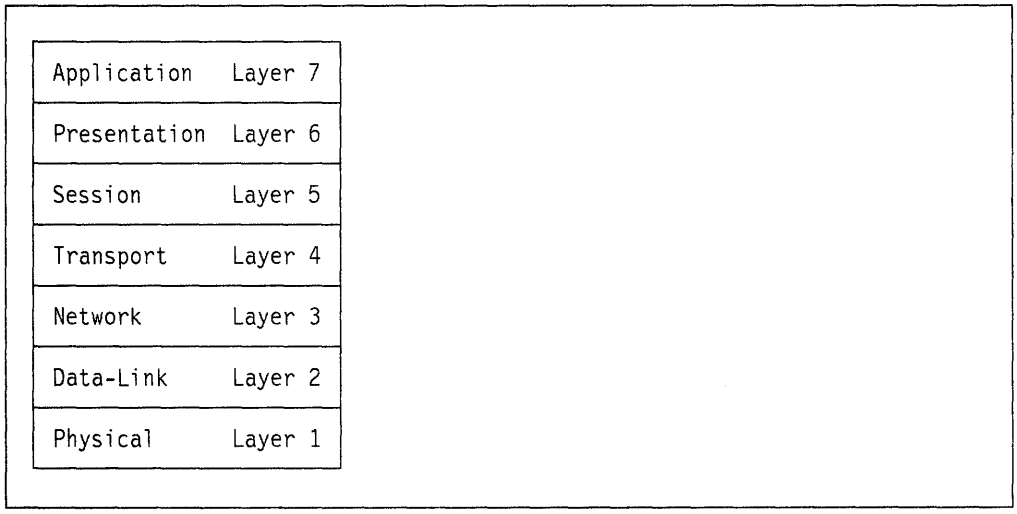


Figure 3. The OSI Reference Model

Most protocol suites do not fit exactly within the OSI Reference Model (except for the OSI protocol suite). However, there are elements of most protocol suites that correspond to some or all of the layers within the OSI Reference Model. Therefore the OSI Reference Model can be used as the basis for discussing these elements, particularly those implemented by the 6611 Network Processor.

The 6611 Network Processor provides *internetworking* services, which relate to the lower three layers of the OSI Reference Model, that is the physical, data link and network layers. These lower three layers are discussed in the following sections.

1.2.2 Physical Layer Protocols

Physical layer protocols define the mechanical and electrical characteristics of a data link between computer systems. This can include specifications for:

- Media type
- Connector mechanical design
- Connector pin out
- Electrical signals used to represent logical one and zero
- Control signals

Physical layer protocols include:

- RS-232, RS-422 and RS-449 defined by the EIA (Electronics Industry Association)
- V.24, V.35, V.36 and X.21 defined by the CCITT (Comité Consultatif International Télégraphique et Téléphonique)
- The physical layer components of the 802.x family of standards defined by the IEEE (Institution of Electrical and Electronics Engineers)

Most physical layer protocols can be used with several protocol suites. For example the physical layer parts of the IEEE 802.x standards are supported by the SNA, TCP/IP, OSI and several other protocol suites.

Some physical layer protocols can support several protocol suites simultaneously. However, this is dependent on the data link layer protocol being used.

Similarly, most protocol suites support several physical layer protocols. For example the SNA protocol suite supports the CCITT V.24, V.35 and X.21 physical layer protocols for use with SDLC data links.

1.2.3 Data Link Layer Protocols

Data link layer protocols define procedures for the exchange of information across a data link or data link network. This can include procedures for:

- Connection establishment
- Connection termination
- Handshaking during information exchange
- Detection of errors

Data link and data link network protocols include:

- SDLC (Synchronous Data Link Control) defined by IBM
- PPP (Point-to-Point Protocol) defined by the IETF (Internet Engineering Task Force) in RFC 1171 and RFC 1172.
- X.25 defined by the CCITT[1]
- *Frame Relay* as defined by CCITT in Q.922/Q.923 and ANSI (American National Standards Institute) in T1.617/T1.618
- The MAC (Media Access Control) and LLC (Logical Link Control) components of the 802.x family of standards defined by the IEEE
- Ethernet defined by DIX (Digital** Intel** Xerox**)

Some data link and data link network protocols can be used by several protocol suites. For example the IEEE 802.x family of data link network protocols is supported by the SNA, TCP/IP and several other protocol suites.

Some data link and data link network protocols can support several protocol suites simultaneously. For example the IEEE 802.x family of standards can

---

1 In some protocol suites, CCITT X.25 is considered to be a network layer protocol (specifically the OSI protocol suite). However, most of the protocol suites discussed here use another network layer protocol on top of CCITT X.25 which is why is has been classified here as a data link layer protocol rather than a network layer protocol.

support several protocol suites simultaneously through the use of a mechanism called SAPs (Service Access Points).

Most protocol suites support several data link and data link network protocols. For example the SNA protocol suite supports SDLC and CCITT X.25 as well as many other data link and data link network protocols.

1.2.4 Network Layer Protocols

Network layer protocols are used to determine the path or *route* that should be taken for information to reach its destination node. *Routing tables* are used by network layer protocols to determine what data link or data link network should be used, and to what intermediate node information should be forwarded, to ultimately reach the correct destination node.

The routing tables used by network layer protocols can be either static (that is, fixed) or dynamic (that is, able to change as network conditions change). If the routing tables are dynamic, some form of routing table maintenance protocol is used to update the routing tables as network conditions change. Such protocols are described in 1.2.5.1, "Routing Table Maintenance Protocols" on page 8.

Network layer protocols include:

- IP (Internet Protocol) which is part of the TCP/IP protocol suite
- IPX** (Internet Packet Exchange**) protocol which is part of the NetWare protocol suite
- IDP (Internetwork Datagram Protocol) which is part of the XNS protocol suite
- DDP (Datagram Delivery Protocol) which is part of the AppleTalk protocol suite
- CLNP (Connection-less Network Protocol) which is part of the OSI protocol suite

The SNA and DECnet protocol suites do have equivalent network layer protocols, but they have no specific name.

1.2.5 Higher Layer Protocols

In general, higher layer protocols (that is, above the network layer) need only be implemented on the source computer system and destination computer system (that is, end nodes). Intermediate nodes (such as the 6611 Network Processor) do not need to interpret higher level protocols as they are transported transparently within the network and data link layer protocols implemented by the 6611 Network Processor.

However there are several higher layer protocols which are necessary for the 6611 Network Processor to:

- Maintain routing tables used by network layer protocols
- Provide systems management functions
- Support the 6611 Network Processor *Data Link Switching* function

These higher layer protocols are described in the following sections.

1.2.5.1 Routing Table Maintenance Protocols

The routing tables used by network layer protocols are maintained by various higher layer protocols. Each of these protocols is specific to a particular protocol suite, and some protocol suites incorporate several alternatives.

Some protocol suites support the partitioning of large networks into smaller networks which can be managed autonomously. These smaller networks are known by various names (depending on the protocol suite) such as *areas* (used in DECnet), *zones* (used in AppleTalk), or *autonomous systems* (used in TCP/IP). Some protocol suites use different routing table maintenance protocols:

- Within each of these smaller networks
- Between each of these smaller networks

For example the TCP/IP protocol suite uses different protocols within and between autonomous systems. These are called interior and exterior protocols respectively.

The routing table maintenance protocols for each protocol suite include:

- TCP/IP Interior Protocols
  - RIP (Routing Information Protocol)
  - Hello
  - OSPF (Open Shortest Path First)
- TCP/IP Exterior Protocols
  - EGP (Exterior Gateway Protocol)
  - BGP (Border Gateway Protocol)
- NetWare
  - RIP (Routing Information Protocol)
- XNS
  - RIP (Routing Information Protocol)
- AppleTalk
  - RTMP (Routing Table Maintenance Protocol)
- OSI
  - IS-IS (Intermediate System-Intermediate System)

Note: The TCP/IP, Netware and XNS protocol suites all use *different* forms of RIP. That is, TCP/IP RIP, Netware RIP and XNS RIP are three different protocols that happen to have the same name.

The DECnet protocol suite does have an equivalent routing table maintenance protocol; however, it does not have a particular name.

1.2.5.2 System Management Protocols

The 6611 Network Processor uses several higher layer protocols for system management purposes. These are all drawn from the TCP/IP protocol suite and include:

- FTP (File Transfer Protocol) which is used for the distribution of configuration and software changes to 6611 Network Processors across a TCP/IP network.

- RSH (Remote Shell) and REXEC (Remote Execution) which are used to remotely execute commands on a 6611 Network Processor across a TCP/IP network.
- TELNET and RLOGIN (Remote Login) which are used to remotely access the 6611 Network Processor System Manager function across a TCP/IP network.
- ICMP (Internet Control Message Protocol) which is used for various TCP/IP network management purposes such as reporting IP routing errors. ICMP can be used by the PING (Packet InterNet Groper) program to determine if a 6611 Network Processor is reachable across a TCP/IP network.
- SNMP (Simple Network Management Protocol) which is used to manage a network of 6611 Network Processors and other TCP/IP devices across a TCP/IP network from a suitable network management system such as IBM AIX* NetView/6000* for the IBM RISC System/6000*.

1.2.5.3 Data Link Switching Support

The *Data Link Switching* function provided by the 6611 Network Processor makes use of a transport layer protocol to provide connections between 6611 Network Processors. The protocol used is TCP (Transmission Control Protocol) which is drawn from the TCP/IP protocol suite. The implementation of the Data Link Switching function is described further in 2.2.3, "Data Link Switching" on page 40.

1.2.6 Addressing

Both data link layer and network layer protocols make use of addresses to transfer information to the correct destination.

Data link layer addresses are used to select which of the nodes connected to the **same** data link or data link network is the destination for an information transfer that makes use of that data link or data link network.

Network layer addresses are used to specify which node is the ultimate destination for an information transfer, no matter how many data links or data link networks are traversed to perform that transfer.

Data link layer and network layer addresses are described further in the following sections.

1.2.6.1 Data Link Layer Addresses

Each type of data link or data link network uses its own form of data link addresses to distinguish between the various nodes that are attached to a common data link or data link network.

The data link layer addresses used by various data link and data link network protocols are:

SDLC Uses polling addresses which are 1 byte long

IEEE 802.x Uses MAC addresses which are 6 bytes long

CCITT X.25 Uses DTE (Data Terminal Equipment) addresses which are 14 decimal digits long

Frame Relay Uses DLCI (Data Link Connection Identifier) addresses which are 10 bits long

Some protocol suites provide protocols to determine the data link layer address that can be used to reach a particular network layer address. For example the TCP/IP protocol suite uses ARP (Address Resolution Protocol) to derive the data link layer address from a network layer address.

1.2.6.2 Network Layer Addresses

Each protocol suite uses its own form of network layer addresses which are used to distinguish between the various nodes throughout a network. The network layer addresses used by various protocol suites are:

TCP/IP Uses IP addresses which are 4 bytes long, comprising a network part of 7, 14 or 21 bits and a host part of 24, 16 or 8 bits respectively.

OSI Uses NSAP addresses which have three parts:

- AFI (Authority and Format Identifier)
- IDI (Initial Domain Identifier)
- DSP (Domain Specific Part)

XNS Uses a two-part address consisting of a 4-byte network number and a 6 byte host number

NetWare Uses a two-part address consisting of a 4-byte network number and a 6 byte host number

AppleTalk Uses a two-part address consisting of a 2-byte network number and a 1 byte node number

DECnet Uses a two-part address consisting of a 6-bit area number and a 10-bit node number

NetBIOS Uses a 16-character name

Some protocol suites can use multiple network layer addresses in a single node. For example the TCP/IP protocol suite uses a different network layer address for each data link or data link network interface.

Some protocol suites use the data link layer address as part of the network layer address. For example the XNS protocol suite uses the data link layer address for the host number part of the network layer address.

Some protocol suites provide a pseudonym capability for network layer addresses which allow an easily understood plain text name to be used in place of a network layer address. Such names can be translated into network layer addresses using protocols designed for that purpose.

For example the AppleTalk protocol suite uses NBP (Name Binding Protocol) to translate names into network layer addresses. Similarly the TCP/IP protocol suite uses *Domain Name Servers* to translate names into network layer addresses.

1.3 Internetworking and Bridging

Internetworking is concerned with the connection of heterogeneous networks. Its primary goal is to hide the details of the underlying network hardware while providing universal communication. Two different approaches to hiding network details exist: application-level and network-level.

Gateways Gateways use application-level programs, executing on each machine in the network that understand the details of the network connection. This system requires each machine to have a different application program for each application running on each machine.

Routers Routers use network-level interconnection and provide a mechanism that delivers packets from their original source to their ultimate destination in real time. Within each network, computers use their own communication protocol. Software, inserted between the technology-dependent communications mechanism and application programs, will hide the low-level details and make the collection of networks appear to be a single large network.

Bridges are used to extend the physical network beyond the repeater function. In a LAN environment a repeater extends the ring length and bridges connect separate ring segments locally or across public or private networks, for example, using high speed ISDN or PSTN (E1 and T1) lines.

Note: The TCP/IP world uses a different definition of a gateway. Networking in the TCP/IP world consists of connecting different networks so that they form one logical interconnected network. This large overall network is called an *internetwork* or, more commonly an *internet*. Each network uses its own physical layer, and the different networks are connected to each other via machines which are called *internet gateways* or simply *gateways*. The function provided by these gateways is to transfer IP datagrams between the two networks. This function is called *routing* and from this the internet gateways are often called *routers*. Recent TCP/IP reference publications have started using the term routers rather than gateway, for example in the OSPF specification.

1.3.1 Internetworking and the OSI Reference Model

The industry and the standards bodies have chosen to give distinct names (*bridges, routers and gateways*), to subnetwork connectors, depending on the layers at which they are used.

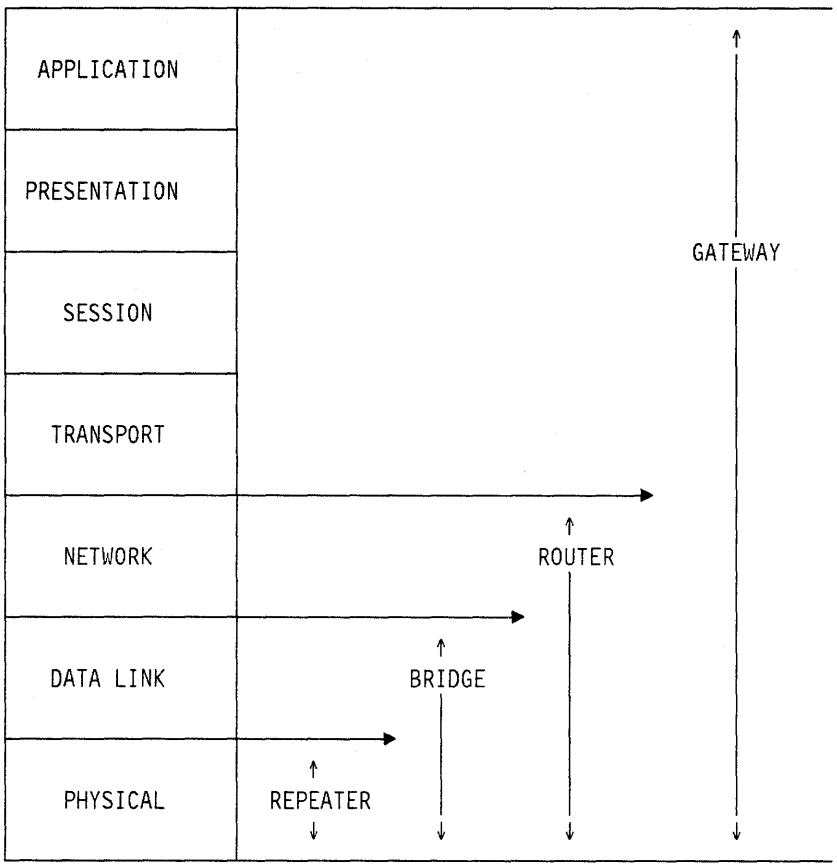


Figure 4. OSI Model

1. **Gateways** operate above layer 3 and support protocol conversion between unlike protocol stacks. Communication between OSI and SNA or OSI and TCP/IP is handled by a *gateway*.
2. **Routers** work up to layer 3. Layer 3 routers can interconnect and route across many physical subnetworks, including LANs and WANs.
3. **Bridges** operate at the second, data link control (DLC) layer. As an extension bridges are also defined to interconnect heterogeneous LANs, for example Token-Ring and Ethernet.
4. **Repeaters** operate at the physical layer, simply extending the physical character of the subnetwork. Repeaters can sometimes also provide media conversion between optical fiber and copper.

Note: **Brouters** have the *bridge* and *router* function in one machine. They transport connection-oriented protocols such as SNA and NetBIOS by bridging these protocols. They may encapsulate the bridged protocol in TCP/IP for transport across the WAN, but to the end station they appear like a bridge. Hence, they do not provide local acknowledgement for LAN-attached SNA or NetBIOS.

1.3.2 Bridges

Bridges operate at the Media Access Control (MAC) layer, which is the lower sublayer of DLC. The MAC sublayer has a DA or *Destination Address* an SA or *Source Address*, and in the case of Token-Ring or 802.5 a RIF or *Routing Information Field*. Two types of *MAC Layer Bridges* exist:

Source Routing Bridges
These bridges forward frames based on the RIF in the MAC.

Transparent Bridges
These bridges forward frames based on the destination address. If the destination address is known on the segment, then no forwarding will take place. If the destination address is unknown on the segment then forwarding will take place through the bridge.

The MAC addresses represent a "physical" connection to a LAN. Every workstation on a given LAN (Token-Ring, Ethernet, etc.) must have a MAC address. Bridges are sometimes called "protocol independent" because the forwarding destination is determined by the MAC address.

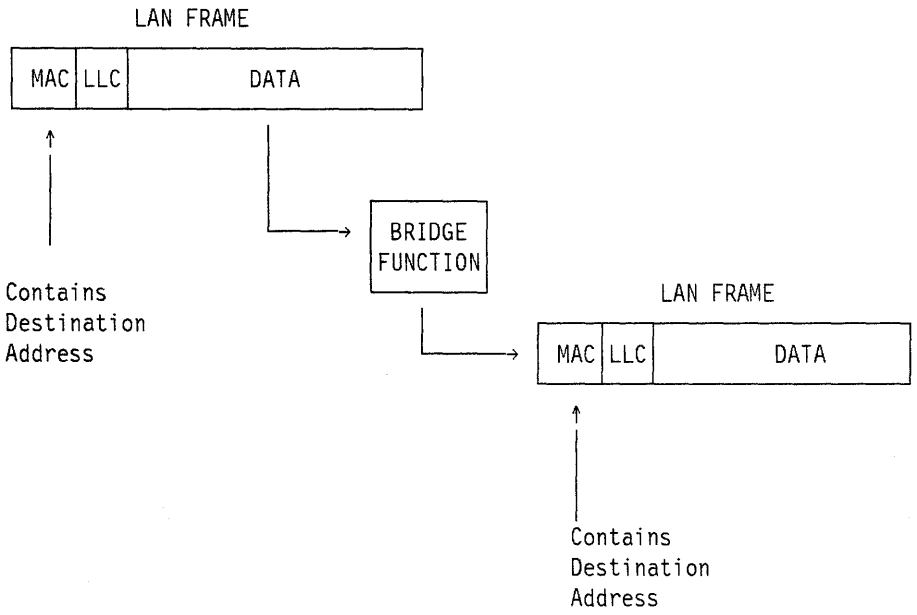


Figure 5. Bridge Operation

Bridges are essentially invisible to an end station. Based on the routing algorithm, *Bridges* decide to forward the frame across or not. Because the bridge is "invisible," there are some bridge characteristics to take into account:

- Do not inadvertently duplicate any MAC addresses in a LAN.
- Bridges forward all layer 2 broadcasts, with a potential danger of broadcast storms with certain protocols, for example, AppleTalk and TCP/IP's ARP.
- Protocols that are connection-oriented at layer 2 must receive end-to-end acknowledgements within some window.

1.3.2.1 Transparent Bridging

Transparent bridging is used to connect Ethernet LANs but can also be used to connect Token-Ring LANs. The bridge builds tables for each half with all the known stations. All frames are copied and forwarded if not in the "known" table.

- The bridge listens to all packets on each connected LAN and builds the forwarding tables by looking at the SOURCE address. The bridge has two of these tables, one for each ring it connects to. See Figure 6 on page 15. One bridge half will only see the SOURCE addresses PC1, PC2 and PC3; the other side will see frames with SOURCE addresses PCA, PCB and PCC.
- Forwarding decisions are based on the DESTINATION address. If it matches an address in the SOURCE table the frame will not be forwarded. If it does not match then the frame will be forwarded not only across the bridge but also on the local segment because the bridge does not really know where the destination is.
- Transparent bridging requires that there be only one path between any two stations in the network configuration. Otherwise, the frames can loop and stay in the network forever. So in fact active **parallel paths** are not supported.
- Each bridge initially enters the network and periodically transmits a *Hello* message carrying an ID, timer values, path cost parameters and flags associated with the spanning tree algorithm. The *Hello* message is received by other bridges attached to that segment, and a *root* bridge on the originating LAN is selected for a *least-cost* path. A *Hello* message is then transmitted on the adjoining LAN segment, with the ID of the root, and the process is repeated. In this way, the identity of the root bridge is propagated across the network, along least-cost paths. The loser bridges enter the blocking state, and the winners enter the learning state.
- When a bridge goes down the SOURCE table is lost and the learning process has to start all over. In fact, all bridges in the network must go through the "Hello" message routine. This could take considerable time and is considered a major drawback in the transparent bridging parallel path network.

The IBM 6611 Network Processor does not support transparent bridging in Release 1.

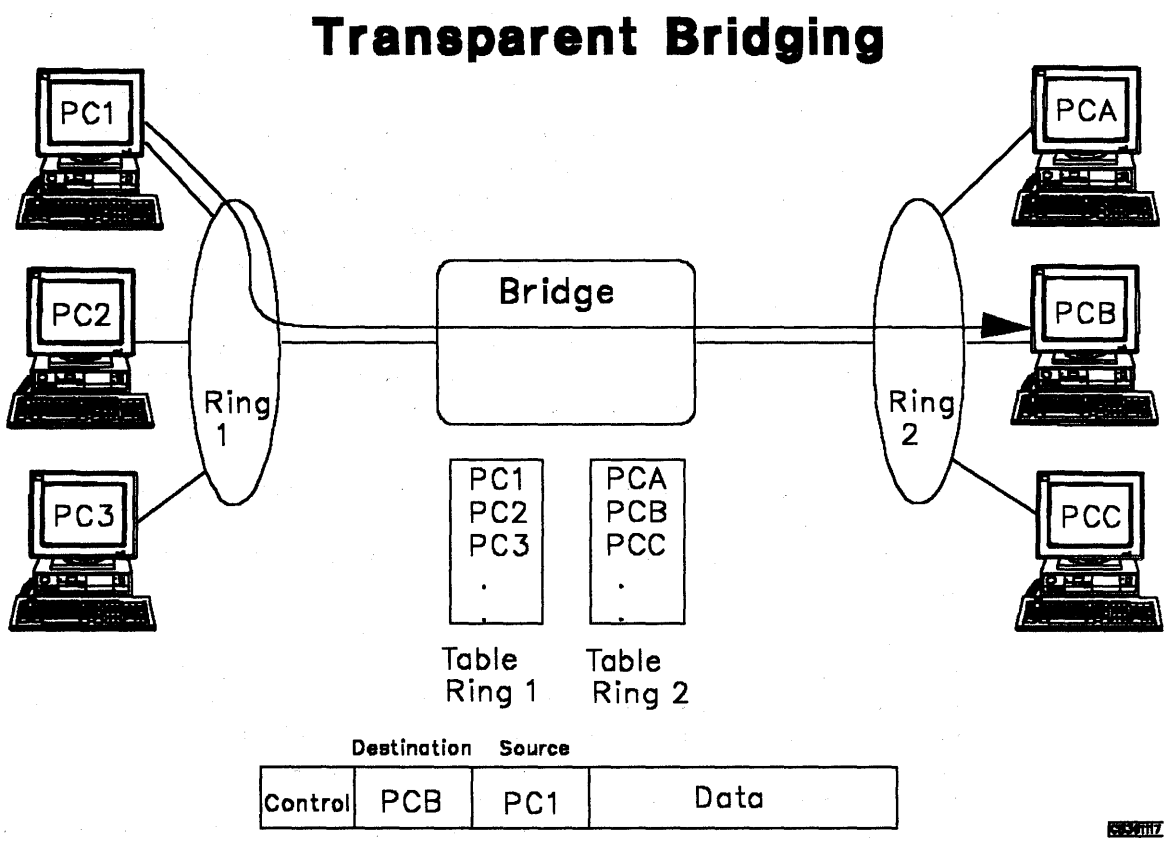


Figure 6. Transparent Bridge Operation

1.3.2.2 Source Route Bridging

Source route bridging is the scheme used by IBM bridges. Frames are forwarded based on the *Routing Information Field* (RIF), which contains a sequence of bridge numbers and segment numbers. If the bridge detects a match between its own bridge number and segment number it will forward the frame, based upon the broadcast indicator. See Figure 7 on page 16.

A path search is required to build the RIF. Different schemes exist:

- **All-routes** broadcast used typically by SNA devices. First it is determined whether the destination is on the local segment by sending a TEST or XID LLC protocol data unit (LPDU) on the local LAN segment. The sending station then waits for a period of time, dependent on the application, and if it does not receive a response it will then resend the TEST or XID LLC with an **All-routes** broadcast set. This All-routes broadcast will go over all bridges and each time the RIF field will be updated. Eventually the destination will be found at which time a return TEST frame will be sent out. This may result in multiple copies of frames arriving at the end station and being returned. The first frame that returns to the originator will be chosen since it has the fastest path and RIF to the end station. All other returning frames will be discarded.
- **Single-route** broadcast used typically by NetBIOS. The primary aim of using single-route broadcast is to minimize the amount of traffic and hence the processing on the target machines. Single-route broadcast frames will only go through bridges that have the single-route parameter set. This can either

be done manually or automatically in which case the spanning tree algorithm is built automatically. The idea of *single-route* broadcast is to present only one frame to the target.

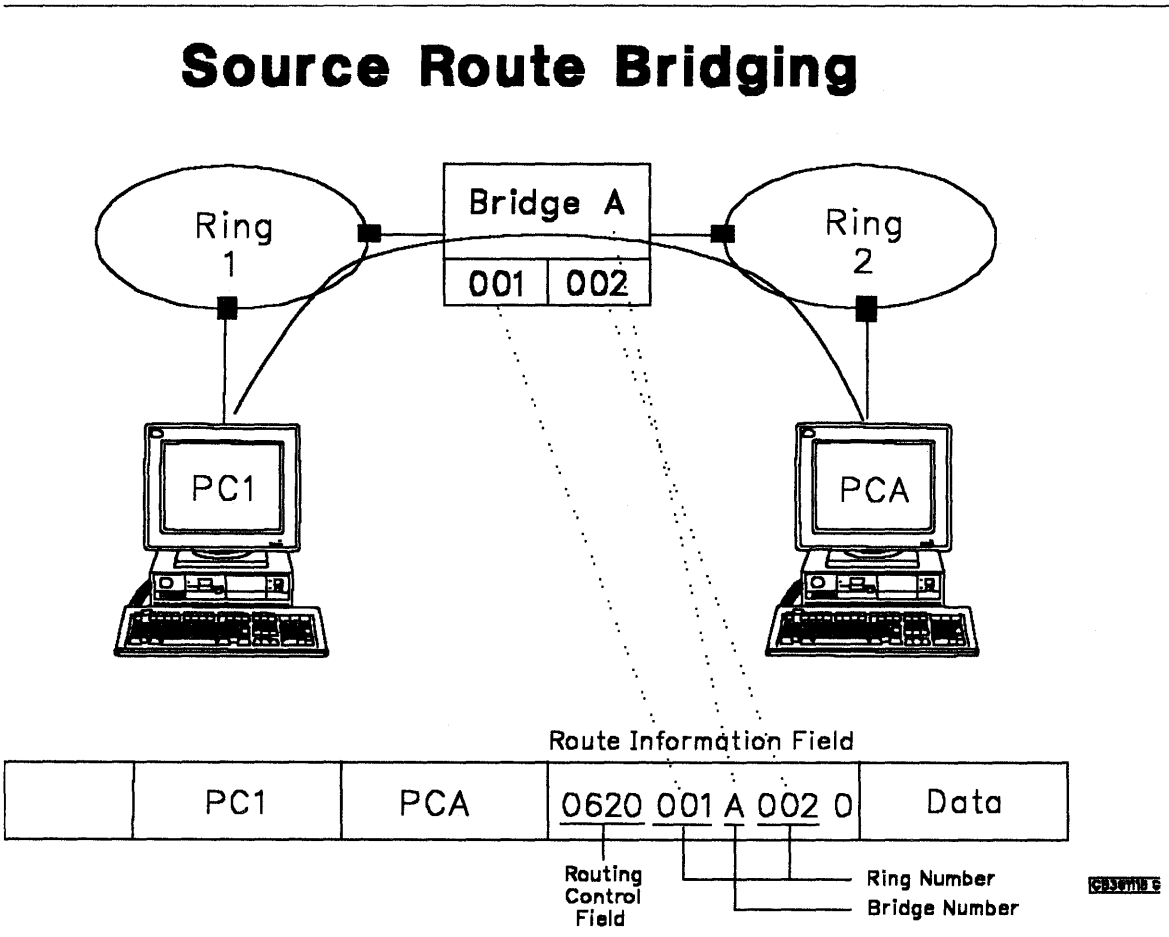


Figure 7. Source Route Bridging Operation

1.3.2.3 Source Route Transparent Bridging

The IEEE 802.1 committee on internetworking has a requirement that source-routing bridges must be capable of inter operating with transparent bridges on the same network. The proposed standard is SRT or *Source Routing Transparent* bridging.

A bridge with the SRT function will look for the RIF field and if present will use the source routing logic; if not it will use the transparent bridging logic.

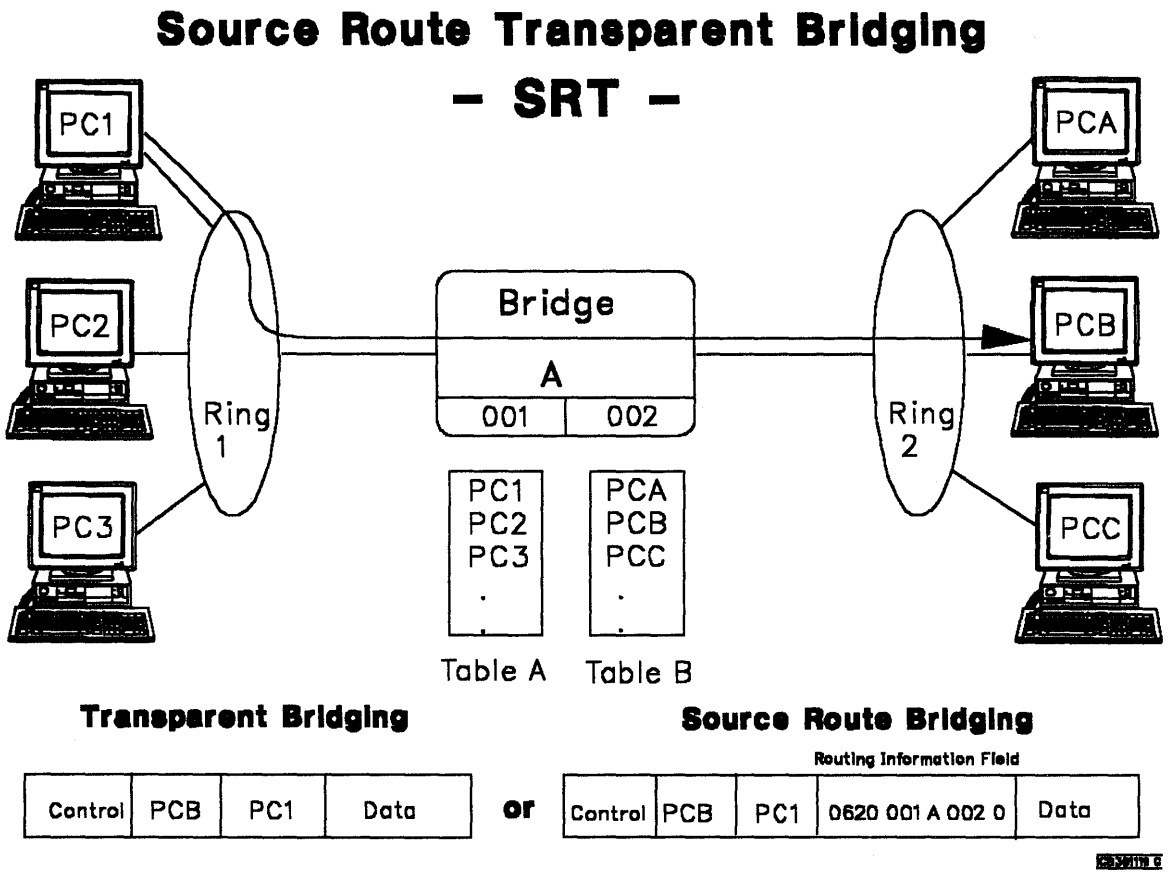


Figure 8. Source Route Transparent Bridging

The 6611 Network Processor does not support SRT.

1.3.2.4 Bridge Weaknesses

Bridges have many weaknesses:

- Availability

  Broadcast storms

  Broadcast storms can occur when running protocols such as AppleTalk and TCP/IP, which can generate a large number of broadcasts. Bridges can set up filters to limit this.

  Timeouts

  Timeouts can occur if LLC acknowledgements do not occur within the timer windows (typically around 1 second). This is most prevalent when bridging over wide area links, due to their lower speeds and/or excessive line utilization. Excessive line utilization may be a result of broadcasts or large file transfers.

- Performance

  No class of service

  This may mean that interactive SNA traffic gets delayed behind large NetBIOS or TCP/IP file transfer.

No flow control
Between the bridge and the end stations.

Bridges must either forward all data they get or discard it. They cannot tell end stations to send data more slowly. Congestion in bridges could result in dropped connections.

When running Type 2 (connection-oriented) Logical Link Control, when an end station detects that frames are being discarded, it reduces its window size. Hence, by dropping data, a bridge is in a sense signalling congestion to an end station.

Unnecessary WAN traffic
Such as keep alive messages and broadcasts, not only waste bandwidth but may result in excessive line utilization which in turn causes timeouts.

- Administration

Hop count limitations of 7
May not be sufficient for some environments (applicable to source routing bridges only).

MAC addresses
Should not inadvertently be duplicated when bridging (only a problem when using locally administered MAC addresses).

An in-depth description of the different bridging schemes can be found in the *IBM Multisegment LAN Design Guidelines* GG24-3398-01.

1.3.3 Routers

Routers make their forwarding decisions based on the layer 3 network address.

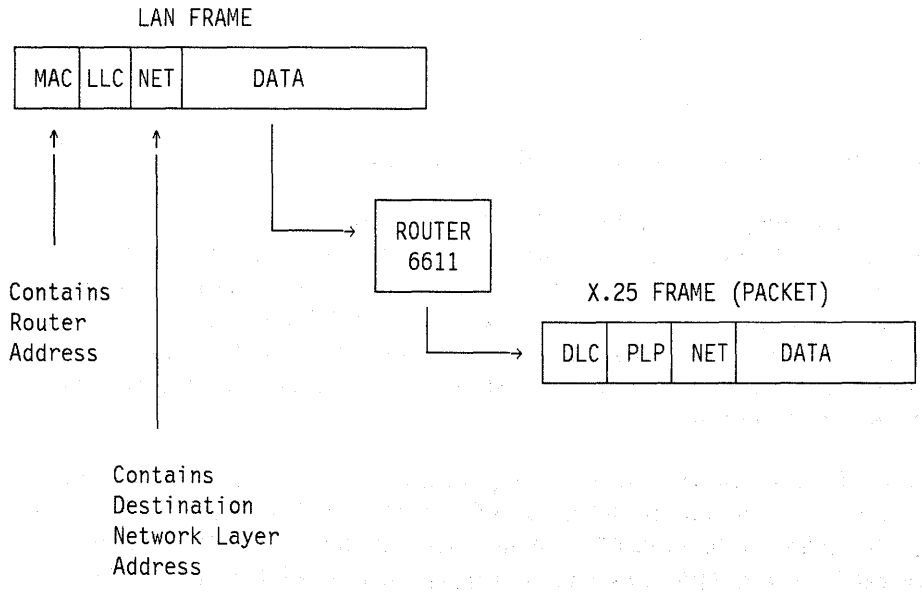


Figure 9. Router Operation

As can be seen in Figure 10 on page 19 each protocol that runs over a LAN has a unique network layer. Each has its own addressing structure and each uses a

unique routing algorithm. Therefore *routers* are protocol dependent and must understand the layer 3 addressing and routing of any protocol they are to forward.

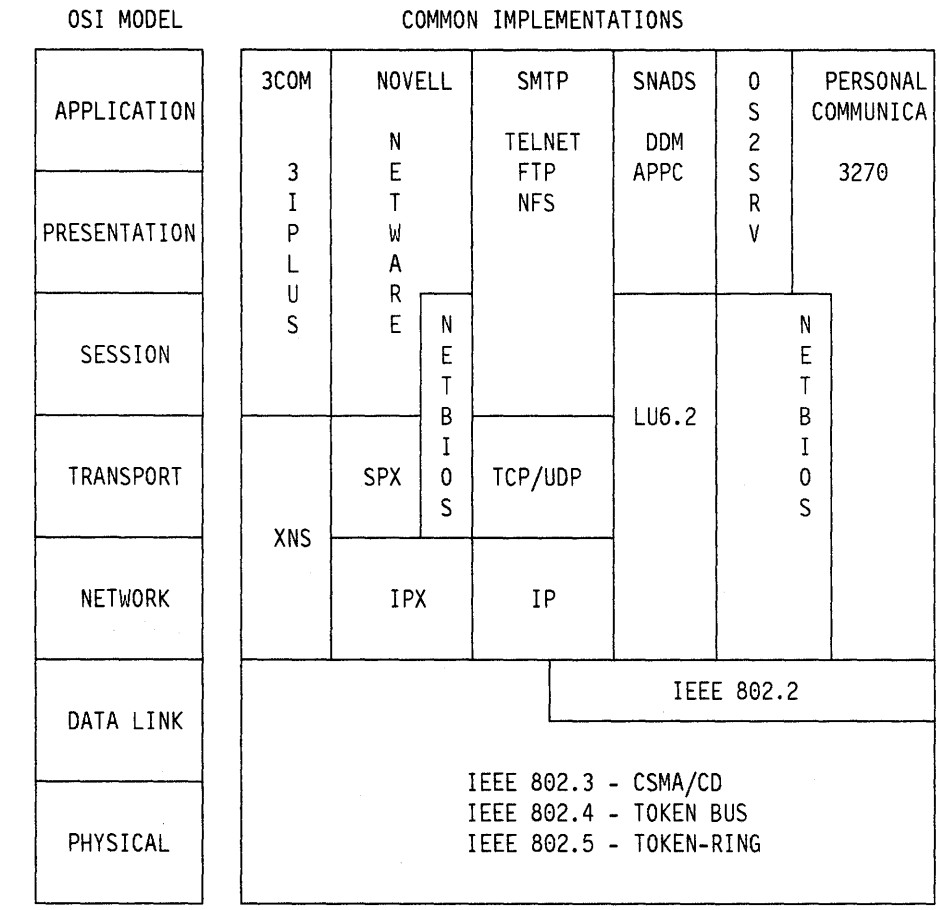


Figure 10. Protocol Layers and Common Implementations

Routers only look at frames addressed directly to them.

They look inside the frame at the **Network Layer Address** and use it to make their forwarding decision. Since *routers* do not use MAC addresses to make their forwarding decisions, duplicate MAC addresses are possible on either side of a router. Routers maintain a unique routing table for each routing protocol they support. Each table is maintained via broadcasts of table updates. Most routable protocols are connection-less at layer 2, so no acknowledgements or keep-alives are required.

Connection-less protocols (those not requiring an acknowledgement by the receiving station), such as IP, Novell's IPX, Xerox's XNS and Apple's AppleTalk, carry all the information needed to make a routing decision to their network layer (level 3). Connection-oriented protocols, such as SNA and NetBIOS, require more end-to-end information than is available at level 3 for their routing decisions.

Most of the protocols supported by today's routers have a connection-less layer 3 with a hierarchical network addressing structure. To handle these protocols, a router need only understand the address and have a table that indicates where

to forward data destined for that address. Most of today's *routers* do not route protocols that are connection-oriented at layer 3. In particular they do not support subarea SNA or APPN. To coexist in current router networks, SNA and NetBIOS must be provided the dynamic characteristics of intermediate node routing while maintaining the system's end-to-end predictability and control. For example, as part of the bind process with subarea SNA, we determine the class of service and hence the virtual route to be used for a session. All session traffic flows over the same virtual route. In APPN, as part of the bind process, each network node builds session connectors. When subsequent session traffic passes through the network node, the network node need only look at the session ID to know how to forward data. For a router to participate in the session setup it would have to be a full PU T4 or an APPN network node (NN). This is far more complicated than simply doing a table look-up when a packet arrives. Hence, in today's routers, SNA is typically bridged and/or encapsulated in TCP/IP.

1.3.4 DLS

Data Link Switching (DLS) is IBM's transport technique for SNA and NetBIOS in the *6611 Network Processor*. The objective of DLS is to integrate the transport of SNA and NetBIOS into multiprotocol router networks, transparent to existing SNA and NetBIOS end user applications. DLS provides SNA and NetBIOS the necessary system-wide control while adding dynamic re-routing and Local Area Network isolation. DLS 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 acknowledgements on the local LAN segments
- Broadcast traffic control through the WAN, because the LLC type 2 connections are terminated at the router
- LAN and WAN control for congestion and data flow.

Although a number of router vendors have implemented alternative techniques to transport SNA and NetBIOS through a multiprotocol internetwork, the effectiveness of each is dependent on the varying degrees of the above functions being provided.

Like bridging, DLS uses the information in the data link header (data link layer address). The DLS function examines the destination MAC address and the destination service access point (DSAP) in the header. Using a routing table that translates MAC addresses to IP addresses the DLS function will encapsulate the SNA or NetBIOS frames into IP packets. These will be sent across the WAN using the Transmission Control Protocol (TCP) of the router.

Chapter 2. Overview of 6611 Hardware and Functions

This chapter provides a summary of the hardware and functions of the IBM 6611 Network Processor when used with the IBM Multiprotocol Network Program (5648-016).

Further information on the 6611 Network Processor hardware can be found in the *IBM 6611 Network Processor: Installation and Service Guide*.

Further information on the functions provided by the 6611 Network Processor when used with the Multiprotocol Network Program can be found in the *IBM 6611 Network Processor: Introduction and Planning Guide*.

2.1 Hardware Overview

The IBM 6611 Network Processor hardware comprises two models, and six different types of communication adapter features that can be used with either model.

The two models of the 6611 Network Processor are:

- The 6611 Network Processor Model 140, a table, shelf, or floor mounting model that can support the installation of up to four communication adapter features.
- The 6611 Network Processor Model 170, a floor mounting model that can support the installation of up to seven communication adapter features.

With the exception of the number of communication adapter features supported, both models of the 6611 Network Processor provide identical function when used with the co-requisite IBM Multiprotocol Network Program (5648-016). There is no upgrade available between the two models of the 6611 Network Processor.

Both models of the 6611 Network Processor comprise a system processor, 16MB of main storage, and an I/O subsystem to support the attachment of various I/O devices. This is illustrated in Figure 11 on page 22.

The system processor uses the IBM POWER Architecture* (Performance Optimization With Enhanced RISC) which was first used by the IBM RISC System/6000. The I/O subsystem incorporates the IBM Micro Channel* architecture which was first used by the IBM Personal System/2* and then later enhanced for use by the IBM RISC System/6000.

The I/O subsystem supports the following I/O devices:

- Up to four (Model 140) or seven (Model 170) communication adapter features
- One 355MB (Model 170) or two 160MB (Model 140) fixed disk drives
- Diskette drive
- Two serial ports
- 3-digit status display

The functions provided by each of these I/O devices are:

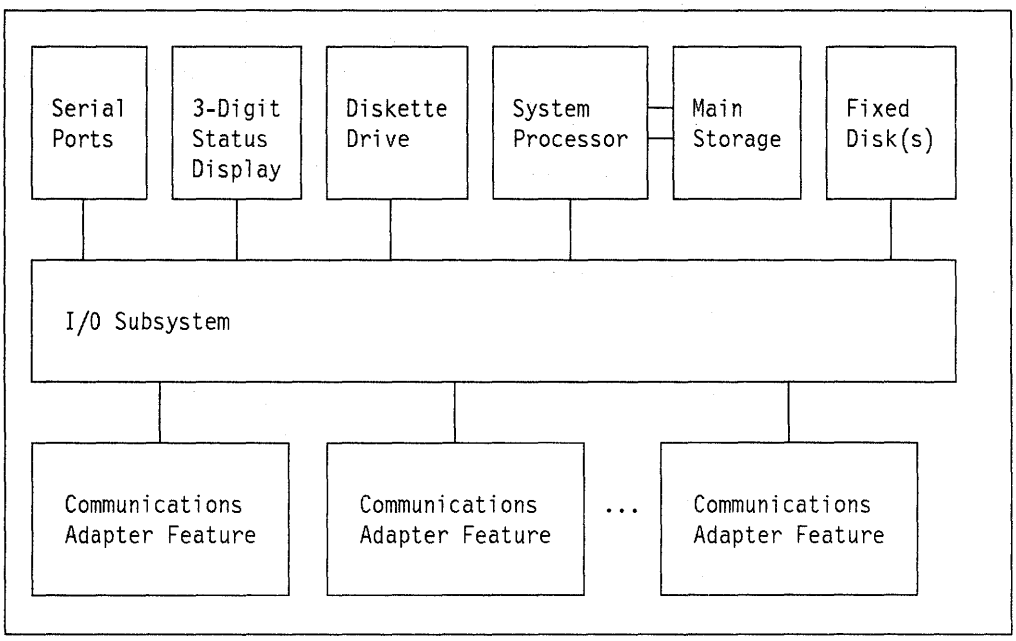


Figure 11. 6611 Hardware Components

Communication Adapter Features

The communication adapter features provide communication interfaces for various common carrier services and various LAN implementations. These features are described further in 2.1.1, "Communication Adapter Features" on page 23.

Fixed Disk Drive(s)

The fixed disk drive(s) are used for storage of the Multiprotocol Network Program, configurations and diagnostics. The Multiprotocol Network Program and diagnostics are pre-installed on the fixed disk drive(s) prior to shipment of the 6611 Network Processor from IBM to the customer. The configurations are loaded onto the fixed disk(s) by the customer either from diskette, via a TCP/IP network or via the System Manager component of the Multiprotocol Network Program. The 6611 Network Processor configuration process is described further in Chapter 3, "Configuring the 6611" on page 55.

Diskette Drive

The diskette drive is used for loading the initial configuration of the 6611 Network Processor and for diagnostic purposes.

Serial Ports

The two serial ports are used for the attachment of ASCII terminals such as the IBM 3151, 3161 or 3164 to the 6611 Network Processor. A terminal (or terminal emulator running on a computer) can either be locally attached (at 9600 bps) or remotely attached (at 2400 bps) via suitable modems, to each of the two serial ports. Terminals attached to the serial ports are used by IBM CEs (Customer Engineers) for diagnostic purposes and by the customer for accessing the System Manager component of the Multiprotocol Network Program. The System Manager is described further in Chapter 4, "Managing the 6611" on page 91.

3-Digit Status Display

The 3-digit display is used for the display of status and diagnostic codes. The meaning of these codes can be found in an appendix for the *IBM Multiprotocol Network Program: User's Guide*.

The communication adapter features supported by the 6611 Network Processor are described in more detail in the following sections.

2.1.1 Communication Adapter Features

The six different types of communication adapter features available for the 6611 Network Processor are:

- 6611 2-Port Serial Adapter, feature #2640
- 6611 2-Port V.35/V.36 Compatible Serial Adapter, feature #2650
- 6611 Token-Ring Network 16/4 Adapter, feature #2660
- 6611 Ethernet Adapter, feature #2680
- 6611 4-Port SDLC Adapter, feature #2720
- 6611 X.25 Adapter, feature #2730

The first four communication adapter features listed (#2640, #2650, #2660, #2680) share a similar design which incorporates a RISC processor with memory on each adapter. These adapters are able to perform adapter-to-adapter transfers without direct intervention of the system processor through the exploitation of the IBM Micro Channel architecture. Additionally, these adapters are able to process network layer and data link layer protocols within the adapter using the RISC processor and memory contained on each adapter.

The combination of these two features (adapter-to-adapter transfers, and protocol processing within the adapter) enable high levels of performance to be achieved. This is because the processing of routing and bridging functions is distributed between, potentially, many RISC processors.

The remaining two communication adapter features (#2720, #2730) are *shallow* adapters which require interaction with the system processor for most functions. This is consistent with the relatively low speed (up to 64 Kbps) communication interfaces provided by these adapters.

Multiple instances of each type of communication adapter feature can be used up to the maximums listed in Table 1. However, the total number of communication adapter features (all types) cannot exceed four for the 6611 Network Processor Model 140 or seven for the 6611 Network Processor Model 170.

Table 1 (Page 1 of 2). Maximum Communication Adapters and Interfaces by Type

Adapter Type	**6611-140**		**6611-170**	
	Adapters	**Interfaces**	**Adapters**	**Interfaces**
6611 2-Port Serial Adapter	4	8	7	14
6611 2-Port V.35/V.36 Compatible Serial Adapter	4	8	7	14
6611 Token-Ring Network 16/4 Adapter	4	4	7	7

Table 1 (Page 2 of 2). Maximum Communication Adapters and Interfaces by Type				
Adapter Type	**6611-140**		**6611-170**	
	Adapters	**Interfaces**	**Adapters**	**Interfaces**
6611 Ethernet Adapter	4	4	7	7
6611 X.25 Adapter	4	4	4	4
6611 4-Port SDLC Adapter	3	12	6	24

Each of the 6611 Network Processor communication adapter features are described in more detail in the following sections.

2.1.1.1 6611 2-Port Serial Adapter (#2640)

The 6611 2-Port Serial Adapter provides two independent synchronous serial communication interfaces. These interfaces are supported at speeds between 19.2 Kbps and 2.048 Mbps, with a maximum aggregate speed of 3.072 Mbps across both interfaces. Each interface can attach to DCEs that provide either an EIA RS-422/RS-449 or a CCITT X.21 physical interface with a continuous clock. Except for the types of DCE physical interfaces supported, the 6611 2-Port Serial Adapter is identical in function to the 6611 2-Port V.35/V.36 Compatible Serial Adapter.

Note: The RS-422/RS-449 interface provided by the 6611 2-Port Serial Adapter does not provide the "Request To Send" signal, nor does it monitor the "Clear To Send" signal. This may cause problems when using DCEs that require a valid "Request To Send" signal. These problems can usually be solved by providing a valid "Request To Send" signal via some other means.

In countries where T1 common carrier services are available, a DSU/CSU (Data Services Unit/Channel Services Unit) is normally used as the DCE. The DSU/CSU must generate the additional framing bits needed to utilize the 1.544 Mbps interface used with T1 services, while providing a continuous clock to the 6611 Network Processor at 1.536 Mbps. Both interfaces of the 6611 2-Port Serial Adapter can be used concurrently at such speeds as the aggregate speed across both interfaces does not exceed 3.072 Mbps (2 x 1.536 Mbps).

In some countries where E1 common carrier services are available, IBM has announced the IBM 6629 RS449/G.703 2.048 Mbps Interface Converter, which can be used as the DCE. It provides conversion between a CCITT G.703 clear channel interface used with the E1 service, and the EIA RS-422/RS-449 interface that can be used by the 6611 Network Processor. If one interface of the 6611 2-Port Serial Adapter is used at 2.048 Mbps, the other interface must be used at a lower speed so that that aggregate speed across both interfaces does not exceed 3.072 Mbps.

Each interface of the 6611 2-Port Serial Adapter can support one of three data link protocols:

- PPP (Point-to-Point Protocol)
- Frame Relay (Permanent virtual circuits only)
- The protocol implemented by the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) when used as one-half of a remote bridge.

Each 6611 2-Port Serial Adapter requires up to two DCE interface cables appropriate to the type of DCE interface in use. The available DCE interface cables are:

6611 Serial Adapter Cable, feature #2645 (EIA RS-422/RS-449 DCE Interface)
6611 SDLC Adapter CCITT X.21 Cable, feature #2729

2.1.1.2 6611 2-Port V.35/V.36 Compatible Serial Adapter (#2650)

The 6611 2-Port V.35/V.36 Compatible Serial Adapter provides two independent synchronous serial communication interfaces. These interfaces are supported at speeds between 19.2 Kbps and 2.048 Mbps, with a maximum aggregate speed of 3.072 Mbps across both interfaces. Each interface can attach to DCEs that provide either a CCITT V.35 or a CCITT V.36 physical interface with a continuous clock. Except for the types of DCE physical interfaces supported, the 6611 2-Port V.35/V.36 Compatible Serial Adapter is identical in function to the 6611 2-Port Serial Adapter.

Note: The 6611 2-Port V.35/V.36 Compatible Serial Adapter is only available in some countries. An IBM representative should be consulted to determine the availability of the 6611 2-Port V.35/V.36 Compatible Serial Adapter in a particular country.

Each interface of the 6611 2-Port V.35/V.36 Compatible Serial Adapter can support one of three data link protocols:

- PPP (Point-to-Point Protocol)
- Frame Relay (Permanent virtual circuits only)
- The protocol implemented by the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) when used as one half of a remote bridge

Each 6611 2-Port V.35/V.36 Compatible Serial Adapter requires up to two DCE interface cables appropriate to the type of DCE interface in use. The available DCE interface cables are:

6611 V.35 Compatible Serial Adapter Cable, feature #2655
6611 V.36 Compatible Serial Adapter Cable, feature #2657

2.1.1.3 6611 Token-Ring Network 16/4 Adapter (#2660)

The 6611 Token-Ring Network 16/4 Adapter provides a single interface to either a 4 Mbps or 16 Mbps IBM Token-Ring Network.

Each 6611 Token-Ring Network 16/4 Adapter requires one 6611 Token-Ring Network Adapter Cable, feature #2665.

2.1.1.4 6611 Ethernet Adapter (#2680)

The 6611 Ethernet Adapter provides a single interface to a 10 Mbps CSMA/CD (Carrier Sense Multiple Access/Collision Detection) local area network using either IEEE 802.3 or DIX Ethernet V2 frame formats.

Each 6611 Ethernet Adapter requires an AUI (Attachment Unit Interface) cable, and a transceiver suitable for the type of Ethernet cabling in use.

2.1.1.5 6611 4-Port SDLC Adapter (#2720)

The 6611 4-Port SDLC Adapter provides four independent synchronous serial communication interfaces that only support the use of SDLC data link protocols.

Each port of the 6611 4-Port SDLC Adapter provides different DCE physical interface attachment capabilities. These are:

Port 0 Supports EIA RS-232D/CCITT V.24, CCITT V.35 or CCITT X.21
Port 1 Supports EIA RS-232D/CCITT V.24 or CCITT V.35
Port 2 Supports EIA RS-232D/CCITT V.24
Port 3 Supports EIA RS-232D/CCITT V.24

DCEs providing a CCITT V.35 or CCITT X.21 physical interface are supported at speeds up to 64 Kbps. DCEs providing an EIA RS-232D/CCITT V.24 physical interface are supported at speeds up to 19.2 Kbps.

Each 6611 4-Port SDLC Adapter requires one 6611 SDLC Adapter Interface Cable, feature #2723, and up to four DCE interface cables appropriate to the DCE interfaces in use. The available DCE interface cables are:

6611 SDLC Adapter EIA RS-232D/CCITT V.24 Cable, feature #2725
6611 SDLC Adapter CCITT V.35 Cable, feature #2727
6611 SDLC Adapter CCITT X.21 Cable, feature #2729

2.1.1.6 6611 X.25 Adapter (#2730)

The 6611 X.25 Adapter provides a single serial communication interface that supports the use of CCITT X.25 protocols using either permanent or switched virtual circuits. The interface can attach to DCEs that provide either a EIA RS-232D/CCITT V.24, CCITT V.35 or CCITT X.21 physical interface.

DCEs providing a CCITT V.35 or CCITT X.21 physical interface are supported at speeds up to 64 Kbps. DCEs providing a EIA RS-232D/CCITT V.24 interface are supported at speeds up to 19.2 Kbps.

Each 6611 X.25 Adapter requires one DCE interface cable appropriate to the DCE interface in use, which can be any one of the following:

6611 X.25 Adapter EIA RS-232D/CCITT V.24 Cable - 3 Meter, feature #2977.
6611 X.25 Adapter EIA RS-232D/CCITT V.24 Cable - 6 Meter, feature #2978
6611 X.25 Adapter CCITT V.35 Cable - 3 Meter, feature #2987
6611 X.25 Adapter CCITT V.35 Cable - 6 Meter, feature #2988
6611 X.25 Adapter CCITT X.21 Cable - 3 Meter, feature #2975
6611 X.25 Adapter CCITT X.21 Cable - 6 Meter, feature #2976

2.2 Functional Overview

The IBM 6611 Network Processor when used with the IBM Multiprotocol Network Program (5648-016) provides three main functions:

- Multiprotocol Routing
- Source Route Bridging
- Data Link Switching

In addition to these main functions the 6611 Network Processor provides various functions to support the configuration and management of a network of 6611 Network Processors. The configuration functions provided by the 6611 Network

Processor will be described in Chapter 3, "Configuring the 6611" on page 55. The management functions provided by the 6611 Network Processor will be described in Chapter 4, "Managing the 6611" on page 91.

Each of the three main functions provided by the 6611 Network Processor can be used concurrently; however, certain considerations may apply to their concurrent use. These considerations are described further in 2.2.4, "Concurrent Use of Functions" on page 50.

2.2.1 Multiprotocol Routing

The 6611 Network Processor provides routing of the network layer protocols used by the following protocol suites:

- TCP/IP
- NetWare
- XNS
- DECnet Phase IV
- AppleTalk Phase 2

Note: Support for the AppleTalk protocol suite will not be included in the initial general availability of the 6611 Network Processor and Multiprotocol Network Program. Refer to the 6611 Network Processor and Multiprotocol Network Program announcement letters for the date when support for the AppleTalk protocol suite will become available.

2.2.1.1 Communication Adapter Features Supported

The communication adapter features supported for each of the protocols that can be routed by the 6611 Network Processor are summarized in Table 2.

Table 2. Communication Adapter Feature Routing Support

Adapter	TCP/IP	NetWare	XNS	DECnet	AppleTalk
6611 2-Port Serial Adapter	Yes	Yes	Yes	Yes	Yes
6611 2-Port V.35/V.36 Compatible Serial Adapter	Yes	Yes	Yes	Yes	Yes
6611 Ethernet Adapter	Yes	Yes	Yes	Yes	Yes
6611 Token-Ring Network 16/4 Adapter	Yes	Yes	Yes	Yes	Yes
6611 X.25 Adapter	Yes	No	No	No	No
6611 4-Port SDLC Adapter	No	No	No	No	No

All the protocol suites that are supported for a communication adapter feature can be used concurrently across the same communication adapter interface. For example an interface on the 6611 2-Port Serial Adapter can be configured to support the transport of TCP/IP, NetWare, XNS, DECnet and AppleTalk protocol suites concurrently.

This is possible because the data link protocols used by the communication adapter features that support multiple protocol suites provide a mechanism for distinguishing between the various protocol suites sharing the same communication interface.

For example, the PPP data link protocol uses a 2-byte protocol code within each frame to distinguish between protocol suites sharing the same communication interface.

Note: The communication adapter features supported for the TCP/IP protocol suite can also be used to support the transfer of information that originates from nodes that use either the SNA or the NetBIOS protocol suites. This is achieved using the 6611 Network Processor Data Link Switching function which encapsulates the SNA or NetBIOS protocols inside the TCP protocol. This is described further in 2.2.3, "Data Link Switching" on page 40.

2.2.1.2 Routing Table Maintenance

The 6611 Network Processor uses separate routing tables for each of the protocol suites it supports. That is, there is one routing table for each protocol suite supported by the 6611 Network Processor.

For the DECnet, XNS, NetWare and AppleTalk protocol suites, their routing tables are maintained using the corresponding routing table maintenance protocol dynamically. For example the XNS protocol suite uses XNS RIP (Routing Information Protocol) for this purpose.

For the TCP/IP protocol suite, several routing table maintenance protocols can be used either singularly or in combination to maintain the single TCP/IP routing table. Additionally, *static routes* can be manually defined during configuration of the 6611 Network Processor.

The TCP/IP routing table maintenance protocols supported by the 6611 Network Processor are:

- Interior protocols used within an autonomous system:

  TCP/IP RIP (Routing Information Protocol)
  Hello
  OSPF (Open Shortest Path First)

- Exterior protocols used between autonomous systems:

  EGP (Exterior Gateway Protocol)
  BGP (Border Gateway Protocol)

Note: Support for BGP will not be included in the initial general availability of the 6611 Network Processor and Multiprotocol Network Program. Refer to the 6611 Network Processor and Multiprotocol Network Program announcement letters for the date when support for BGP will become available.

2.2.1.3 Filtering

The 6611 Network Processor multiprotocol routing function provides a very comprehensive filtering capability. There are three types of filtering provided:

1. Filtering based on protocol suite

   The routing of each supported protocol suite can be selectively disabled or enabled for each 6611 Network Processor. That is, each 6611 Network Processor can be configured to either ignore (filter) or route each of the supported protocol suites.

   For example, a 6611 Network Processor can be configured to ignore the DECnet protocol suite, and only route the TCP/IP, XNS, AppleTalk and NetWare protocol suites. Frames received by the 6611 Network Processor

that are identified as DECnet will be discarded, and frames received that are identified as either TCP/IP, XNS, AppleTalk or NetWare will be routed.

2. Filtering based on communication interface

   If the routing of a particular protocol suite is enabled for a 6611 Network Processor, it can be selectively disabled or enabled for each communication interface. That is, each communication interface can be configured to either ignore or route a particular protocol suite.

   For example, a 6611 Network Processor that is enabled for routing the TCP/IP protocol suite, can be configured to ignore the TCP/IP protocol suite on one of its communication interfaces, and only route the TCP/IP protocol suite on the remaining communication interfaces.

3. Filtering based on network layer address

   For each protocol suite the 6611 Network Processor provides additional filtering capabilities that allow the enabling or disabling of routing based on network layer addresses. These filters are either specific to a particular communication interface or global to all communication interfaces.

   The specifics of these filters vary between protocol suites as each protocol suite uses a different form of network layer addressing.

2.2.2 Source Route Bridging

The 6611 Network Processor provides source route bridging between IBM Token-Ring Networks. The following types of bridging are possible:

- Local bridging
- Remote bridging between 6611 Network Processors
- Remote bridging between a 6611 Network Processor and a PS/2 running the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) with PTF UR37051

All types of bridging can be combined in a single configuration if required. Also the bridging functions can be used concurrently with the other functions provided by the 6611 Network Processor. This is described further in 2.2.4, "Concurrent Use of Functions" on page 50.

Each type of source route bridging provided by the 6611 Network Processor is described in the following sections.

2.2.2.1 Local Bridging

The 6611 Network Processor provides local source route bridging between multiple Token-Ring Network segments that are directly attached to a 6611 Network Processor.

An example 6611 Network Processor local bridging configuration is illustrated in Figure 12 on page 30.

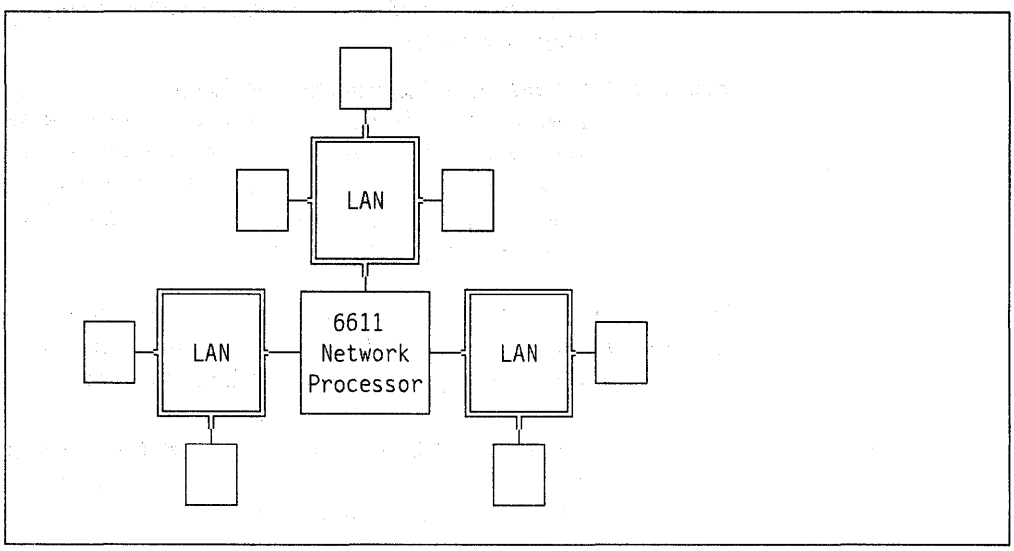


Figure 12. 6611 Used as a Local Source Route Bridge

Each Token-Ring Network segment is attached to the 6611 Network Processor using a 6611 Token-Ring Network 16/4 Adapter. The 6611 Network Processor Model 140 can support the attachment of up to four local Token-Ring Network segments. The 6611 Network Processor Model 170 can support the attachment of up to seven local Token-Ring Network segments.

Each 6611 Network Processor that is enabled for the bridging function must be assigned a single bridge number, and each Token-Ring Network interface which is enabled for the bridging function, must be configured with the segment number for the Token-Ring Network segment to which the interface is attached.

Note: Each 6611 Network Processor can only have a single interface configured for bridging for each Token-Ring Network segment. Since the 6611 Network Processor can only implement a single bridge number, multiple interfaces (configured for bridging) cannot be attached to the same Token-Ring Network segment.

The 6611 Network Processor when used as a source route bridge can forward three types of frames:

All-Routes Broadcast

When the 6611 Network Processor receives an all-routes broadcast frame on one of its Token-Ring Network interfaces, it copies the frame to all the other Token-Ring Network segments to which it is attached. In doing so it updates the RI (Routing Information) field of each copy of the received frame with its bridge number, and the segment number of the destination Token-Ring Network segment. The RI field is also updated with the source segment number if it is not already present within the RI field.

Single-Route Broadcast

When the 6611 Network Processor receives a single-route broadcast frame, it only copies the frame to the other Token-Ring Network segments if the corresponding interface has been enabled for the forwarding of single-route broadcast frames. Each interface can either be manually or automatically configured for the forwarding of single-route broadcast frames. The RI field for each copy of the

received frame is updated in the same manner as for all-routes broadcast frames.

Non-Broadcast with Routing Information Field

When the 6611 Network Processor receives a non-broadcast frame that contains an RI (Routing Information) field it will forward the frame if the next entry in the RI field contains the bridge number of the 6611 Network Processor and the segment number of a segment attached to the 6611 Network Processor.

The 6611 Network Processor is able to participate in the automatic configuration of the single-route broadcast function using the spanning tree algorithm with other source route bridges that support this capability.

2.2.2.2 Remote Bridging - between 6611 Network Processors

The 6611 Network Processor provides remote source route bridging between multiple Token-Ring Network segments that are attached to two or more 6611 Network Processors.

An example 6611 Network Processor remote bridging configuration is illustrated in Figure 12 on page 30.

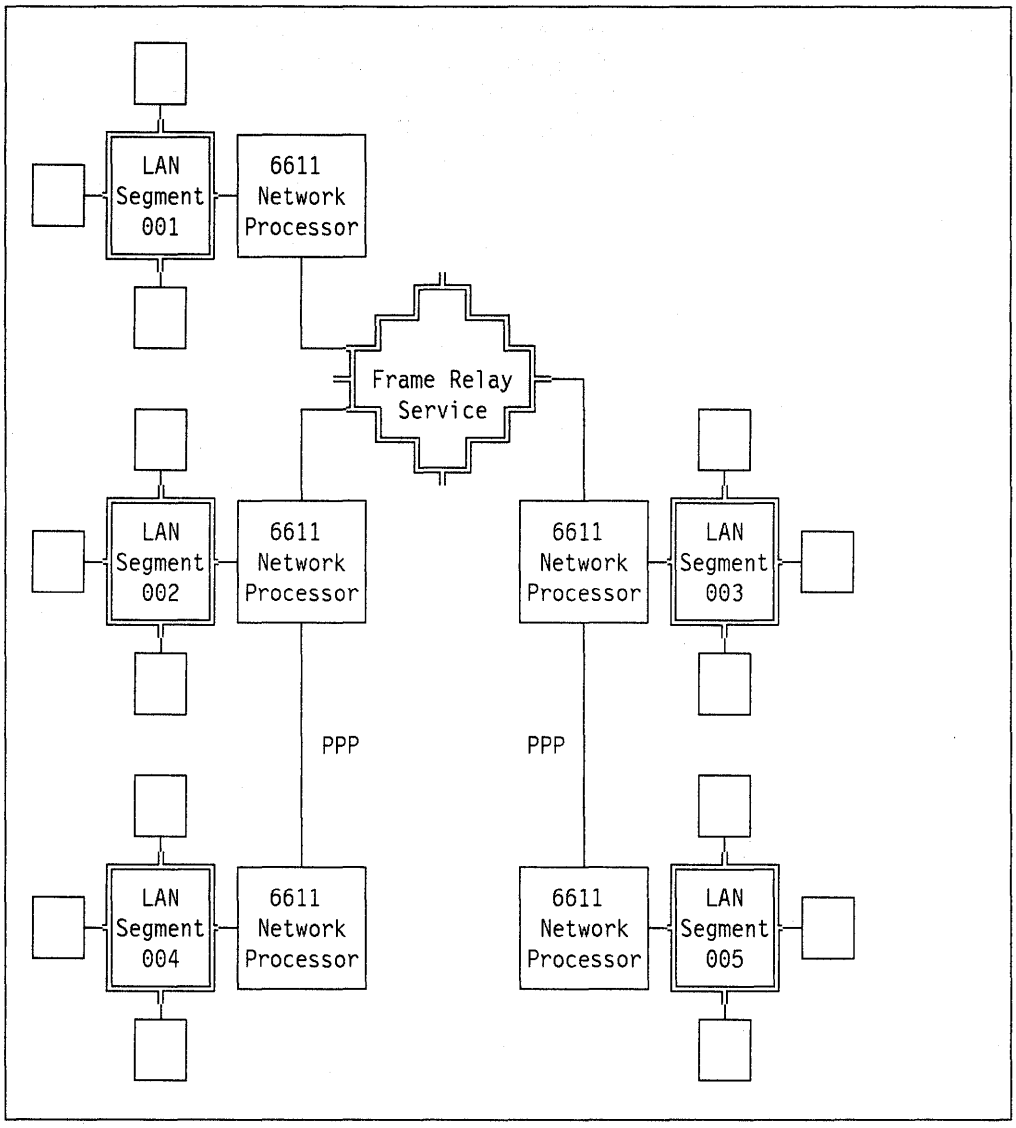


Figure 13. 6611s Used as Remote Source Route Bridges - Physical View

Each Token-Ring Network segment is attached to a 6611 Network Processor using a 6611 Token-Ring Network 16/4 Adapter. The remote connections between each 6611 Network Processor utilize the 6611 2-Port Serial Adapter or 6611 2-Port V.35/V.36 Compatible Serial Adapter, and can use either the PPP or frame relay data link protocols at speeds between 19.2 Kbps and 2.048 Mbps.

Each connection between 6611 Network Processors can be either:

- A point-to-point communication facility such as the T1 or E1 services provided by many common carriers. Such a connection would use PPP data link protocols.
- A DLC (Data Link Connection) across a frame relay service. Many DLCs can share the same physical interface to a frame relay service using a unique DLCI (Data Link Connection Identifier) to distinguish between each DLC. This allows a 6611 Network Processor to establish connections with many other 6611 Network Processors using a single physical interface to a frame relay service.

For example, in Figure 13, each 6611 Network Processor that is attached to the frame relay network would have two DLCs, one to each of the other 6611 Network Processors attached to the frame relay network. This is illustrated in Figure 14 on page 33.

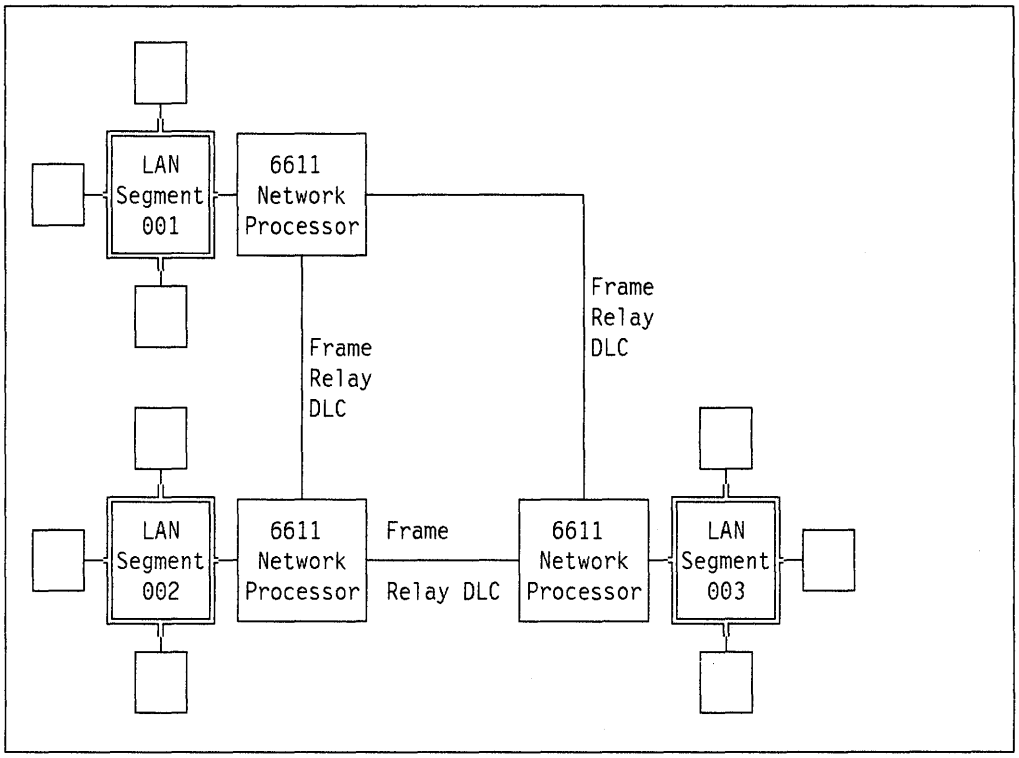


Figure 14. Data Link Connections across a Frame Relay Network

As is the case for local bridging, each 6611 Network Processor that is enabled for the bridging function must be assigned a single bridge number, and each Token-Ring Network interface which is enabled for the bridging function, must be configured with the segment number of the Token-Ring Network segment to which the interface is attached.

The bridge number assigned to the 6611 Network Processor will be used not only for bridging with remote Token-Ring Network segments attached to other 6611 Network Processors, but also for local bridging and remote bridging with PS/2s.

Additionally, each remote connection between 6611 Network Processors is assigned a unique Token-Ring Network segment number which will be referred to as a *link segment number*. The 6611 Network Processor remote bridging function uses each remote connection (or *link segment*) in the same manner as the 6611 Network Processor local bridging function would use a real Token-Ring Network segment.

For example the network illustrated in Figure 13 on page 32 is equivalent to the network illustrated in Figure 15 on page 34 where each connection between 6611 Network Processors has been replaced by a link segment.

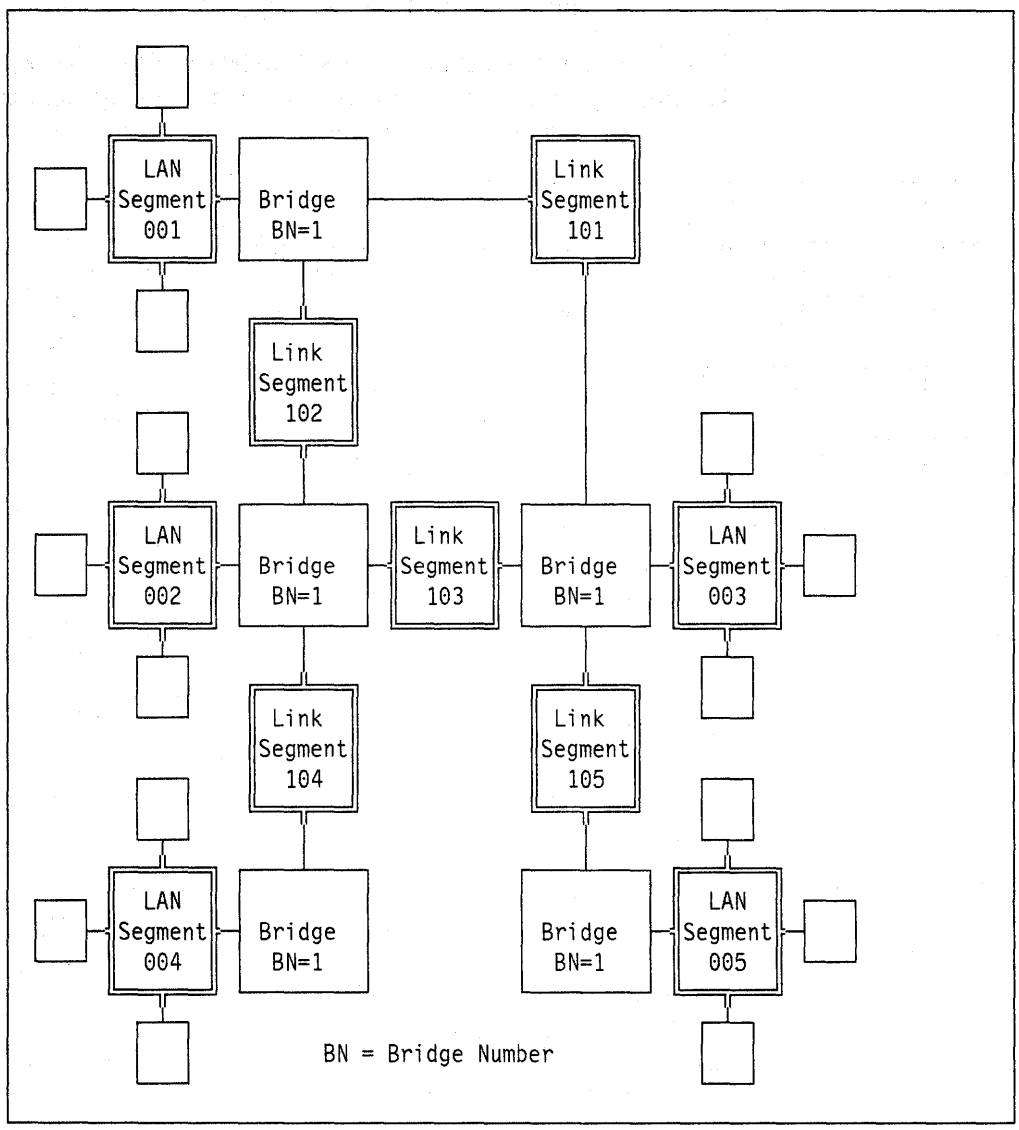


Figure 15. 6611s Used as Remote Source Route Bridges - Logical View

The use of link segment numbers differs significantly from previous IBM remote bridging products such as the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) which had no such concept. In particular, the number of hops used within the RI (Routing Information) field of each frame can become quite large in complex networks of 6611 Network Processors.

For example in Figure 13 on page 32, as many as four hops are required within the RI field to reach other Token-Ring Network segments via the shortest path, such as between segments 004 and 005. The shortest path in the RI field from segment 004 to segment 005 is X'004 1 104 1 103 1 105 1 005 0', or more simply:

1. LAN segment 004 (source segment)
2. Bridge 1 (6611)
3. Link segment 104 (a PPP link)
4. Bridge 1 (6611)
5. Link segment 103 (a Frame Relay link)
6. Bridge 1 (6611)
7. Link segment 105 (a PPP link)
8. Bridge 1 (6611)

9. LAN segment 005 (destination segment)

This is further illustrated in Table 3 which lists the shortest paths between all the Token-Ring Network segments in Figure 13 on page 32 using the link segment and bridge numbering scheme provided in Figure 15 on page 34.

Table 3. Shortest Paths between Token-Ring Network Segments

From Segment	To Segment X'001'	To Segment X'002'	To Segment X'003'	To Segment X'004'	To Segment X'005'
X'001.'	N/A	X'001 1 102 1 002 0'	X'001 1 101 1 003 0'	X'001 1 102 1 104 1 004 0'	X'001 1 101 1 105 1 005 0'
X'002'	X'002 1 102 1 001 0'	N/A	X'002 1 103 1 003 0'	X'002 1 104 1 004 0'	X'002 1 103 1 105 1 005 0'
X'003'	X'003 1 101 1 001 0'	X'003 1 103 1 002 0'	N/A	X'003 1 103 1 104 1 004 0'	X'003 1 105 1 005 0'
X'004'	X'004 1 104 1 102 1 001 0'	X'004 1 104 1 002 0'	X'004 1 104 1 103 1 003 0'	N/A	X'004 1 104 1 103 1 105 1 005 0'
X'005'	X'005 1 105 1 101 1 001 0'	X'005 1 105 1 103 1 002 0'	X'005 1 105 1 003 0'	X'005 1 105 1 103 1 104 1 004 0'	N/A

2.2.2.3 Remote Bridging - between 6611 Network Processor and PS/2

The 6611 Network Processor provides remote source route bridging between multiple Token-Ring Network segments that are attached to a 6611 Network Processor, and multiple IBM Personal System/2s running the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R), each attached to a single Token-Ring Network segment.

An example 6611 Network Processor with PS/2 remote bridging configuration is illustrated in Figure 16 on page 36.

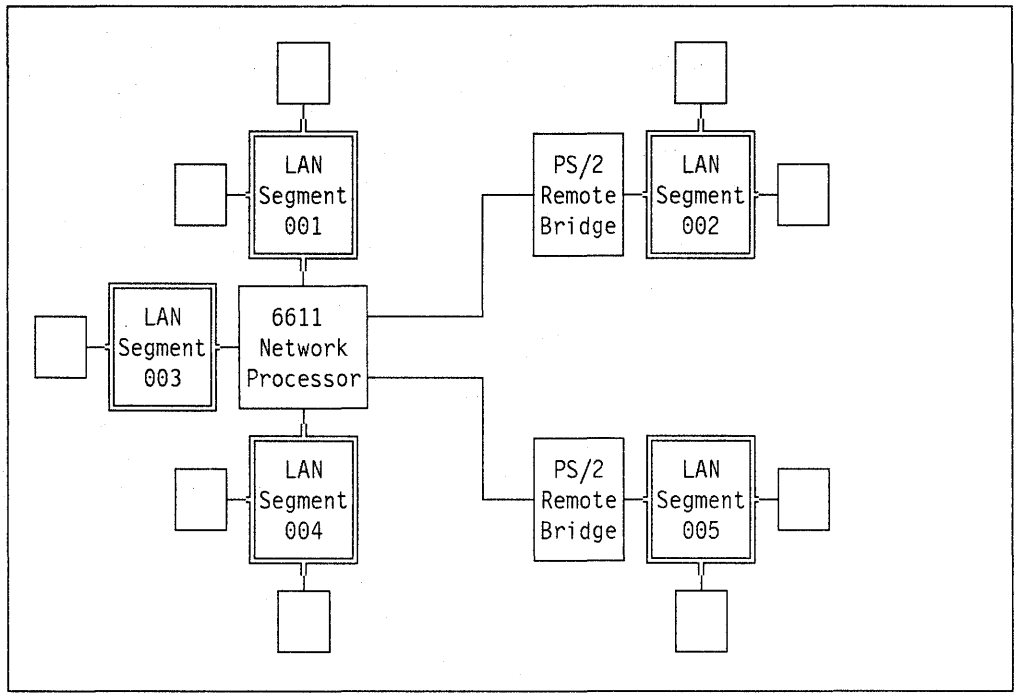


Figure 16. 6611 Used with PS/2s as Remote Bridges - Physical View

Token-Ring Network segments are attached to the 6611 Network Processor using the 6611 Token-Ring Network 16/4 Adapter. Remote connections between 6611 Network Processors and PS/2s utilize point-to-point links at speeds between 19.2 Kbps and 1.344 Mbps (2.048 Mbps in some countries), and are attached to the 6611 Network Processor using the 6611 2-Port Serial Adapter or 6611 2-Port V.35/V.36 Compatible Serial Adapter.

Each PS/2 remote bridge is configured as the secondary half of a remote bridge configuration using the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R). PTF UR37051 should be installed on the PS/2 remote bridge if management of the remote Token-Ring Network segment by IBM LAN Network Manager is required. This PTF should only be installed on a PS/2 remote bridge that is connected to a 6611 Network Processor.

As is the case for local bridging, each 6611 Network Processor that is enabled for the bridging function must be assigned a single bridge number, and each Token-Ring Network interface which is enabled for the bridging function, must be configured with the segment number of the Token-Ring Network segment to which the interface is attached.

The bridge number assigned to the 6611 Network Processor will be used not only for bridging with remote Token-Ring Network segments attached via PS/2s, but also for local bridging and remote bridging with other 6611 Network Processors.

Note: The 6611 Network Processor can only have a connection to a single PS/2 remote bridge attached to each remote Token-Ring Network segment. Multiple connections to the same Token-Ring Network segment are not possible as the 6611 Network Processor can only implement a single bridge number.

Additionally, one of the Token-Ring Network segments locally attached to the 6611 Network Processor must be selected to become the *designated segment*. All the PS/2 remote bridges connected to a 6611 Network Processor are logically bridged to the designated segment. This is illustrated in Figure 17 on page 37.

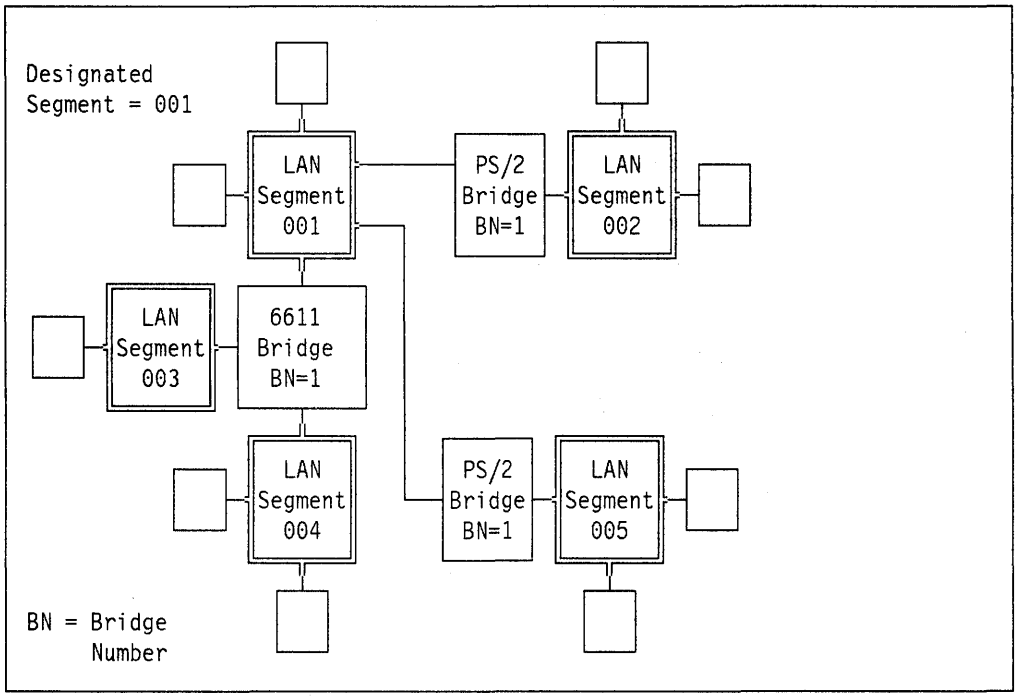


Figure 17. 6611 Used with PS/2s as Remote Bridges - Logical View

Note: Frames transported by the 6611 Network Processor between Token-Ring Network segments other than the designated segment, do not appear on the designated segment. Instead they are processed entirely within the 6611 Network Processor. However the designated segment number does appear in the RI field of frames transported to or from remote Token-Ring Network segments attached to PS/2 remote bridges.

For example, consider Table 4 which lists the shortest paths between all the Token-Ring Network segments in Figure 16 on page 36 using the bridge numbering scheme provided in Figure 17.

Table 4. Shortest Paths between Token-Ring Network Segments

From Segment	To Segment X'001'	To Segment X'002'	To Segment X'003'	To Segment X'004'	To Segment X'005'
X'001'	N/A	X'001 1 002 0'	X'001 1 003 0'	X'001 1 004 0'	X'001 1 005 0'
X'002'	X'002 1 001 0'	N/A	X'002 1 001 1 003 0'	X'002 1 001 1 004 0'	X'002 1 001 1 005 0'
X'003'	X'003 1 001 0'	X'003 1 001 1 002 0'	N/A	X'003 1 004 0'	X'003 1 001 1 005 0'
X'004'	X'004 1 001 0'	X'004 1 001 1 002 0'	X'004 1 003 0'	N/A	X'004 1 001 1 005 0'
X'005'	X'005 1 001 0'	X'005 1 001 1 002 0'	X'005 1 001 1 003 0'	X'005 1 001 1 004 0'	N/A

2.2.2.4 Filtering

The 6611 Network Processor source route bridging function provides a very comprehensive filtering capability.

Filters can be configured for each communication interface that participates in source route bridging. This includes interfaces on both the 6611 Token-Ring Network 16/4 Adapter and the 6611 2-Port Serial Adapter or 6611 2-Port V.35/V.36 Compatible Serial Adapter when remote source route bridging is used.

For each communication adapter interface, both inbound and outbound filters can be configured. Inbound filters act upon frames received by the 6611 Network Processor across the communication interface. Outbound filters act upon frames scheduled for transmission by the 6611 Network Processor across the communication interface.

There are five types of filters which can be configured for each interface. With the exception of the hop count filter, each type can be configured separately for inbound and outbound operation. The five filter types available are:

Hop Count This filter can be used to process frames that have more than an allowable number of hops in their RI (Routing Information) field.

MAC Address This filter can be used to process frames that are to or from specific MAC (Media Access Control) addresses.

Source SAP This filter can be used to process frames that contain a specific source SAP (Service Access Point).

SNAP Value This filter can be used to process frames that contain a specific SNAP (Sub-Network Access Protocol) header. SNAP headers exist in frames that have source and destination SAP values of X'AA'.

Segment Number This filter can be used to process frames that contain a specific origin segment number within the RI (Routing Information) field.

Each type of filter only acts upon either single route broadcast, or all-routes broadcast frames, or both. Each type of filter can be set to operate in one of two modes:

- Include only frames which match the filter characteristic (not used by the hop count filter). This is *permit* mode.
- Exclude only frames which match the filter characteristic (always used by the hop count filter). This is *deny* mode.

With the exception of the hop count filter, each type of filter provides the capability for multiple values to be filtered concurrently, and a mask capability allows a range of values to be specified with a single entry. Only those bits set in the mask are used for comparisons between the value specified and the frame being processed by the filter.

All five types of filters can be used concurrently if required. With the exception of the hop count filter, each type of filter can be individually enabled or disabled.

Notes:

1. Use of the SNAP value filter requires that the corresponding source SAP filter also be enabled. For example, to use the outbound SNAP value filter for an interface, the outbound source SAP filter for the same interface *must* also be enabled. No SAPs need be defined for the source SAP filter if only the SNAP value filter is required.
2. The hop count filter can be effectively disabled by setting the hop count value to "7" which is the maximum hop count possible in Token-Ring Networks.

To illustrate how multiple filters work together, consider the following scenario where outbound source SAP, outbound ring number and hop count filters are used concurrently for a Token-Ring Network interface. The filter settings are listed in Table 5.

Table 5. Example Filter Settings

Filter Type	Mode	Value(s)
Outbound Source SAP	Deny	X'AA' X'F0'
Outbound Ring Number	Permit	X'100' X'200' X'300'
Hop Count	Deny	2

For a frame to pass through the interface for which these filters are enabled it must meet *all* of the following criteria:

1. It must have a source SAP that is not X'AA' or X'F0'. For example, a frame with a source SAP of X'04' would meet this requirement, whereas a frame with a source SAP of X'F0' would not.
2. It must contain an origin segment number of X'100', X'200' or X'300'. For example a frame with a routing information field of X'100 1 300 0' would meet this requirement, whereas a frame with a routing information field of X'400 1 300 0' would not.
3. The routing information field must contain 2 hops or less. For example a frame with a routing information field of X'100 1 200 1 300 0' would meet this requirement, whereas a frame with a routing information field of X'200 1 800 1 100 1 300 0' would not.

2.2.2.5 Coexistence with Other IBM Bridge Products

The 6611 Network Processor can coexist with other bridges such as the IBM 8209 LAN Bridge Version 1.0 and the IBM Personal System/2 using the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R). This includes support for automatic single-route broadcast configuration using the spanning tree algorithm.

However the 6611 Network Processor does not implement the following functions provided by other IBM bridge products:

- RPS (Ring Parameter Server)
- REM (Ring Error Monitor)
- CRS (Configuration Report Server)
- LRM (LAN Reporting Mechanism)
- LBS (LAN Bridge Server)

As a consequence there are some limitations when using IBM LAN Network Manager to manage interconnected Token-Ring Networks that incorporate 6611 Network Processor based bridges. These limitations are described further in 4.3, "IBM LAN Network Manager (LNM) Considerations" on page 132.

2.2.3 Data Link Switching

The 6611 Network Processor provides a new function called Data Link Switching or more simply DLS. The DLS function provides the capability to integrate the transport of the NetBIOS and SNA protocol suites with the other protocol suites that can be routed by the 6611 Network Processor.

Devices which make use of the DLS function are configured as if they were directly attached to each other via a single data link or data link network. This is illustrated in Figure 18.

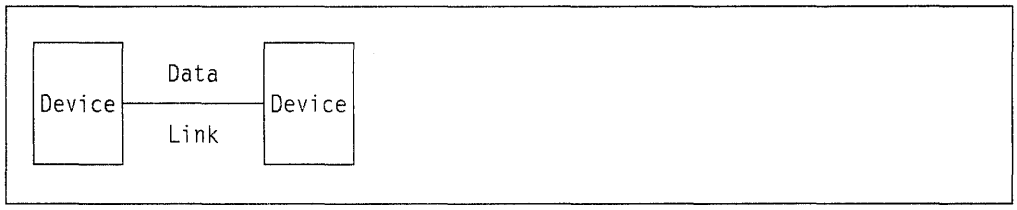


Figure 18. Device View of a DLS Connection

In reality these devices only have a direct data link or data link network connection to a 6611 Network Processor. The 6611 Network Processor then transports information received on the data link or data link network connection to another 6611 Network Processor. This second 6611 Network Processor has a direct data link or data link network connection with the ultimate destination device. This is illustrated in Figure 19.

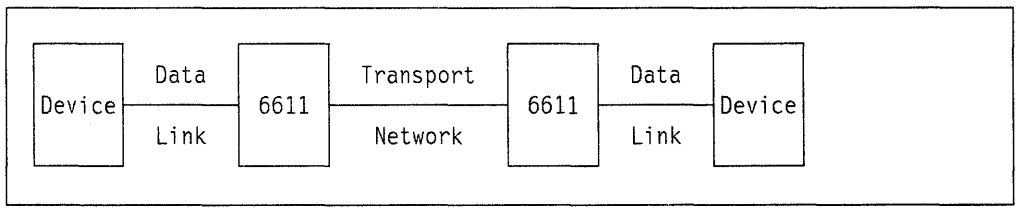


Figure 19. Real View of DLS Connection

The two data links or data link networks that are connected via the DLS function need not be the same type of data link or data link network. For example an SNA device attached via an SDLC data link to a 6611 Network Processor can use the DLS function to connect to an SNA device attached via a Token-Ring Network data link network.

The DLS function uses the TCP transport layer protocol (part of the TCP/IP protocol suite) to implement a transport network between 6611 Network Processors. This transport network can comprise many intermediate nodes, data links and data link networks, if required, through the use of the IP network layer protocol (also part of the TCP/IP protocol suite).

Note: Intermediate nodes in the transport network used to connect 6611 Network Processors that are providing the DLS function do not have to be 6611 Network Processors, provided that they can support the IP network layer protocol.

A TCP connection is automatically established between each pair of 6611 Network Processors that are participating in the DLS function across the TCP/IP transport network. To support the establishment of these TCP connections, each 6611 Network Processor is configured with the TCP/IP network addresses of the other 6611 Network Processors participating in the DLS function.

It is possible to configure a 6611 Network Processor to accept incoming DLS TCP connections from other 6611 Network Processors without explicitly configuring the other 6611 Network Processors. This may reduce the amount of configuration effort required to set up complex DLS environments. However, at least one of the two 6611 Network Processors participating in each DLS TCP connection must be configured with the TCP/IP network address of the other 6611 Network Processor.

The communication adapter features that can be used with the DLS function fall into four categories:

- Those which support direct data links to SNA devices.
- Those which support direct data links to NetBIOS devices.
- Those which support indirect data links to Token-Ring Network devices (both SNA and NetBIOS) via a remote source route bridge configuration.
- Those which support connection to the TCP/IP transport network used to interconnect 6611 Network Processors that provide the DLS function.

The communication adapter features that can be used with the DLS function in each of these roles are summarized in Table 6.

Table 6. Communication Adapter Features Supported for Data Link Switching

Adapter	Direct SNA	Direct NetBIOS	Remote Bridge	TCP/IP Transport
6611 2-Port Serial Adapter	No	No	Yes	Yes
6611 2-Port V.35/V.36 Compatible Serial Adapter	No	No	Yes	Yes
6611 Ethernet Adapter	No	Yes	No	Yes
6611 Token-Ring Network 16/4 Adapter	Yes	Yes	No	Yes
6611 X.25 Adapter	No	No	No	Yes
6611 4-Port SDLC Adapter	Yes	No	No	No

Note: Support for NetBIOS devices attached via the 6611 Ethernet Adapter will not be included in the initial general availability of the 6611 Network Processor. Refer to the 6611 Network Processor and Multiprotocol Network Program announcement letters for the date when support for NetBIOS devices attached via the 6611 Ethernet Adapter will become available.

The DLS function incorporates several features to reduce the need to send data across the TCP/IP network that interconnects the 6611 Network Processors participating in the DLS function.

The key feature is the *cache* in which each 6611 Network Processor maintains a table of remote SNA and NetBIOS devices along with the 6611 Network Processor that is able to reach that remote device by the fastest path. Each 6611 Network Processor constructs its cache dynamically by sending queries to other

6611 Network Processors only when needed. The cache can be preloaded with default entries when the 6611 Network Processor is configured to further reduce the need for queries to be sent to other 6611 Network Processors.

An age out timer is used to remove old cache entries after a a period of time. The timeout used by the age out timer can be set when the 6611 Network Processor is configured.

Note: At the time of writing, the cache used by the DLS function could only be used to locate the MAC addresses of remote SNA and NetBIOS devices. As a consequence, NetBIOS requests to locate particular NetBIOS names were copied to all interfaces enabled for DLS on all 6611 Network Processors that participate in the DLS function. However, it is intended that the cache will also be able to be used to locate NetBIOS names of remote NetBIOS devices. This would dramatically reduce the number of NetBIOS broadcasts that flow across the TCP/IP network that interconnects all 6611 Network Processors participating in the DLS function.

There are several differences in the operation of the DLS function for SNA and NetBIOS devices. For this reason each will be described separately in the following sections.

2.2.3.1 SNA Data Link Switching

The DLS function supports the interconnection of SNA devices attached to either a Token-Ring Network or an SDLC multipoint non-switched line. A typical example of the use of the DLS function for SNA devices is illustrated in Figure 20.

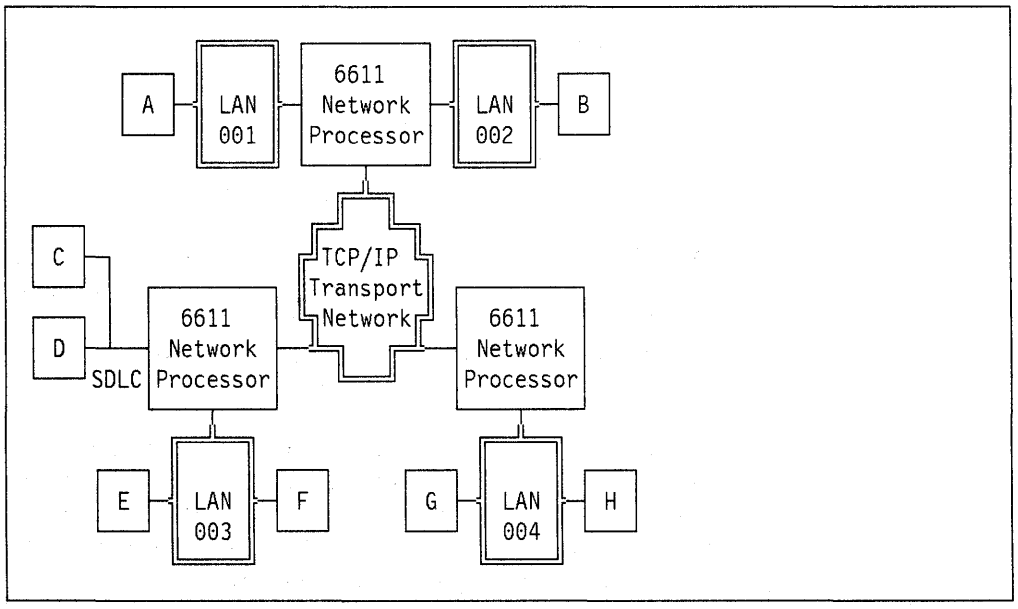


Figure 20. SNA Data Link Switching - Example Configuration

As a prerequisite for the DLS function, each participating 6611 Network Processor that supports Token-Ring Network attached SNA devices, must be configured to support source route local bridging on all Token-Ring Network interfaces used with the DLS function.

Note: Local bridging will be used in preference to the DLS function to provide connections between Token-Ring Network attached SNA devices that are

connected to the same 6611 Network Processor via different Token-Ring Network segments.

Each 6611 Network Processor participating in the DLS function must also be configured with a *virtual segment number*. This *virtual segment* must be the same for all 6611 Network Processors participating in the DLS function.

Additionally, SNA devices attached to a 6611 Network Processor via a SDLC multipoint non-switched line are assigned a Token-Ring Network LAA (Locally Administered Address), SAP (Service Access Point) and SNA XID (Exchange ID) which will be used by the 6611 Network Processor to represent such devices to other SNA devices that are using the DLS function.

SNA devices attached to a 6611 Network Processor via Token-Ring Network segments establish connections with SNA devices attached to other 6611 Network Processors as if they are on the virtual segment. This is illustrated in Figure 21 for the SNA devices on Token-Ring Network segments X'001' and X'002' in Figure 20 on page 42.

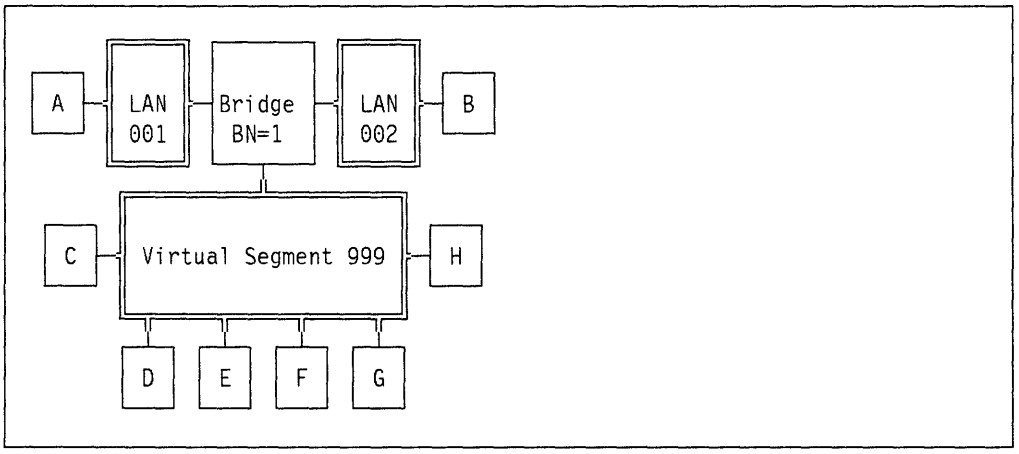


Figure 21. Logical View for SNA Devices on Segments 001 and 002

Note: A single hop is used in the RI (Routing Information) field to reach an SNA device accessible via the DLS function from a Token-Ring Network segment directly attached to a 6611 Network Processor. Therefore SNA devices can be at most six hops (seven less one) from a 6611 Network Processor to reach SNA devices accessible via the DLS function.

SNA devices attached to a 6611 Network Processor via Token-Ring Network segments establish connections with SNA devices attached to the same 6611 Network Processor via SDLC as if they were on the virtual segment. This is illustrated in Figure 22 on page 44 for the SNA devices on Token-Ring Network segment X'003' in Figure 20 on page 42.

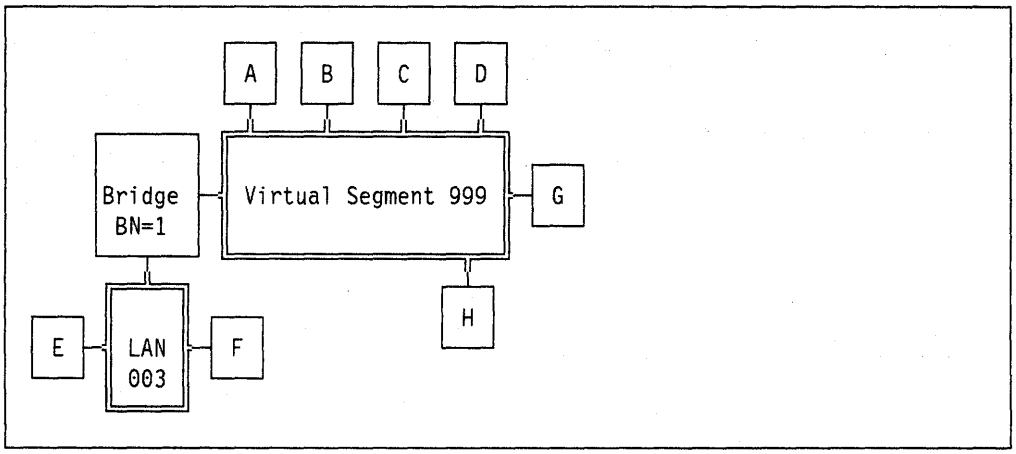


Figure 22. Logical View for Devices on Segment 003

The DLS function only supports the attachment of SNA devices via SDLC multipoint lines that are of PU (Physical Unit) type 2.0. The attachment of PU type 2.1 devices is not supported unless they provide a PU type 2.0 compatibility mode. The attachment of PU type 4 devices (such as the IBM 3745 Communications Controller) is not supported either.

There are two consequences of this:

1. SDLC attached devices cannot establish connections with other SDLC attached devices. This is because SNA PU type 2.0 devices cannot directly communicate with each other as peers.
2. SDLC attached devices can only support a single connection to another SNA device attached to a Token-Ring Network. The other SNA device will usually be a PU type 4 such as the IBM 3745 Communications Controller or a PU type 5.

For example, Figure 23 shows the logical view of the SNA devices attached to the SDLC line in Figure 20 on page 42. Each SDLC attached device can be logically connected to only one other Token-Ring Network attached SNA device at any time.

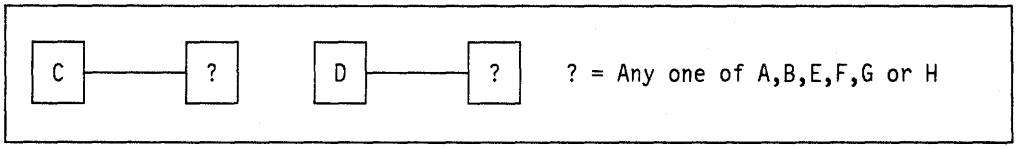


Figure 23. Logical View for Devices on SDLC Multipoint Line

2.2.3.2 NetBIOS Data Link Switching

The DLS function supports the interconnection of NetBIOS devices attached to either a Token-Ring Network or a CSMA/CD (Carrier Sense Multiple Access/Collision Detection) LAN using either DIX Ethernet V2 or IEEE 802.3 frame formats. A typical example of the DLS function for NetBIOS devices is illustrated in Figure 24 on page 45.

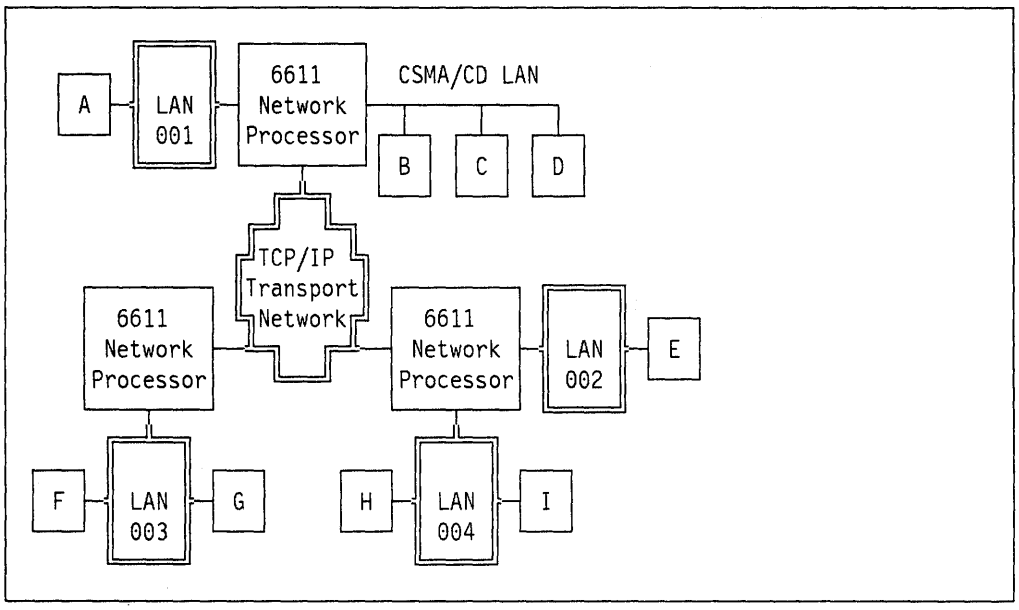


Figure 24. NetBIOS Data Link Switching - Example Configuration

NetBIOS devices on Token-Ring Networks are handled in a similar way to SNA devices on Token-Ring Networks. That is, remote NetBIOS devices will appear as if they are on the DLS virtual segment.

NetBIOS devices on CSMA/CD LANs cannot be handled in a similar way to that used for SNA devices on Token-Ring Networks. Instead the ability of NetBIOS to dynamically bind a MAC address to a NetBIOS name is exploited.

From the perspective of NetBIOS devices on CSMA/CD LANs all remote NetBIOS devices appear as if they have the MAC address of the 6611 Ethernet Adapter. This is possible because the NetBIOS protocol discovers the MAC address of other NetBIOS devices using broadcast frames sent to the NetBIOS functional address.

2.2.3.3 Connection Establishment

From the perspective of SNA and NetBIOS devices using the 6611 Network Processor DLS functions, there is no difference in how connections are established when the DLS function is used.

However, it is useful to understand the connection flows that occur when the DLS function is used, to both aid problem determination and also understand the behavior of the DLS function.

To illustrate how connections using DLS are established between Token-Ring Network attached devices, consider the example configuration illustrated in Figure 25 on page 46.

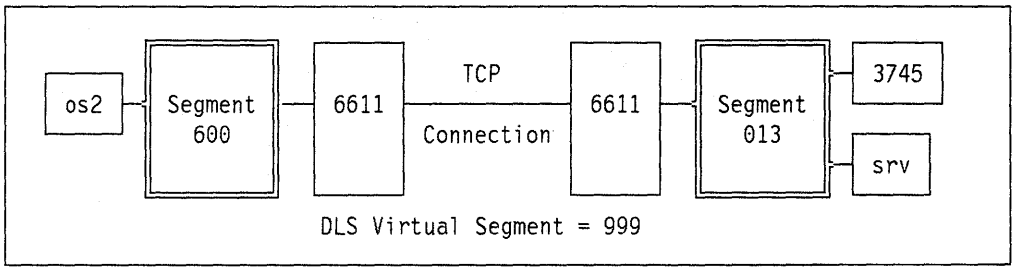


Figure 25. Example Configuration for DLS Connection Establishment

In Figure 25 an OS/2 workstation "os2" is configured to communicate with a communications controller "3745" using SNA protocols, and with an OS/2 server "srv" using NetBIOS protocols.

The establishment of the SNA connection between "os2" and "3745" is illustrated in Figure 26 on page 47 which shows a trace of the frames that are transmitted between each of the SNA devices and the 6611 Network Processors in Figure 25.

The left part of Figure 26 on page 47 under the heading "Token Ring Segment 600" shows frames that appear on the Token-Ring Network segment X'600' and flow between "os2" and the 6611 Network Processor attached to that segment. The first field "Direction" illustrates the source and destination MAC addresses of each frame. The source MAC address is at the tail of the arrow and the destination MAC address is at the head of the arrow. The second field "Route" illustrates the routing information that is part of each frame. The third field "Frame" illustrates the type of frame.

The central part of Figure 26 on page 47 under the heading "DLS TCP Flows" shows when frames are sent between the two 6611 Network Processors across their TCP connection.

The right part of Figure 26 on page 47 under the heading "Token-Ring Segment 013" shows frames that appear on the Token-Ring Network segment X'013' and flow between "3745" and the 6611 Network Processor attached to that segment. The fields "Direction," "Route" and "Frame" have the same meaning as described previously.

The key points to note from this example are:

1. The TEST frame from "os2" to "3745" with an ARB route will be sent to all 6611 Network Processors participating in the DLS function and will be copied to all attached Token-Ring Network segments enabled for DLS. This is the only frame for which this occurs, and all subsequent frames only appear on the Token-Ring Network segments X'600' and X'013'. This behavior is necessary because the 6611 Network Processor that received the TEST frame had no entry for the MAC address of "3745" in its cache and therefore does not know which 6611 Network Processor is able to reach "3745" by the most direct path. Subsequent SNA connections would take advantage of a cache entry for the MAC address of "3745" that is created when the response to the TEST frame is received back from "3745" via the other 6611 Network Processor. This would then remove the need for a TEST frame to be propagated to all Token-Ring Network segments enabled for DLS that are attached to all 6611 Network Processors that participate in the DLS function.

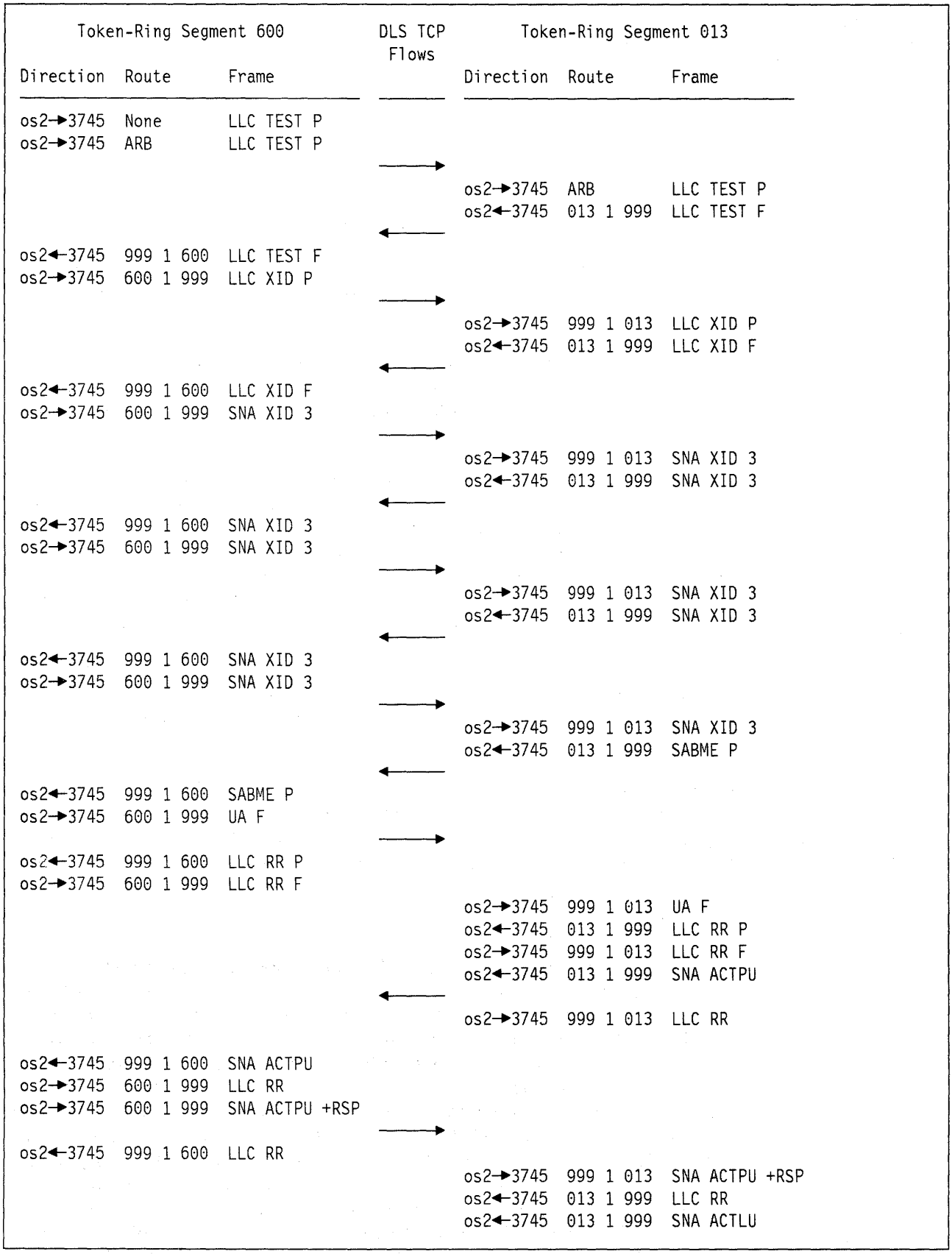


Figure 26. SNA DLS Connection Establishment - No Cached MAC Addresses

2. Once the 6611 Network Processors have seen a successful SABME frame and UA response frame flow between "3745" and "os2" they will use local acknowledgements of frames received and sent. Only information frames are sent across the TCP connection to the other 6611 Network Processor that is supporting an SNA connection using DLS.

The connection establishment illustrated in Figure 26 on page 47 assumes that both 6611 Network Processors initially have no entries in their DLS MAC address cache. If a previous DLS connection had existed or exists with "3745" the connection establishment would differ slightly from that illustrated in Figure 26 on page 47. The main difference lies in the ability of the 6611 Network Processor to respond to the initial TEST frame sent by "os2" without having to send it across the TCP connection to the other 6611 Network Processor.

This is illustrated in Figure 27 which shows the very early part of the SNA connection establishment when the MAC address of "3745" is already in the cache of the 6611 Network Processor receiving the TEST frame.

```
    Token-Ring Segment 600          DLS TCP      Token-Ring Segment 013
                                     Flows
Direction  Route      Frame                     Direction  Route      Frame
-------------------------------------------------------------------------
os2→3745   None       LLC TEST P
os2→3745   ARB        LLC TEST P
os2←3745   999 1 600  LLC TEST F
os2→3745   600 1 999  LLC XID P
                                   ------>
                                              os2→3745   999 1 013  LLC XID P
                                              os2←3745   013 1 999  LLC XID F
                                   <------
os2←3745   999 1 600  LLC XID F
os2→3745   600 1 999  SNA XID 3
```

Figure 27. SNA Connection Establishment - Cached MAC Address

The establishment of the NetBIOS connection between "os2" and "srv" is illustrated in Figure 28 on page 49, which shows a trace of the frames that are transmitted between each of the NetBIOS devices and the 6611 Network Processors in Figure 25 on page 46.

The left part of Figure 28 on page 49 under the heading "Token-Ring Segment 600" shows frames that appear on Token-Ring Network segment X'600' and flow between "os2" and the 6611 Network Processor attached to that segment. The first field "Direction" illustrates the source and destination MAC addresses of each frame. The source MAC address is at the tail of the arrow and the destination MAC address is at the head of the arrow. A destination MAC address of "NETB" is used to indicate frames sent to the NetBIOS functional address. The second field "Route" illustrates the routing information that is part of each frame. The third field "Frame" illustrates the type of frame.

The central part of Figure 28 on page 49 under the heading "DLS TCP Flows" shows when frames are sent between the two 6611 Network Processors across their TCP connection.

The right part of Figure 28 on page 49 under the heading "Token-Ring Segment 013" shows frames that appear on the Token-Ring segment X'013' and flow

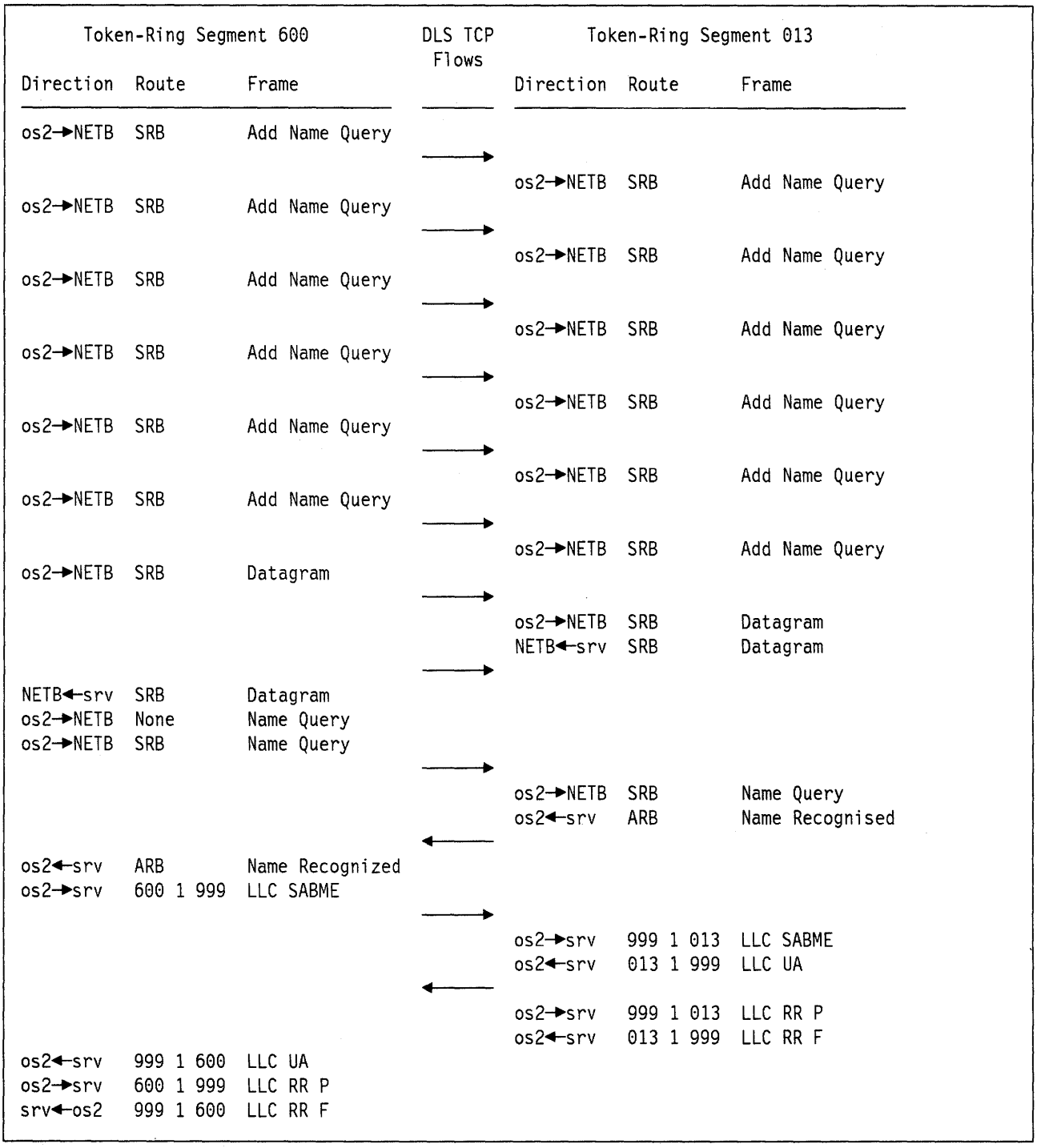


Figure 28. NetBIOS Connection Establishment

between "srv" and the 6611 Network Processor attached to that segment. The fields "Direction," "Route" and "Frame" have the same meaning as described previously.

The key points to note from this example are:

1. Frames sent to the NetBIOS functional address will be sent to all 6611 Network Processors participating in the DLS function and will be copied to all attached Token-Ring Network segments enabled for DLS.

2. Once the 6611 Network Processors have seen a successful SABME frame and UA response frame flow between "os2" and "srv" they will use local acknowledgements of frames received and sent.

2.2.3.4 Filters

The DLS function provides a comprehensive filtering capability for both the SNA and the NetBIOS protocol suites.

Filters are applied at the establishment of DLS connections.

Four filters are provided, two for each protocol suite. These are:

- A source filter for SNA
- A source filter for NetBIOS
- A destination filter for SNA
- A destination filter for NetBIOS

Each filter can be configured to perform comparisons with multiple values concurrently. The type of values used for each protocol suite are:

SNA Filters process both the source MAC address field and the destination MAC address field of SNA frames. Masks are available to allow comparisons with a range of MAC addresses in a single operation. Only those bits set in the mask are used for comparisons between the value specified and the frame being processed by the filter.

NetBIOS Filters process the NetBIOS source or destination name field.

Each of the four filters can be set to operate in one of two modes:

- Include only frames which match the filter characteristic
- Exclude only frames which match the filter characteristic

All four DLS filters can be individually enabled or disabled, and all can be used in any combination concurrently if required.

2.2.4 Concurrent Use of Functions

The three main functions provided by the 6611 Network Processor (that is, routing, source route bridging and DLS) can all be used concurrently if required.

To understand how the 6611 Network Processor operates when multiple functions are used concurrently, it is most convenient to consider each communication adapter feature separately.

2.2.4.1 6611 Token-Ring Network 16/4 Adapter

The 6611 Token-Ring Network 16/4 Adapter can be used by the routing, source route bridging and DLS functions.

The following summary describes the processing performed by the 6611 Network Processor for interfaces on 6611 Token-Ring Network 16/4 Adapters.

1. If a frame is directed to either the interface MAC address or the all stations MAC address (X'FFFF FFFF FFFF'), the 6611 Network Processor will copy the frame. The frame header will then be examined to determine what protocol is contained within the frame. If the protocol is recognized and enabled for the interface on which the frame was received, the frame is processed by the

6611 Network Processor routing function for that protocol. Otherwise the frame is discarded.

2. If the source route bridging function is enabled for the interface, frames observed on the interface that contain an RI (Routing Information) field are processed by the source route bridging function.
3. If the DLS function is enabled, it will receive from the source route bridging function, any single route and all routes broadcast frames, and any non-broadcast frames that are destined for the DLS virtual segment.

Notes:

1. Frames directed to the all stations MAC address (X'FFFF FFFF FFFF') that also contain an RI field (usually denoting a single route or all routes broadcast) can be processed by both the routing function and the source route bridging function. For example TCP/IP ARP frames would be processed in this way.
2. The DLS function requires that the source route bridging function be operational.

2.2.4.2 6611 Ethernet Adapter

The 6611 Ethernet Adapter can be used by the routing and DLS functions. The DLS function only provides support for the NetBIOS protocol suite on the 6611 Ethernet Adapter

The following summary describes the processing performed by the 6611 Network Processor for interfaces on 6611 Ethernet Adapters.

1. If a frame is directed to either the interface MAC address or the all stations MAC address (X'FFFF FFFF FFFF'), the 6611 Network Processor will copy the frame. The frame header will then be examined to determine what protocol is contained within the frame. If the protocol is recognized and enabled for the interface on which the frame was received, the frame is processed by the 6611 Network Processor routing function for that protocol, except for NetBIOS which will be processed by the DLS function if enabled. Otherwise the frame is discarded.
2. If a frame is directed to the NetBIOS functional address X'C000 0000 0080' it will be processed by the DLS function if enabled.

2.2.4.3 6611 2-Port Serial Adapter and 6611 2-Port V.35/V.36 Compatible Serial Adapter

The 6611 2-Port Serial Adapter and 6611 2-Port V.35/V.36 Compatible Serial Adapter can be used by the routing and source route bridging functions.

The following summary describes the processing performed by the 6611 Network Processor for interfaces on 6611 2-Port Serial Adapters and 6611 2-Port V.35/V.36 Compatible Serial Adapters.

1. If the interface is configured to use either the PPP or Frame Relay data link protocol, the 6611 Network Processor will examine the header of each frame received. The frame header indicates whether the frame should be processed by the source route bridging function, or the routing function for a particular protocol.

2. If the interface is configured to use the protocol used by the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R), then the frame is processed by the source route bridging function.

2.2.4.4 6611 X.25 Adapter

This communication adapter feature is only used by the routing function for the routing of the TCP/IP protocol suite. Therefore there are no considerations regarding its concurrent use by multiple functions.

2.2.4.5 6611 4-Port SDLC Adapter

This communication adapter feature is only used by the DLS function for the attachment of SNA SDLC devices. Therefore there are no considerations regarding its concurrent use by multiple functions.

Part 2. Using the IBM 6611

Chapter 3. Configuring the 6611

This chapter describes how to configure an IBM 6611 Network Processor. The different parts are:

- An overview of the configuration options
- The structure of the *Configuration Program*
- A description of the underlying panels
- How to configure for bridging, routing and DLS

A full description of the *Configuration Program* is given in the *Multiprotocol Network Program User's Guide, SC30-3559-00*. For a full understanding of the routing parameters an in depth knowledge of TCP/IP routing protocols is needed. Refer to *Internetworking with TCP/IP Volume 1: Principles, Protocols and Architecture, SC31-6144*, and *TCP/IP Tutorial and Technical Overview, GG24-3376-02*.

3.1 The Configuration Options

There are two ways to configure the 6611 Network Processor:

1. Via the System Manager (updates only)
2. Via the Configuration Program

3.1.1 The System Manager

The *System Manager* lets you access and change the configuration parameters on the 6611 in native mode. It also allows the user to create a *minimal* configuration. This utility runs on the 6611. Because there is no error checking there is a high risk of introducing errors and corrupting the configuration. It is therefore not recommended to use the *System Manager* to change the configuration on the 6611 Network Processor. For a further description of the System Manager's configuration options see 4.1, "System Manager" on page 91.

3.1.2 The Configuration Program

The *Configuration Program* comes as a set of five diskettes and can be loaded either on any IBM Personal System/2 running Microsoft Windows** in *Enhanced Mode* or on an IBM RISC System/6000 with AIXwindows*. The detailed installation procedure is described in *IBM Multiprotocol Network Program: User's Guide*.

Note: Windows must run in the 386 enhanced mode and as such cannot run in a seamless windows mode under OS/2 Version 2.

The IBM 6611 Network Processor comes preloaded with the IBM Multiprotocol Network Program (5648-016). The adapter cards are loaded but not configured. The initial configuration of the 6611 Network Processor can be done via the System Manager or the Configuration Program. If you use the System Manager for initial configuration, you should remember that there is no error checking done by the System Manager and this initial configuration should be just enough to provide an IP address for either a 6611 Ethernet Adapter or a 6611 Token-Ring Network 16/4 Adapter. Once this is done use the Configuration Program to finish the initial configuration. Any time after that, configuration updates can be made

by reading in the configuration diskette and updating, by updating the saved first configuration file or by simply making a new configuration. These updates can then be loaded into the 6611 Network Processor locally via a diskette or remotely over an IP network from the configuration stations. If the configuration station is an IBM RISC System/6000 use the *communicate* option on the menu bar, if your configuration station is an IBM Personal System/2 you will need to have TCP/IP installed to use the FTP option and transfer the configuration file to your 6611 Network Processor.

Advantages of using the *Configuration Program* are:

- Error checking on the protocol and port parameters
- Ability to retain configuration information for later use
- Online help
- User-friendly graphical interface

The configuration is read and activated on the 6611 Network Processor using the *Configuration Process*. Other functions of this process are the sending of configuration files to other 6611 Network Processors using their IP address, and additional functions related to network management. See also 4.1, "System Manager" on page 91.

The flow chart in Figure 29 on page 57 gives an overview of the options when configuring a 6611 Network Processor or updating an existing configuration.

Note: 1 TCP/IP connection to the 6611 Network Processor is either using the *Communicate* option via an IBM RISC System/6000 or using FTP when TCP/IP is installed on a PS/2.

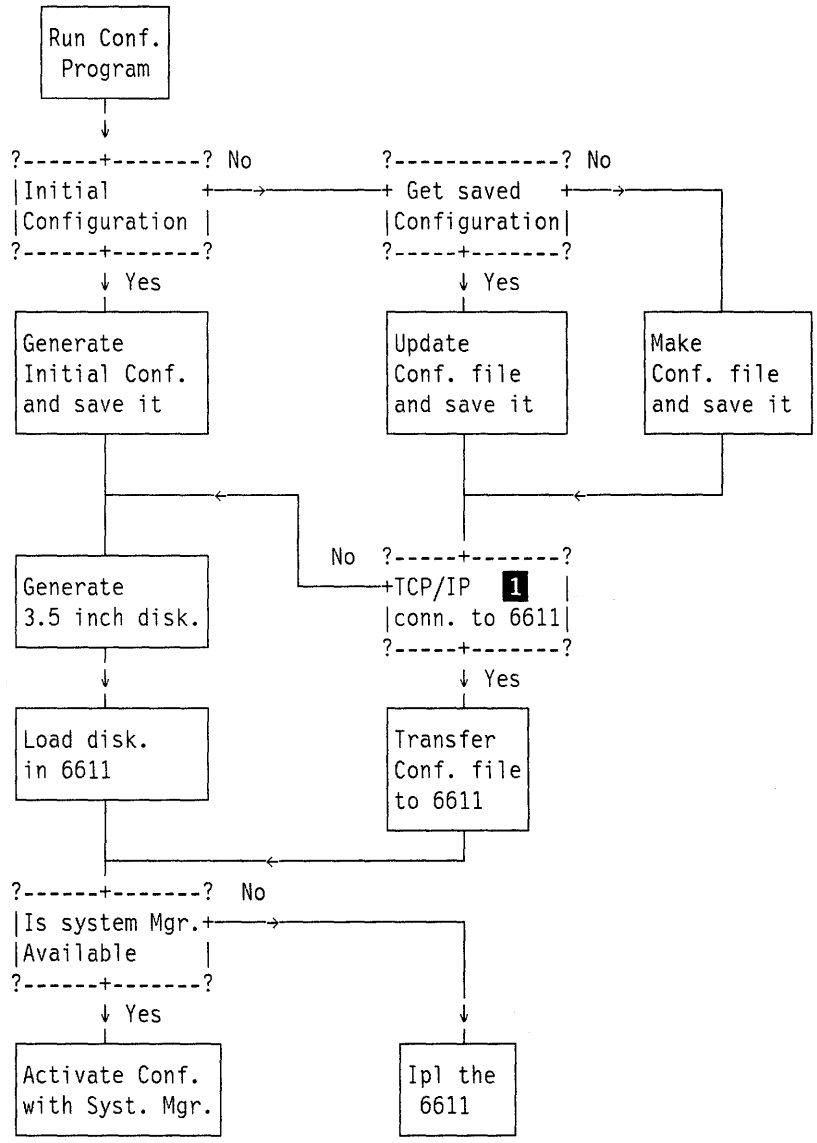


Figure 29. Configuration Flow

3.2 The Structure of the Configuration Program

The *Configuration Program* is menu-driven and is based on system-wide parameter configuration and adapter configuration. The System Management configuration is a third part of the Configuration Program.

The first menu comes up with a reference to the *version id*. Following the first menu is the 6611 Configuration Program Menu, as shown in Figure 30 on page 58. On the menu bar the following options exist:

Configure This pull-down menu lets you configure a new IBM 6611 Network Processor or update an existing configuration, and lets you write it to a diskette or a file.

Communicate This entry lets you communicate with the router over the TCP/IP network and retrieve or download a configuration. Either any host (meaning a system connected to an IP network), can access the router or the list is limited to those hosts defined in the *System Management* entry: **Configuration Hosts**.

Options This pull-down menu allows you to change the colors and fonts, set the startup preference as a 6611-140 or a 6611-170 and set the validity checking. *Validity checking* should always be activated.

Help The help pull-down menu has the following entries:

- Summary Panel, which explains how the help function is structured throughout the Configuration Program.
- Button/Key gives the corresponding PF-key values for the menu entries. For example: PF6 corresponds to activating the Add button on a menu with a mouse.
- Table of Contents of General Help. Highlighting any entry in this list will give a description of the function.
- Help for Help lists the two types of Help panels: General (Window) and Contextual (parameter).
- Copyright.
- Trademarks.
- Tutorial on *Understanding the Configuration Program Windows*.

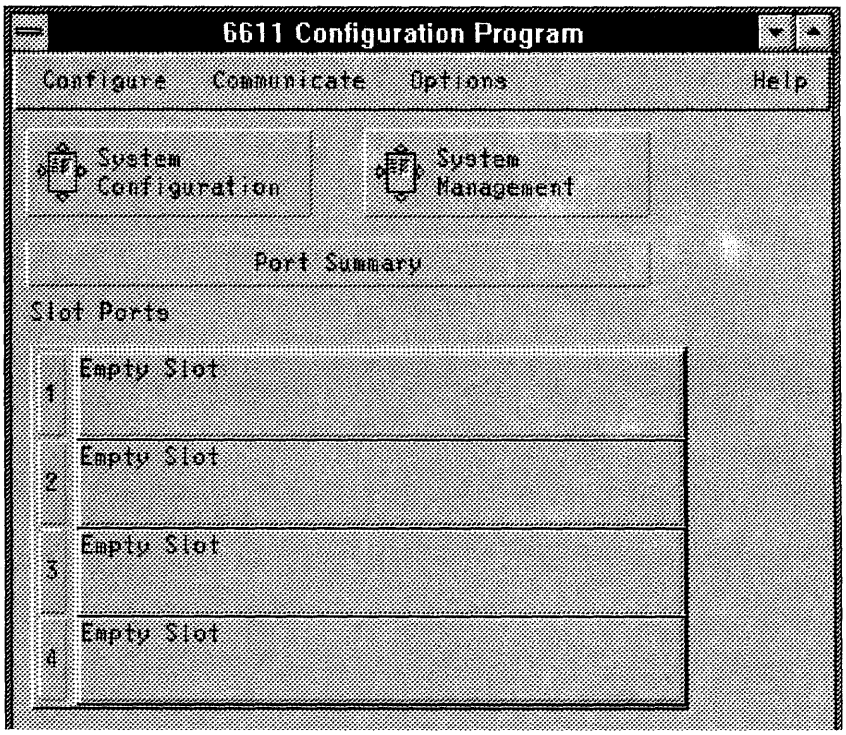


Figure 30. Startup Menu of the Configuration Program

3.2.1 Configure

Selecting **Configure** will start the Configuration Program with the following options:

New Configuration

This entry starts the new configuration session and gives the option of configuring a 6611 Network Processor Model 140 or a Model 170. There is an option in the **Options** pull-down menu that defines the default startup as a Model 140 or a Model 170.

Open Configuration

This entry will come back with a menu that lets you select an entry from the configurations stored on your system. Selection is possible per IP address and per 6611 Network Processor model. See Figure 31. The IP address entry enables you to get to configurations for a router with that IP address.

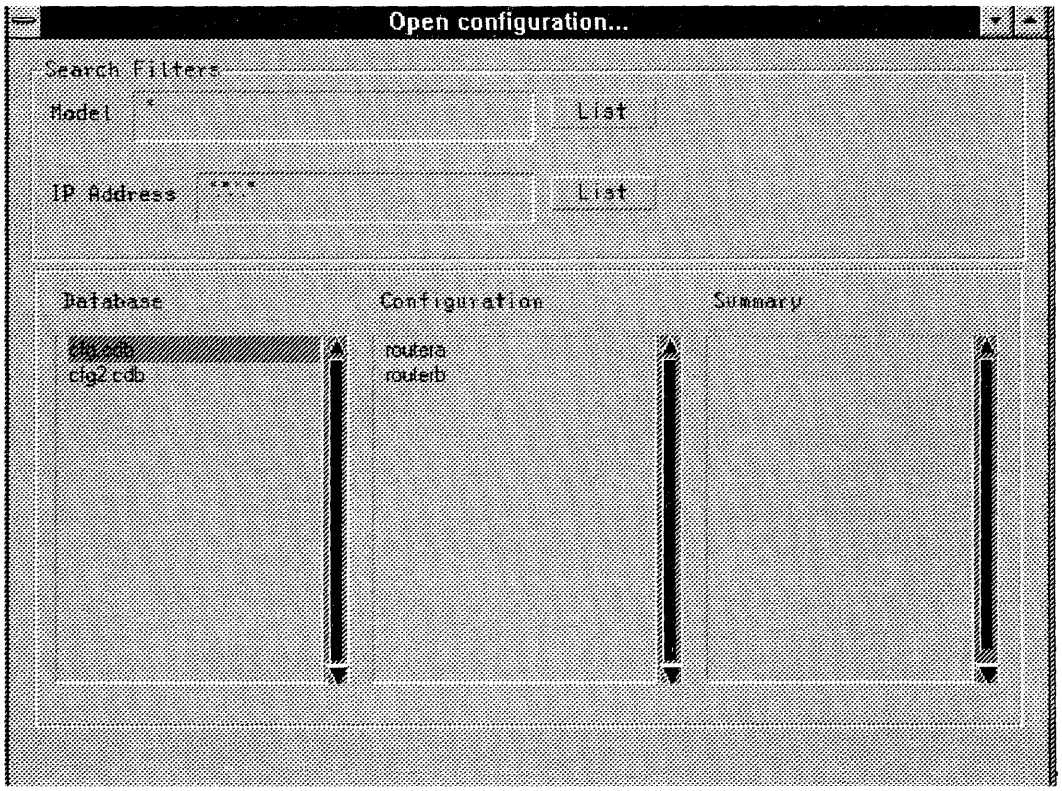


Figure 31. Open Configuration Menu

Save Configuration

This entry lets you save the configuration on your system. It returns a menu that allows you to name the new configuration and save it in a choice of databases. See Figure 32 on page 60.

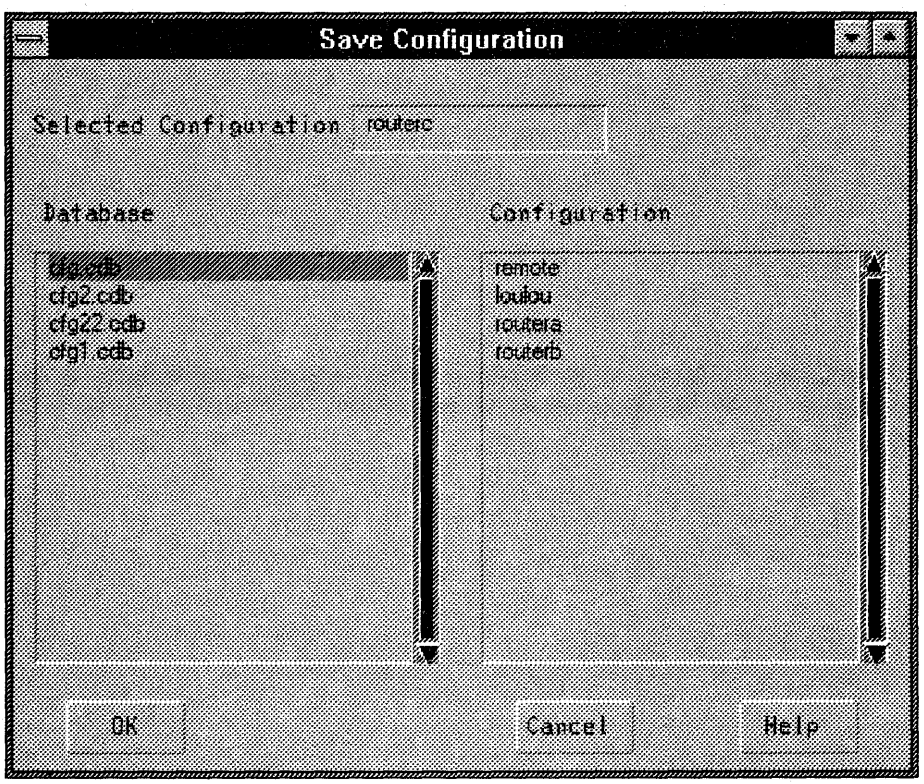


Figure 32. Saving a Configuration

Delete Configuration

This entry enables you to highlight existing configurations and delete them. It returns the same menu as the save *Open Configuration* option.

Write IML File to File

This entry lets you write the configuration file to a file. This file can then be sent to your 6611 Network Processor via FTP. It is this option that needs to be chosen to send an IML file to the 6611 from a PS/2 using TCP/IP. Remember that the Configuration Program running on a PS/2 does not allow you to send the IML file via an IP link to the 6611 using the Communicate menu. See also 3.2.2, "Communicate" on page 61.

Create Configuration Diskette

Use this option to create a configuration diskette to be loaded on the 6611. This diskette will then be loaded into the 6611 and activated via an IPL or via the Systems Manager. See Figure 29 on page 57.

Read Configuration Diskette

Reads a configuration diskette.

Copy from Another Configuration Database

This entry lets you copy a configuration from one database into another configuration database and rename it. For example in Figure 33 on page 61: configuration called *routera* on database *cfg* is copied into *routery* on database *cfg2*.

Exit

Terminates the Configure option.

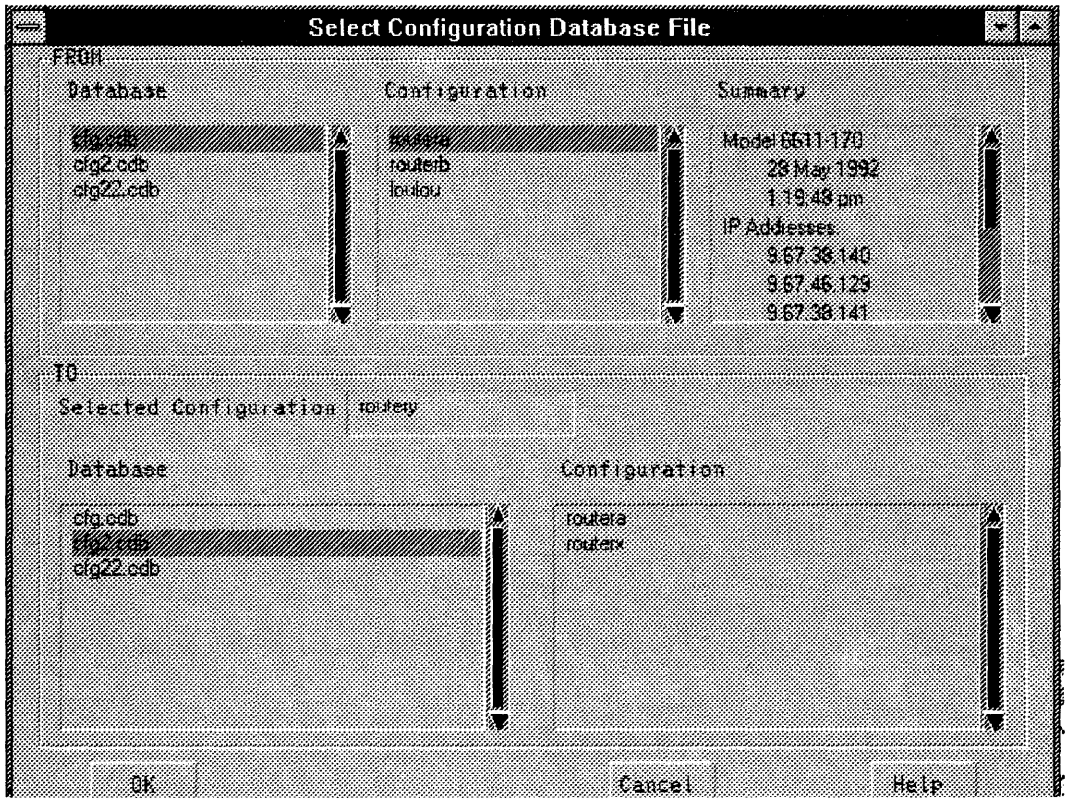


Figure 33. Example of a Configuration Copy

3.2.2 Communicate

Selecting the **Communicate** pull-down menu will start the options available on an IBM RISC System/6000 to send and retrieve configuration files from the 6611. This option is only active on the IBM RISC System/6000 because the Configuration Program uses a TCP/IP *Socket-to-Socket* protocol to transfer the configuration to the 6611. This protocol is supported by the TCP/IP code that runs in the IBM RISC System/6000 but not on TCP/IP for DOS. The **communicate** pull-down menu can be accessed on the IBM RISC System/6000 from a workstation running TCP/IP for OS/2 and using the TELNET function.

The communicate option can only access a 6611 Network Processor after it was initially configured with a configuration diskette.

The options available with **Communicate** are:

Retrieve adapter information...
This entry will connect to the designated router via its IP address and read the configuration file for its adapter information. It will display the configuration of the **Slot Ports**.

Send configuration...
This entry sends an entire configuration file. The configuration file being sent is the one presently active.

Retrieve configuration...
Will retrieve the configuration file from the 6611 Network Processor you are connecting to and place it online.

Retrieve configuration status...
Request the status of the configuration on the 6611 Network Processor.

Delete Configuration from router...
Delete a configuration from the router.

Retrieve log from router...
Gives a chronological overview of the different configurations the 6611 Network Processor has been through, and how they were implemented, for instance, via diskette or IMPORTED.

3.2.3 Port Summary

The **Port Summary** window gives an overview of the defined ports and the protocols that are routed and discarded, and whether source route bridging is active. See Figure 34. It also gives an overview of the protocol filtering based on the communication interface as described in 2.2.1.3, "Filtering" on page 28.

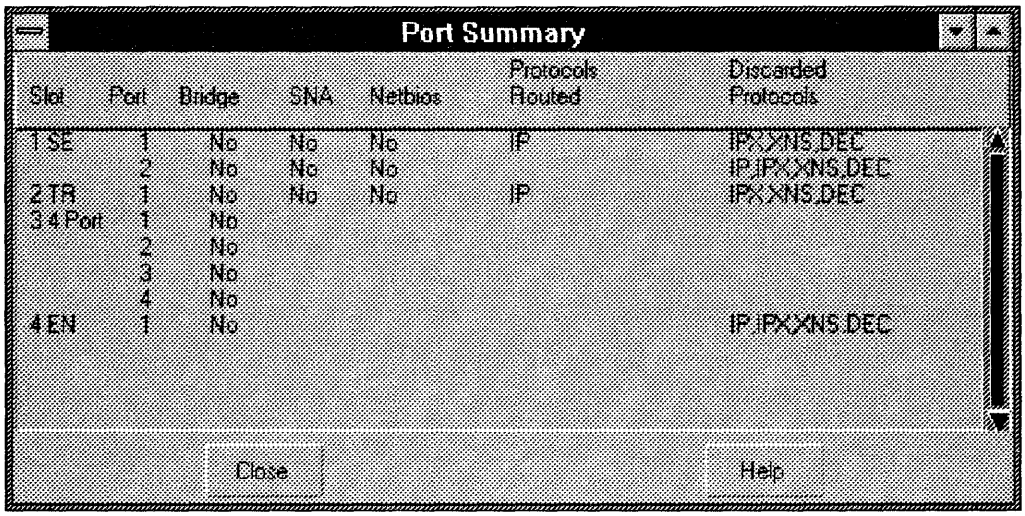


Figure 34. Ports Summary Screen

3.2.4 System Configuration and System Management

Underneath the menu bar, two push buttons are selectable:

1. System Configuration
2. System Management

3.2.4.1 System Configuration

Clicking on this box opens the screen that allows you to configure the system-wide routing parameters of the IBM 6611 Network Processor. It is here that the system-wide routing versus bridging of protocols is defined. Routing of protocols supersedes the bridging, or protocols that are not defined here to be routed will be bridged if *Source Route Bridging* is enabled. Otherwise the protocol suite will be discarded on the interface. In 2.2.1.3, "Filtering" on page 28 this is mentioned as filtering based on protocol suite.

Once the system-wide and adapter configurations are finished it is up to the application in the workstation to define if a protocol suite is bridged or routed.

Remember that routers only look at frames addressed directly to them, while source route bridges look at everything and decides whether to bridge or not based on the presence of a Routing Information (RI) field. As a function of the IBM Token-Ring Network adapter, if a frame contains a Routing Information field, the high-order bit of the first byte of the Source Address field will be turned-on.

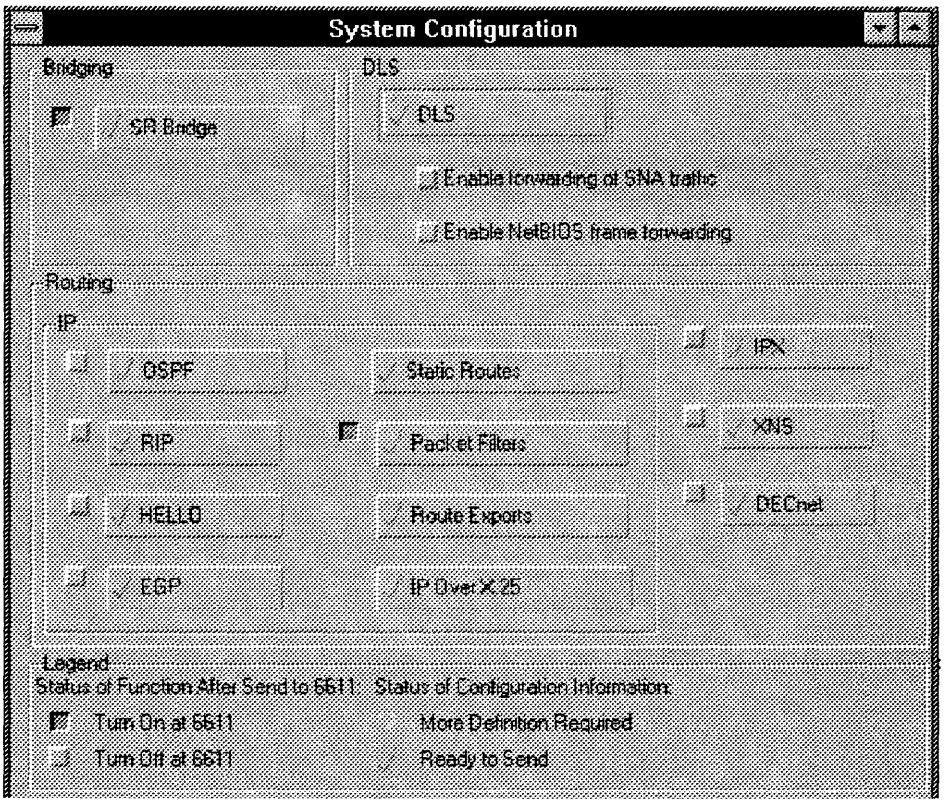


Figure 35. System Configuration Screen

The table below gives an overview of routing versus bridging.

Table 7. Overview of Routing versus Bridging

Port parameter ↓ System-wide parameter →	**Protocol Enabled**	**Protocol Not Enabled**
Protocol Enabled	Protocol is routed	Protocol not routed **1**
Protocol not Enabled	Protocol not routed **1**	Protocol not routed **1**

Note: **1** Bridging will take place if three conditions are met:

1. The frame has a Routing Information (RI) field
2. Source bridging is active system-wide
3. Source route bridging is active on the port

3.2.4.2 System Management

Clicking on this box opens the screen that allows you to define the system management options. See also 4.1, "System Manager" on page 91.

There are several options here:

SNMP

Defines the system as an SNMP agent by its contact person, system name, the SNMP traps, and others variables. In the SNMP world these translate into the MIB variables of *sysContact*, *sysName*, *sysLocation* and others. These MIB variables are described in 4.2.1.1, "Management Information Base" on page 115.

Users of System Manager

Defines the Controlling and Viewing users of the System Manager and their passwords. Controlling users can access all functions of the System Manager. Viewing users can only access a subset of the System Manager functions which are non-intrusive.

Configuration Hosts

Defines the hosts that can perform configurations on this 6611 over a TCP/IP link. The hosts are defined by their IP address. The options are either all hosts or the list given here. By default, all hosts can perform configuration. A *Host* in the TCP/IP world is any computer that is known by its IP address. Hosts can be normal processors, such as any PS/2 running TCP/IP for DOS or OS/2, or any router.

Time to Perform Configuration

Defines the time the received configuration file should be made active. This could be either immediately, at next IML or at a given time.

Remote Hosts

Defines the list of host names with their matching IP addresses. This table is used to manage remote hosts and addresses them by their name rather than by their IP address.

Name Servers

Gives the IP addresses of the *Name servers*. If the Internet uses Names for hosts rather than their IP address, the resolution is done by name servers. These can be located anywhere in the Internet. The entries here give the IP addresses of these *Name Servers*. If the system manager wishes to manage a remote host and access it by its name it would first look in the *Remote Hosts* table; if it cannot find the corresponding IP address in there it would then access the *Name Server* for identification.

Time Servers

Gives the IP address of remote *Time Servers*. The remote timer service allows the 6611 Network Processor to get its time from a remote IP node on the network.

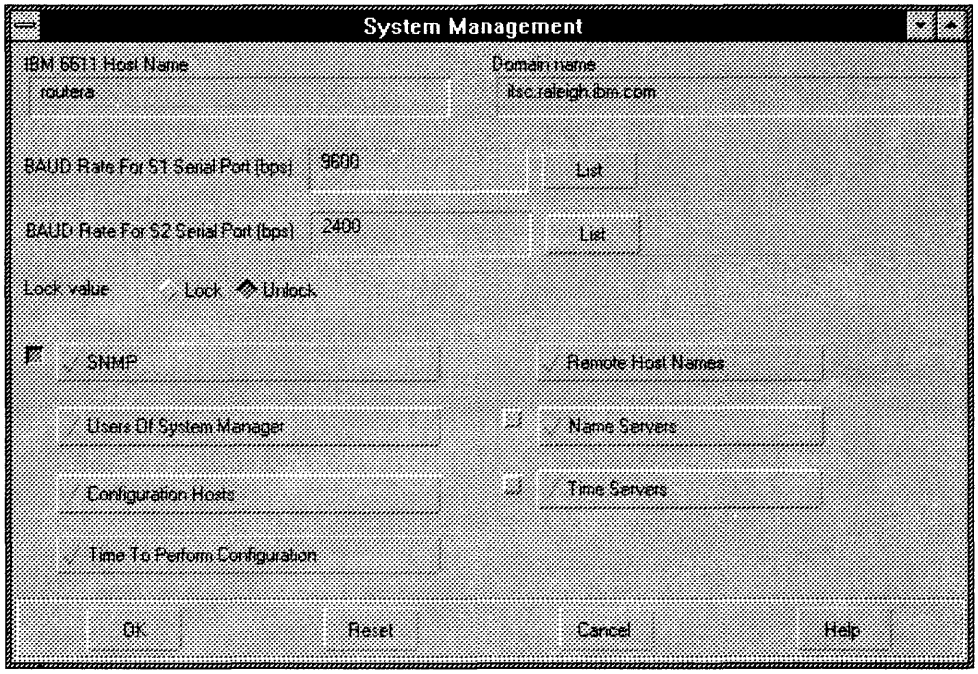


Figure 36. System Management Screen

3.2.5 Protocol Suite Configuration

As seen in Figure 30 on page 58 the Configuration Program has a three-fold logical structure:

1. System-wide protocol configuration given via System Configuration
2. System Management
3. Adapter protocol configuration via Slot Ports 1 through 4 or 1 through 7

Figure 35 on page 63 shows what protocols can be routed on a system-wide basis and if *Source Route Bridging* is activated on the 6611 Network Processor. It also defines SNA and NetBIOS via *Data Link Switching*.

Each protocol needs to be activated on a port basis for those ports where that protocol needs to be routed.

The structure is shown in Table 8 on page 66.

Table 8. Structure of the Configuration Program								
	System Wide	**Token-Ring Adapter**	**Ethernet Adapter**	**2-port Serial Adapter**			**4-port SDLC Adapter** 1	**X.25 port Adapter** 2
				TR Bridge	PPP	Frame Relay		
SR Bridge	X	X		X	X	X		
SR Bridge Filters		X		X	X	X		
IP	X	X	X		X	X		X
IPX	X	X	X		X	X		
XNS	X	X	X		X	X		
DECnet	X	X	X		X	X		
DLS	X							
SNA		X		X	X	X	X	
NetBIOS		X		X	X	X		

As can be seen from this table IP can be activated system-wide but also on the port, and this is valid for many protocols. When a protocol is enabled to be *routed* on a system-wide basis all the relevant parameters that come with that protocol need to be set in the underlying menus.

The 2-port serial card can either be enabled to support the LAN Bridge protocol, PPP or Frame Relay.

Note: 1 The 6611 4-Port SDLC Adapter can only be used for SDLC connections. Its only configuration options are:

- The Physical Interface defining the connection as EIA232D, V.35 or X.21.
- The SNA stations that connect over the SDLC line. SNA stations are defined by their polling address, for example, C1.

Note: 2 The 6611 X.25 Adapter only supports the TCP/IP protocol.

For information on the *concurrent use of functions* on the adapter cards see 2.2.4, "Concurrent Use of Functions" on page 50.

3.3 The Underlying Panels

Each entry in the *System Configuration* panel in Figure 30 on page 58 has many underlying panels that enable the full configuration of the protocol, for example XNS, or how *Source Route Bridge* will operate.

The following section, 3.4, "How to Configure for Bridging, Routing and DLS" on page 70 will explain the details of configuration, while Chapter 5, "Basic TCP/IP Example Scenario" on page 145 gives a walk-through of the configuration for several easy and several complex scenarios.

3.3.1 System Configuration Structure

The description below gives the full structure of the System Configuration Panels.

Source Route Bridge

- Enable Source Route Bridging
- Bridge Number
- Designated Ring Number
- Spanning Tree Parameters

IP

- IP Static Routes
- IP Packet Filters
  - Enable IP Filters
  - List of IP Packet Filters
- Route Exports
  - List of Exports
- IP over X.25
  - Connection Decay Interval
- RIP
  - Enable RIP
  - Source Routers
  - Trusted Routers
  - RIP Interface Setting
  - Imports
- HELLO
  - Enable HELLO
  - Broadcast
  - Source Routers
  - Trusted Routers
  - HELLO Interface Settings
  - Imports
- OSPF
  - Enable OSPF
  - Router ID
  - OSPF Areas
  - OSPF Interfaces
  - OSPF Neighbors
  - OSPF Network Ranges
  - OSPF Virtual Links
- EGP
  - Enable EGP
  - Local Autonomous System Number
  - Maximum Initial Packet Size
  - Preference
  - Generate Default Route
  - Default Metric
  - EGP Groups
  - EGP Neighbors
  - EGP Group Options
  - EGP Imports
  - EGP Import Destinations

IPX

- Enable IPX Router
- Split Horizon for RIP Filters - On/Poison Reverse/Off

- SAP Filters
  - Enable SAP Filters
  - List of SAP Filters
- RIP Router Filters
  - Enable RIP Router Filters
  - Filtering Mode - Deny/Permit
  - List of RIP Router Filters
- Inbound RIP Filters
  - Enable Inbound RIP Filters
  - Filtering Mode - Deny/Permit
  - List of Inbound IPXRIP Filters
- Outbound RIP Filters
  - Enable Outbound RIP Filters
  - Filtering Mode - Deny/Permit
  - List of Outbound IPXRIP Filters

XNS

- Enable XNS Router
- Split Horizon - On/Poison Reverse/Off
- RIP Router Filters
  - Enable RIP Router Filters
  - Filtering Mode - Deny/Permit
  - List of RIP Router Filters
- Inbound RIP Filters
  - Enable Inbound RIP Filters
  - Filtering Mode - Deny/Permit
  - List of Inbound RIP Filters
- Outbound RIP Filters
  - Enable Outbound RIP Filters
  - Filtering Mode - Deny/Permit
  - List of Outbound RIP Filters

DECnet

- Enable DECnet Routes
- Local DECnet Address
- Node Type Routing IV/Area
- DECnet Filters
  - List of Packet Filters
- DECnet Operational Parameters

DLS

- Enable Forwarding of SNA Traffic
- Enable NetBIOS Frame Forwarding
- DLS Specific Parameters
  - Virtual Ring Segment Number
  - Destination Cache Timeout
  - Default DLS IP Address for This 6611
  - Participating DLS Routers
- SNA
  - IP Address of Destination Router
  - Destination MAC Address
  - SNA Source Frame Filters
    - Enable Source Frame Filters
    - Source Frame Filter Type - Deny/Permit
    - List of SNA Source Frame Filters
  - SNA Destination Frame Filters
    - Enable Destination Frame Filters
    - Destination Frame Filter Type -Deny/Permit

        - List of SNA Source Frame Filters
- NetBIOS
  - Destination Name
  - IP Address of Destination Router
  - NetBIOS Source Name Filters
    - Enable Source Name Filters
    - Source Name Filter Type - Deny/Permit
    - List of NetBIOS Source Name Filters
  - NetBIOS Destination Name Filters
    - Enable Destination Name Filters
    - Destination Name Filter Type -Deny/Permit
    - List of NetBIOS Source Name Filters

3.3.2 Adapter Configuration Structure

The IBM 6611 Network Processor supports the following adapters:

- 6611 Token-Ring Network 16/4 Adapter
- 6611 Ethernet Adapter
- 6611 2-Port Serial Adapter
- 6611 4-Port SDLC Adapter
- 6611 X.25 Adapter

6611 Token-Ring Network 16/4 Adapter with the following configuration options:

- Physical Interface
- SR Bridge
- SR Bridge Filters
- IP
- IPX
- XNS
- DECnet
- SNA
- NetBIOS

6611 Ethernet Adapter with the following configuration options:

- Physical Interface
- IP
- IPX
- XNS
- DECnet

6611 2-Port Serial Adapter with a 3-fold configuration option:

- LAN Bridge Protocol
  - Physical Interface
  - LAN Bridge Port Defaults
  - SR Bridge
  - SR Bridge Filters
  - 1 SNA
  - 1 NetBIOS
- PPP
  - Physical Interface
  - PPP
  - SR Bridge

  - SR Bridge Filters
  - IP
  - IPX
  - XNS
  - DECnet
  - [1] SNA
  - [1] NetBIOS
- Frame Relay
  - Physical Interface
  - Frame Relay
  - SR Bridge
  - SR Bridge Filters
  - IP
  - IPX
  - XNS
  - DECnet
  - [1] SNA
  - [1] NetBIOS

6611 4-Port SDLC Adapter with the following configuration options:

- EIA232D
  - Physical Interface
  - SNA Stations
- V.35
  - Physical Interface
  - SNA Stations
- X.21
  - Physical Interface
  - SNA Stations

6611 X.25 Adapter with the following configuration options:

- Enable X.25
- Subscription
- IP
- Network Tuning
- IP/X.25 Mapping

Note: [1] The definition of SNA and NetBIOS parameters on the 6611 2-Port Serial Adapter is only active when source route bridging is also activated. This is the condition to have DLS active over the link.

3.4 How to Configure for Bridging, Routing and DLS

This section will explore the procedure of how to configure your IBM 6611 Network Processor to perform the bridging, routing and DLS functions available to it. Refer also to Table 8 on page 66.

3.4.1 How to Configure Bridging

The IBM 6611 Network Processor only does *source route bridging*; there are three options:

- Local bridging between several rings connected to one 6611 Network Processor
- Remote bridging between two 6611 Network Processors

- Remote bridging as one half of an IBM source routing remote bridge

Remote bridging between two 6611 Network Processors can be either over a PPP link or over frame relay. The table below gives an overview of the options that need to be chosen. All three types can be chosen the same 6611.

Table 9. Configuration for Bridging

	System Wide	Token-Ring Adapter	2-port Serial Adapter		
			LAN Bridge	PPP	Frame Relay
Local Bridge	X	X			
Point-to-Point using PPP	X	X		X	
Point-to-Point using Frame Relay	X	X			X
Half of Remote Bridge	X	X	X		

3.4.1.1 Local Bridge Configuration

System-wide parameters are:

Bridge Number
This is the bridge number given to the 6611 Network Processor in all three source route bridging cases.

Designated Ring Number
This ring number must only be defined in the case of source route bridging to a remote half of the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R). This entry is not required here, however the configuration program requires an entry. Choose one of the existing ring segment numbers.

See Figure 37 on page 72.

Port-type parameters are:

Ring Number
Defined on the token-ring adapter this parameter defines the *segment number* per attached ring in case of local bridging.

Bridge Filter
A multitude of filters are possible based on hop count, MAC address, SNAP Ethertype field, SAP or ring number. Filters can act on inbound and outbound frames.

Hop Count Frames that have more than the number of hops defined here in their RIF will be discarded. The frame can be either a Single-Route Broadcast (SRB), All-Routes Broadcast (ARB) or both SRB and ARB.

MAC Address Filters based on the MAC address will permit/deny frames from a source MAC address to flow to a destination MAC address. Unlike the routing filter this is a dual filter meaning a source/destination pair needs to be defined. The inbound filter defines

incoming source/destination pairs, the outbound filter defines outgoing source/destination pairs. The frame can be either a Single-Route Broadcast (SRB), All-Routes Broadcast (ARB) or both SRB and ARB.

SAP Address This type of filter will deny/permit frames with a given SAP value flowing in (in case of inbound filter) or out (in case of the outbound filter) from being received. Again the frame can be either SRB, ARB or both.

SNAP Value This type of filter will deny/permit frames with a SNAP (Sub-Network Access Protocol) header from entering (in case of an inbound filter) or leaving (in case of an outbound filter). SNAP headers appear in frames that have source and destination SAPs of X'AA'. Note however that for the SNAP filter to be active, the SAP filtering must be enabled.

Ring Number Inbound or outbound frames with a ring number that is part of those given in the filter will be either permitted or denied from entering or leaving the bridge. Again frames can be either SRB, ARB or both.

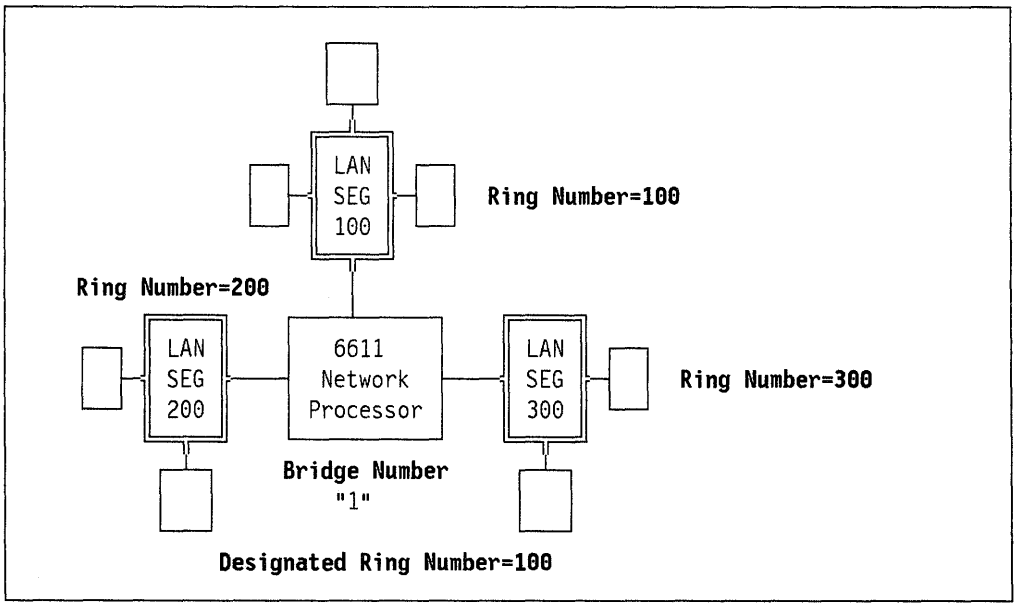


Figure 37. Local Bridge Configuration

On the 6611 Token-Ring Network 16/4 Adapter ports: enable source route bridging, define the physical interface with broadcast type set to **Non-Local**, and set the ring number to that of the attached segment.

3.4.1.2 Remote Bridging - between 6611 Network Processors

The point-to-point bridge runs over the 6611 2-Port Serial Adapter card and uses either PPP or Frame-Relay.

See Figure 38 on page 73

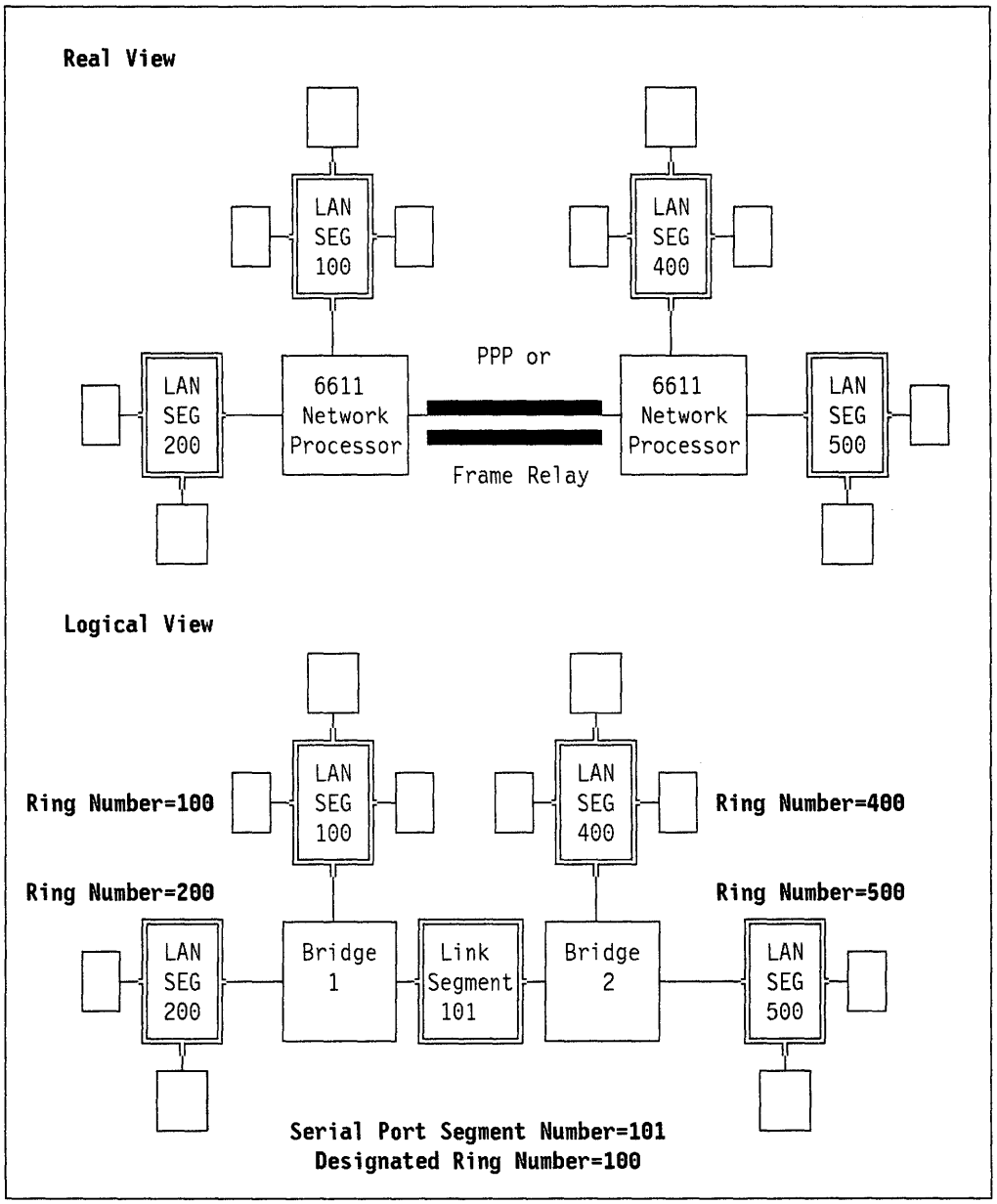


Figure 38. Remote Bridge between 6611s Configuration

System-wide parameters are:

Bridge Number
This is the bridge number given to the 6611 Network Processor in all three source route bridging cases.

Designated Ring Number
This ring number must only be defined in the case of source route bridging to a remote half of the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R). This entry is not required here, however the configuration program requires an entry. Choose one of the existing ring segment numbers.

Port-type parameters are:

Ring Number

Defined on the token-ring adapter this parameter defines the *segment number* per attached ring. Defined on the 6611 2-Port Serial Adapter this parameter defines the single **link-segment** in case of PPP or multiple **link segments**, each with their corresponding DLCI number in the case of frame relay.

Bridge Filter

A multitude of filters are possible based on hop count, MAC address, SNAP Ethertype field, SAP and ring number.

Hop Count Frames that have more than the number of hops defined here in their RIF will be discarded. The frame can be either a Single-Route Broadcast (SRB), All-Routes Broadcast (ARB) or both SRB and ARB.

MAC Address Filters based on the MAC address will permit/deny frames from a source MAC address to flow to a destination MAC address. Unlike the routing filter this is a dual filter meaning a source/destination pair needs to be defined. The inbound filter defines incoming source/destination pairs, the outbound filter defines outgoing source/destination pairs. The frame can be either a Single-Route Broadcast (SRB), All-Routes Broadcast (ARB) or both SRB and ARB.

SAP Address This type of filter will deny/permit frames with a given SAP value flowing in (in case of inbound filter) or out (in case of the outbound filter) from being received. Again the frame can be either SRB, ARB or both.

SNAP Value This type of filter will deny/permit frames with a SNAP (Sub-Network Access Protocol) header from entering (in case of an inbound filter) or leaving (in case of an outbound filter). SNAP headers appear in frames that have source and destination SAPs of X'AA'. Note however that for the SNAP filter to be active, the SAP filter must be enabled.

Ring Number Inbound or outbound frames with a ring number that is part of those given in the filter will be either permitted or denied from entering or leaving the bridge. Again frames can be either SRB, ARB or both.

3.4.1.3 Remote Bridging to a PS/2

The 6611 Network Processor has the capability of compatibility with the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) running in a PS/2.

Note

The bridge program requires PTF UR37051.

The 6611 must always be **Primary**.

See Figure 39 on page 75.

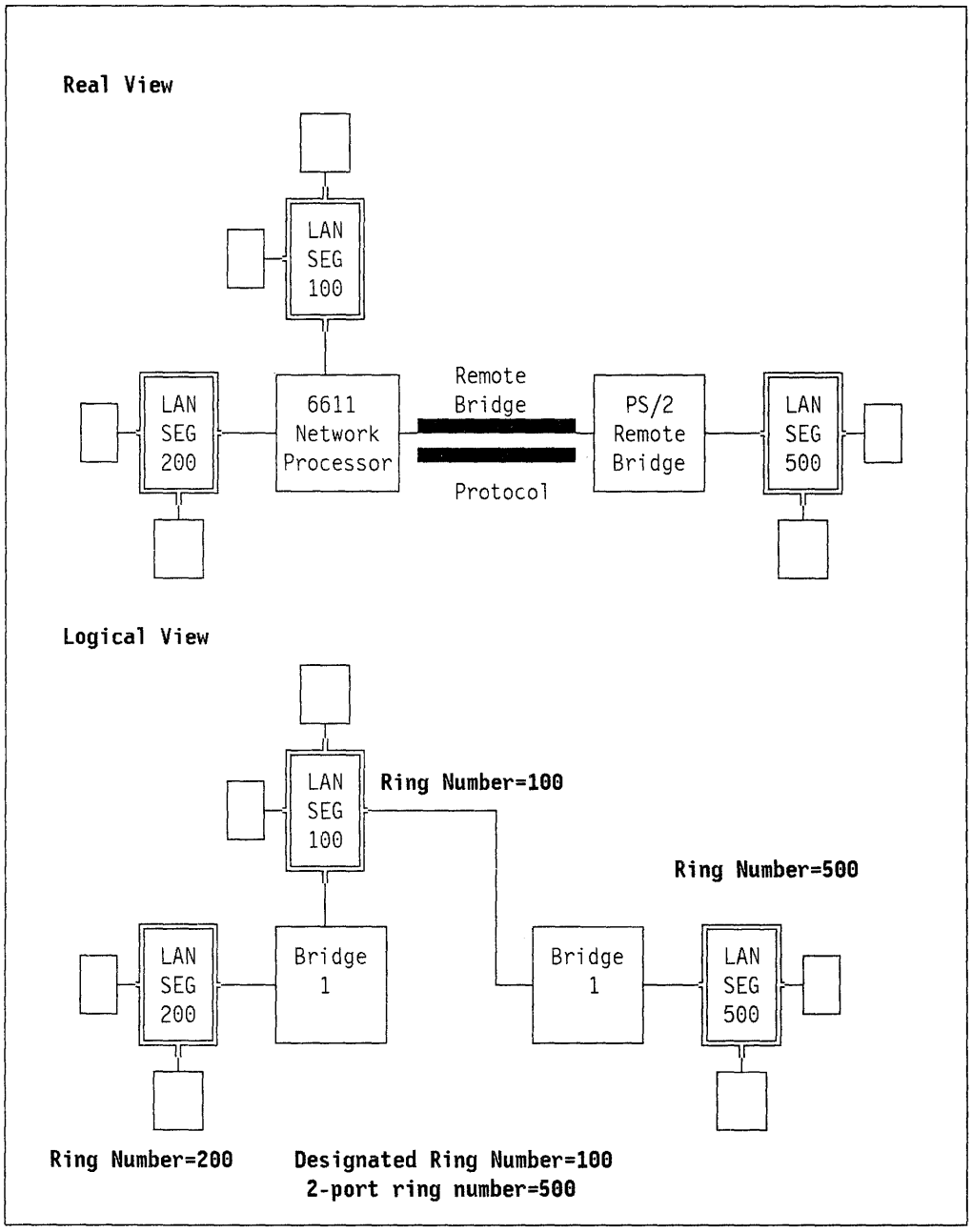


Figure 39. Remote Bridge Compatibility with a PS/2 Bridge

System-wide parameters are:

Bridge Number
This is the bridge number given to the 6611 Network Processor in all three source route bridging cases. Although the bridge numbers are shown to be the same here, they may in fact be different per 6611 Network Processor.

Designated Ring Number
This ring number needs to be defined here. This ring number must be the same as one of the token-ring segments locally attached to the 6611 Network Processor, for example, 100.

Port-type parameters are:

Ring Number

The *ring number* on the 6611 2-Port Serial Adapter defines the remote segment number. In Figure 39 on page 75 this is the 2-port serial ring number.

Choose LAN Bridging Protocol on the 6611 2-Port Serial Adapter card; this will emulate the primary bridge of a remote bridge protocol. Figure 40 on page 77 shows the screen. Notice that SNA and NetBIOS can be chosen. This will be explained in 3.4.3.3, "SNA and NetBIOS over Bridged Links" on page 88. The protocol is defined here as: **PS/2 LAN Bridge Point-to-Point** or **LAN Bridge PPP**. Do not be confused with PPP as defined for the TCP/IP protocol suite.

Bridge Filter

A multitude of filters are possible based on hop count, MAC address, SNAP Ethertype field, SAP and ring number.

Hop Count Frames that have more than the number of hops defined here in their RIF will be discarded. The frame can be either a Single-Route Broadcast (SRB), All-Routes Broadcast (ARB) or both SRB and ARB.

MAC Address Filters based on the MAC address will permit/deny frames from a source MAC address to flow to a destination MAC address. Unlike the routing filter this is a dual filter meaning a source/destination pair needs to be defined. The inbound filter defines incoming source/destination pairs, the outbound filter defines outgoing source/destination pairs. The frame can be either a Single-Route Broadcast (SRB), All-Routes Broadcast (ARB) or both SRB and ARB.

SAP Address This type of filter will deny/permit frames with a given SAP value flowing in (in case of inbound filter) or out (in case of the outbound filter) from being received. Again the frame can be either SRB, ARB or both.

SNAP Value This type of filter will deny/permit frames with a SNAP (Sub-Network Access Protocol) header from entering (in case of an inbound filter) or leaving (in case of an outbound filter). SNAP headers appear in frames that have source and destination SAPs of X'AA'. Note however that for the SNAP filter to be active, the SAP filter must be enabled.

Ring Number Inbound or outbound frames with a ring number that is part of those given in the filter will be either permitted or denied from entering or leaving the bridge. Again frames can be either SRB, ARB or both.

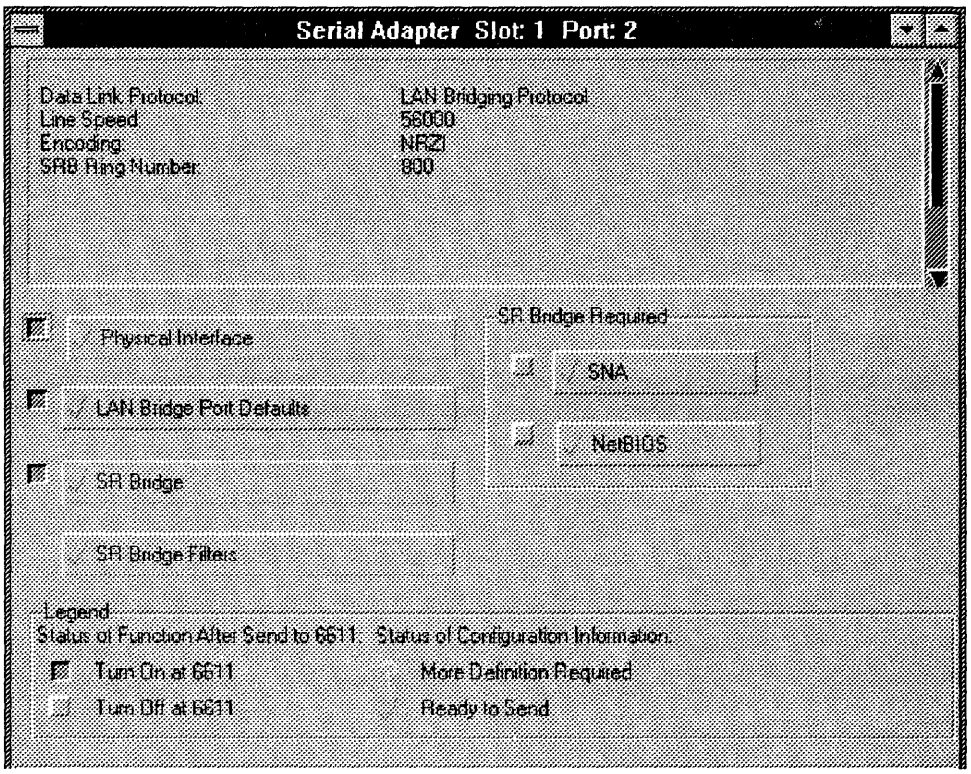


Figure 40. Serial Adapter Definition for Remote Bridge to a PS/2

See Figure 41 on page 78 and Figure 42 on page 78 for an overview of the bridge parameters. Note that due to programming internals the default password of eight "0's" must be entered manually. All these parameters make up the ECCPARMS.BIN file in the primary bridge, with the exception of frame forwarding which is always active by default.

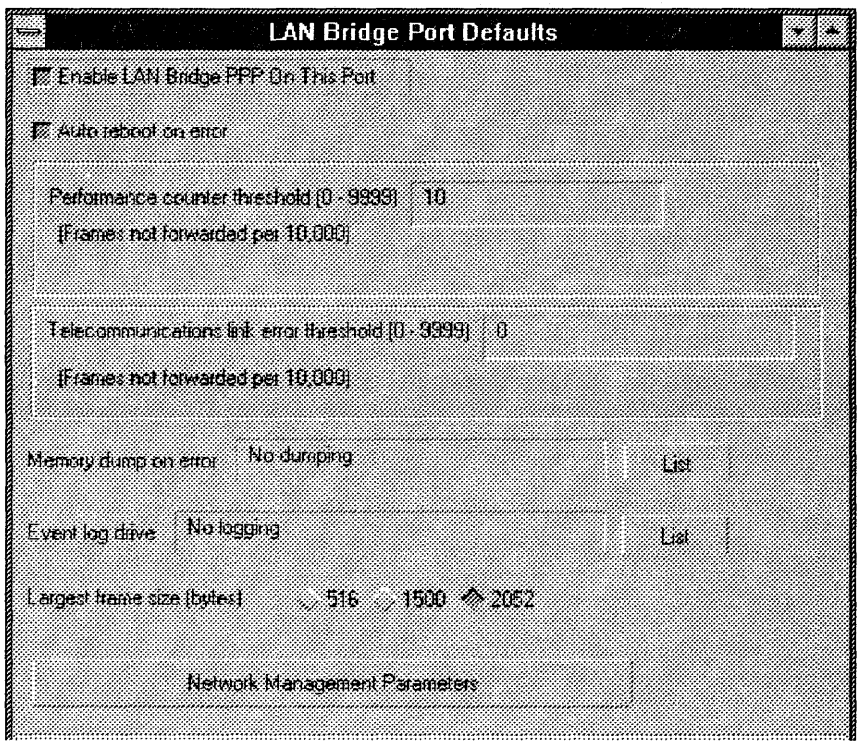


Figure 41. LAN Bridge Compatibility Serial Port Definitions

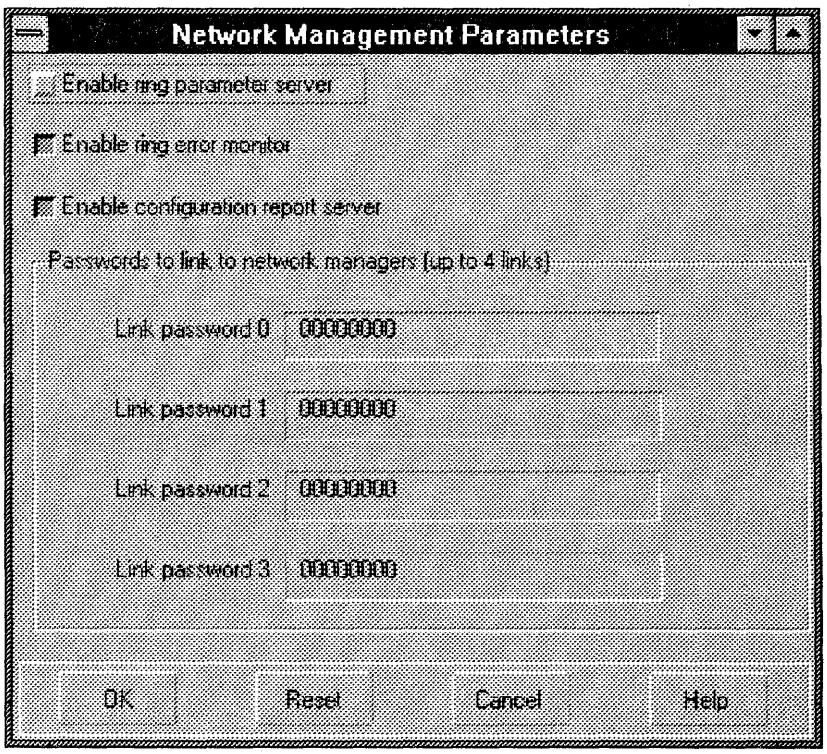


Figure 42. LAN Bridge Network Management Parameters

3.4.2 How to Configure Routing

Remember that routers only look at frames addressed to them directly, whereas bridges look at everything and will act on the RIF field in the case of source route bridging.

Configuring for routing requires:

1. Defining the protocol system-wide. This is done at system configuration time
2. Defining the protocol on the incoming adapter
3. Defining the protocol on the outgoing adapter

The 6611 Network Processor has protocol stacks and routing tables for every protocol suite it routes. Each protocol suite has its appropriate routing table maintenance protocol. For example, when receiving IPX packets, the 6611 Network Processor will route them based on the IPX routing tables. The routing table maintenance protocol used by IPX and XNS is RIP, DECnet uses a proprietary routing scheme. IP has many routing table maintenance protocols: RIP, Hello, EGP, BGP, OSPF.

Note: The basis for RIP is the routing algorithms used in ARPANET, which have been available since 1969. This evolved into the RIP as used by XNS. The "routed" version of RIP is largely the same but it has a more general address format able to handle IP and other types of addresses and with routing updates limited to every 30 seconds. So the RIP as use by XNS is different from the RIP as used by IP. The RIP for IP, as used by the 6611 Network Processor, is based on RFC1058.

Network addresses that are the basis of the routing protocol, differ from protocol suite to protocol suite.

- IP uses dotted decimal notation with a subnet mask, for example, "9.67.38.64" with subnet mask "255.255.255.129." See also Appendix A, "TCP/IP Routing Table Maintenance Protocols" on page 179 .
- IPX uses a 32-bit, hexadecimal number, followed by a 48-bit MAC address that is also in hexadecimal form. For example: X'000000d5.0013.ff00.45d3' corresponds to host X'0013.ff00.45d3' on network X'000000d5'.
- XNS network numbers are also in 32-bit, hexadecimal form. The XNS host address is a 48-bit hexadecimal number and is automatically set to the value of the MAC address on the Token-Ring or Ethernet card.
- DECnet uses the notion of *area* and nodes. Within an area node are either routers or hosts. Areas have values of 1 to 63. Nodes have 4-digit values. So "61.1002" defines host "1002" in area "61."

3.4.2.1 System-Wide Parameters for Routing

The first column in Table 8 on page 66 has entries for IP, IPX, XNS, DECnet, and DLS. Routing SNA and/or NetBIOS traffic is defined via DLS and is described in 3.4.3, "How to Configure Data Link Switching" on page 85.

IP Here the Routing Table Maintenance Protocol is defined in the case of dynamic routing, or the IP Static Routes in the case of static routing. See also Figure 35 on page 63.

- Static Routing

  This defines the static routes. Entries are made by *Adding* a *Destination Address* with subnet mask and a *Next Hop Router*.

The destination defines the destination network this router is connected to. The next hop router defines the IP address of the interface through which the next router is to be reached.

Consider Figure 43 where a host in network "9.67.38.64" needs to send something to a host in network "9.67.47.128" . Router A will be configured to route the traffic from any number of ports over the serial link a. The destination will be "9.67.38.64" and the *Next Hop Router* will be "9.67.38.140" . For an explanation of IP routing see also Appendix A, "TCP/IP Routing Table Maintenance Protocols" on page 179.

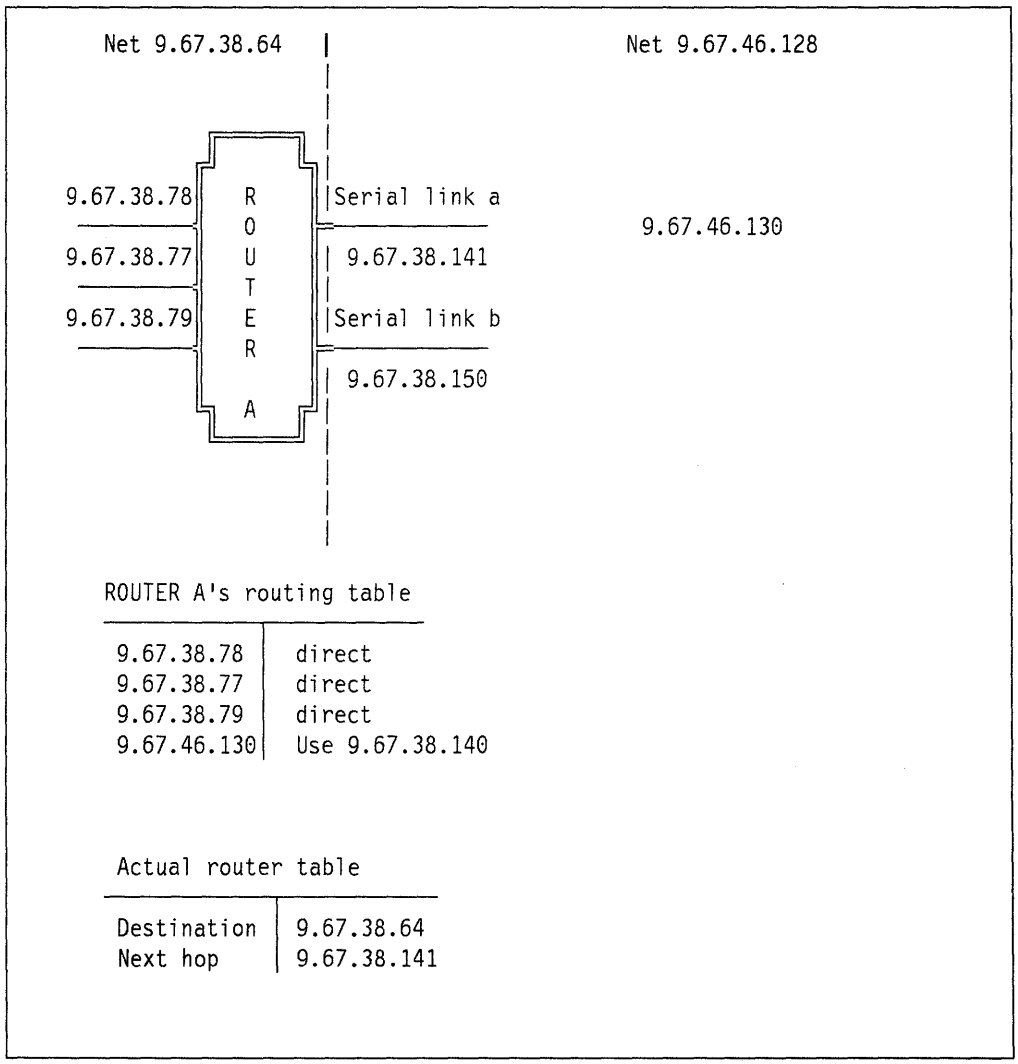


Figure 43. IP Static Routing

- IP Packet Filters

  IP filters permit or deny specific traffic from passing through the 6611 Network Processor. This is done by enabling or disabling packets from an IP address to flow through the 6611 Network Processor in case of singular mode or from flowing to another IP address in case of dual mode. For example in Figure 44 on page 81 traffic from "9.34.45.2" with subnet mask "255.255.0.0" is

denied from passing through the 6611 Network Processor to "9.45.12.34" with subnet mask "255.255.255.0." The effect of the subnet mask is that no traffic from subnet "9.34.0.0" will flow to "9.45.12.0."

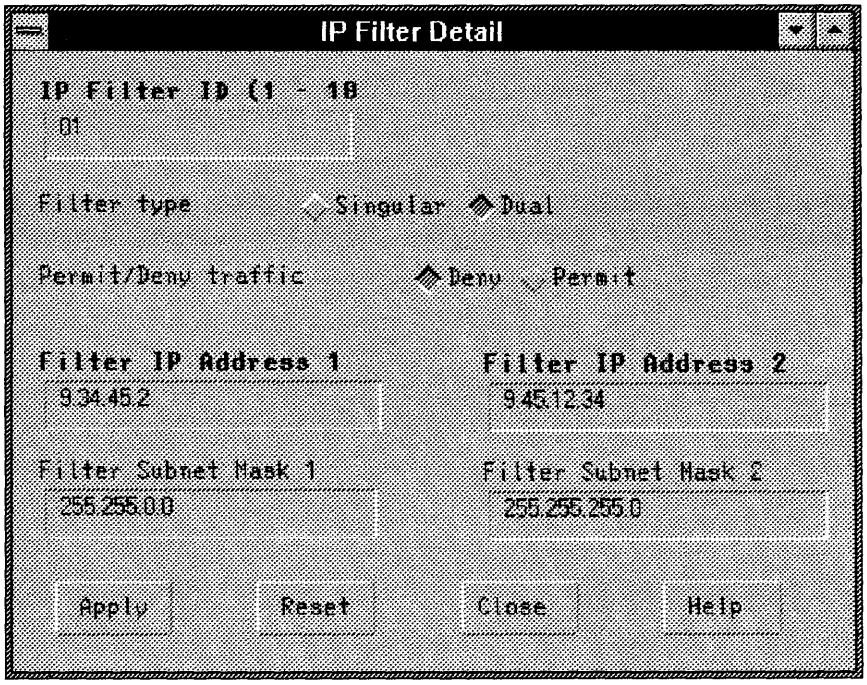


Figure 44. IP Filtering

- Router Export

  Defines the list of routes, with their metrics, that will be exported to EGP.

- IP over X.25

  Connection Decay Interval defines how long an X.25 SVC connection will be held up after the last IP session closes.

- RIP
  - *Broadcast* specifies whether this router will broadcast its routing table every 30 seconds.
  - *Zero Reserved Fields* verifies that unused fields in RIP packets are set to 0.
  - *Route Preference* specifies the preference value for this router. When multiple routes to the same destination exist, the router with the lowest preference value will be chosen.
  - *RIP Interface Settings* defines the IP address of the port over which RIP updates will be sent and/or received.
  - *Source Routers* lists the routers to which updates are to be sent in non-broadcast networks.
  - *Trusted Routers* lists the routers from which routing table updates will be applied. Routing information from other routers will be discarded.

- *Imports* defines filters on imported routing table updates for destinations as defined in List of RIP Destinations. Routing table updates can be received from all sources, from defined interfaces or from remote routers. The defined interfaces must be part of those defined in *RIP Interface Settings*.

- IP-Hello
  - *Broadcast* specifies whether this router will broadcast its routing table every 30 seconds.
  - *Zero Reserved Fields* verifies that unused fields in RIP packets are set to 0.
  - *Route Preference* specifies the preference value for this router. When multiple routes to the same destination exist, the router with the lowest reference value will be chosen.
  - *Hello Interface Settings* defines the IP address of the port over which Hello updates will be sent.
  - *Source Routers* lists the routers to which updates are to be sent when no broadcasting is defined.
  - *Trusted Routers* lists the routers from which routing information will be applied. Routing information from other routers will be discarded.
  - *Imports* defines filters on imported routing table updates for destinations as defined in List of RIP Destinations. Routing table updates can be received from all sources, from defined interfaces or from remote routers. The defined interfaces must be part of those defined in *RIP Interface Settings*.

- IP-OSPF

  Refer to *IBM Multiprotocol Network Program: User's Guide* for a detailed description of the parameters involved with OSPF.

- IP-EGP

  Refer to *IBM Multiprotocol Network Program: User's Guide* for a detailed description of the parameters involved with EGP.

Configuring these Routing Table Maintenance Protocols is no easy feat, and requires in-depth knowledge of these protocols and of TCP/IP in general. While RIP and Hello might be straightforward, designing an OSPF router into an existing network requires advanced skills.

IPX The IPX system-wide parameters are: how split horizon is set up, the RIP parameters of router filters and inbound and outbound filters, and the SAP filters.

XNS The XNS system-wide parameters are: how split horizon is set up the RIP parameters of inbound and outbound filters, and the RIP router filter.

DECnet Defines the DECnet parameters.

3.4.2.2 Port-Type Parameters for Routing

Again, referring to Table 8 on page 66, protocols need to be specified on the 6611 Token-Ring Network 16/4 Adapter, the 6611 Ethernet Adapter, the 6611 X.25 Adapter and the 6611 2-Port Serial Adapter. Figure 45 shows an example of the 2-Port Serial Adapter Configuration screen.

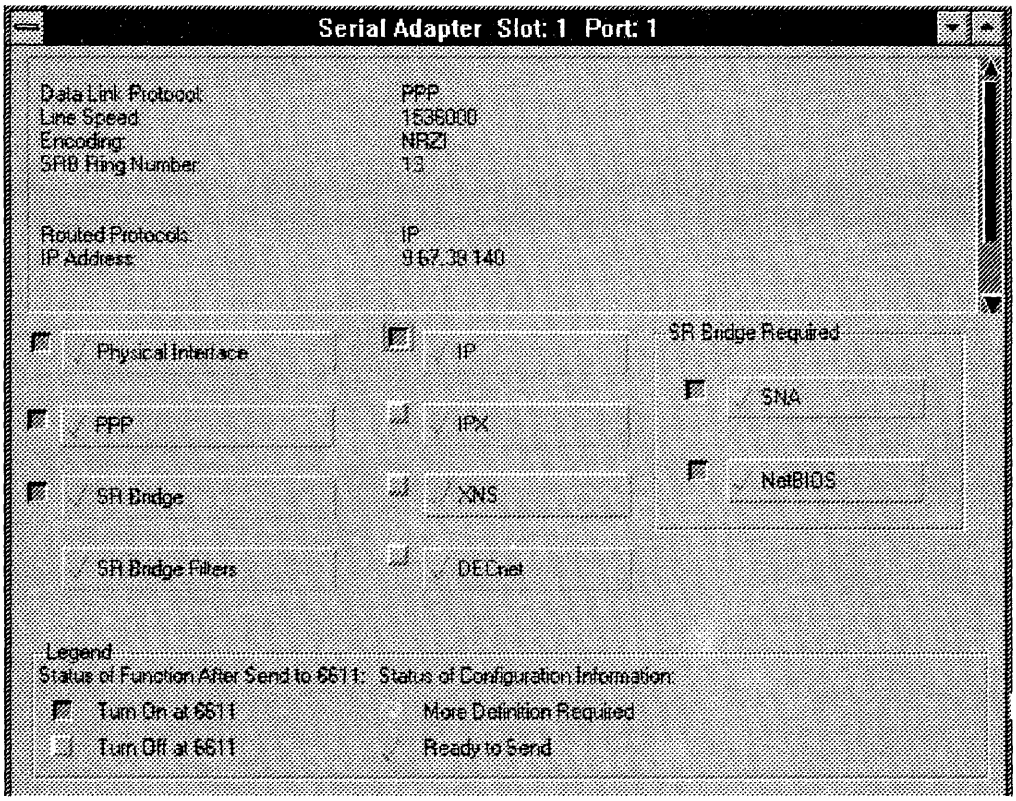


Figure 45. The 2-Port Serial Adapter Configuration Screen

IP The configuration consists of enabling IP routing on the interface, giving the correct IP address for the port with its subnet mask and the MTU or *Maximum Transmission Unit*. This is valid for token-ring, Ethernet the 2-port serial adapter and the X.25 port. The importance of MTU is reflected in the following: if datagrams with larger frame sizes than the MTU are transmitted they will be fragmented with an immediate effect on throughput and response time. Ethernet LANs have a maximum MTU of 1500 while Token-Ring LANS can go much higher. The limiting factor however is the link between the routers and their immediate effect if bridging is used. The IP specification says that routers must be able to accept datagrams of up to 576 bytes.

IPX The IPX parameters for all ports are:

- IPX network number, which is a 32-bit hexadecimal number. The IPX address is this network address followed by a 48-bit MAC address for example: X'000000d2.0010.c0d2.456f'.
- The encapsulation method. Defines the LLC encapsulation method used for the transmission of IPX packets on this port. The encapsulation depends on the media: token-ring or Ethernet. Packets can be encapsulated in Ethernet V2, in Ethernet SNAP, in Ethernet 802.3 or in Ethernet 802.2. In case of Ethernet, or, in

case of token-ring the encapsulation methods are Token-Ring 802.5 or Token-Ring SNAP.

- The checksum method - Packet/Header/Off.
- Whether software loopback is active, which enables IPX packets to be looped back at the router.
- IPX port filters.
- Destination address for PPP or destination per DLCI in case of frame relay. This defines the destination host address on the 2-port serial link. This corresponds to a static route.

XNS The XNS parameters for the ports are:

- XNS network number, which is a 32-bit hex number. The hosts in the network have 48-bit hex numbers and are equal to the MAC address.
- The encapsulation method which defines the LLC encapsulation method used for transmitting IPX packets on this port. The encapsulation depends on the media: token-ring or Ethernet. Packets can be encapsulated in Ethernet V2, in Ethernet SNAP, in Ethernet 802.3 or in Ethernet 802.2. In case of Ethernet, or, in case of token-ring the encapsulation methods are Token-Ring 802.5 or Token-Ring SNAP.
- The checksum method - Packet/Header/Off.
- Number of bytes returned in an error protocol.
- Error Protocol Active, Y/N.
- Software Loopback Active, Y/N.
- Destination address for PPP, or destinations per DLCI in case of frame relay. This defines the destination host address on the 2-port serial link. This corresponds to a static route.
- Define XNS port filters.

DECnet Defines the DECnet port parameters and the port filters including:

- Circuit cost, which defines the cost of using the circuit, and is a way of balancing traffic.
- Hello timer, which defines the interval between consecutive Hello messages.
- Router priority, where the router with the highest priority is chosen first.
- Routing timer, which defines the interval between consecutive routing table update messages.
- Maximum routers, which defines the maximum number of routers allowed on a circuit.
- Remote DECnet address using PPP or per DLCI in case of frame relay. This is the 16 bit DECnet address of the router at the other end of the serial link.
- Remote DECnet Node Type - Area, Routing IV, Endnode.
- Port filters.

3.4.3 How to Configure Data Link Switching

Note that the only parameter to configure for DLS is a *system-wide* option. The DLS function, however, requires that the source route bridging function and SNA and/or NetBIOS be specified on the port where the traffic enters. On the 6611 2-Port Serial Adapter which is the outgoing port, IP (and SNA and/or NetBIOS) must also be configured.

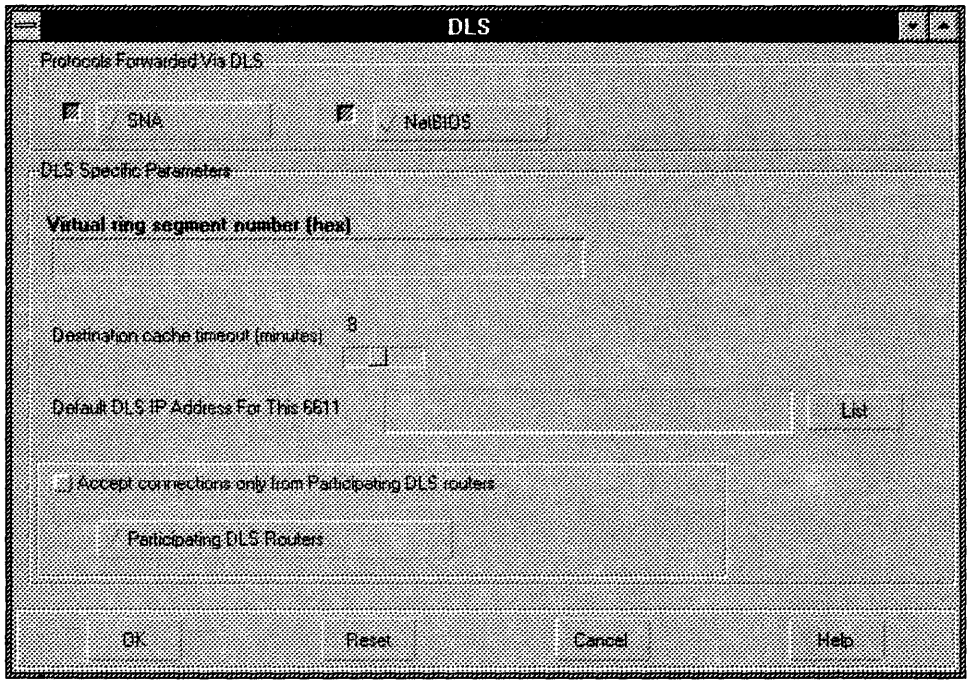


Figure 46. The DLS Configuration Panel

The configuring options are:

Enable Protocols Forwarded by DLS

Specifies SNA and/or NetBIOS to be routed by DLS.

- The SNA parameters are:
  - The IP address of the destination router
  - The MAC address of the destination

  The two entries above build the SNA Default Destination table.
  - List of SNA Source Frame Filters
  - List of SNA Destination Frame Filters

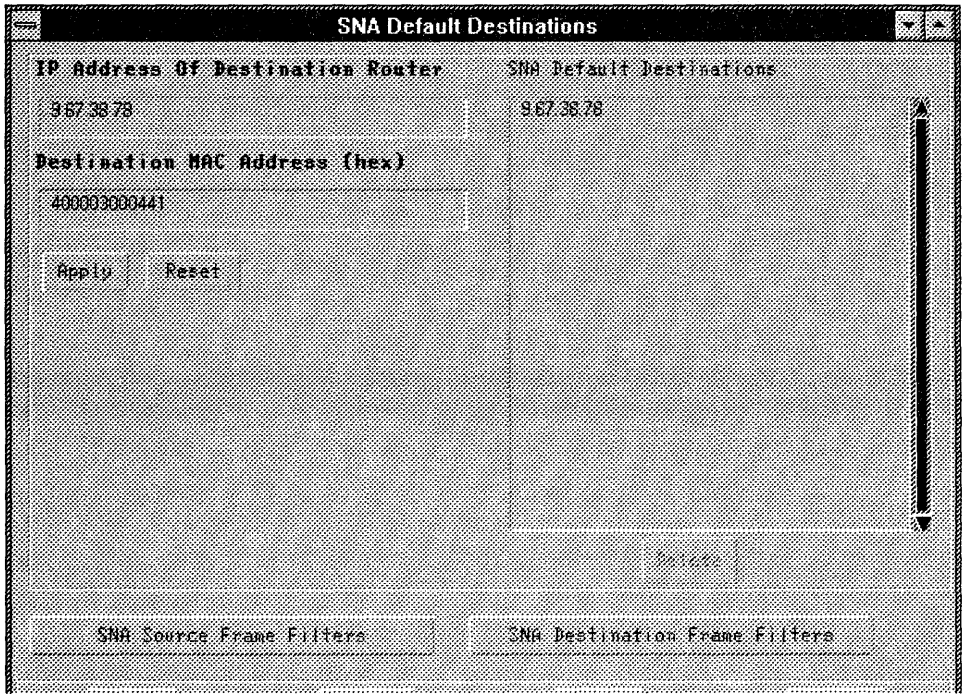


Figure 47. The DLS Configuration Options for SNA

- The NetBIOS configuration options are:
  - The IP address of the destination router
  - The MAC address of the destination

    The two entries above build the NetBIOS Default Destination table.
  - List of SNA Source Frame Filters
  - List of SNA Destination Frame Filters

Virtual Ring Segment Number

It is this ring segment number that will be placed in the token-ring Routing Information (RI) field as the DLS traffic leaves the 6611 Network Processor. It is **recommended** that the number be the same for every 6611 Network Processor that connects with DLS active.

Destination Cache Timeout

The DLS function will build routing tables with learned destinations (cache). These tables contain the destination MAC address with the IP address of the router to choose. These tables are refreshed and entries are deleted on timeout value given here.

Default DLS Address for This 6611

The IP address of the token-ring card. This will enable DLS to recover much faster in case of a TCP/IP link failure. See also 2.2.3, "Data Link Switching" on page 40.

Accept Connections only from Specific 6611 Routers

If **NO** , then this 6611 will receive SNA and/or NetBIOS traffic from any 6611 Network Processor that has DLS enabled. If **YES**, then SNA and/or NetBIOS traffic will only be accepted from the routers whose IP address is defined below as Participating DLS router.

Participating DLS Routers
IP address of 6611 Network Processor from which SNA and/or NetBIOS traffic will be accepted.

3.4.3.1 Configuring Remote Data Link Switching

Remote DLS is the normal case where stations attached to a token-ring wish to forward SNA and/or NetBIOS traffic over the router network to some application on that network.

The port type SNA configuration enables SNA traffic and asks for the SAP values to be forwarded.

The port type NetBIOS configuration enables NetBIOS traffic on the port and specifies Datagram and Datagram Broadcast.

3.4.3.2 Configuring Local Data Link Switching

Local DLS is the case of SDLC attached devices wishing to forward SNA frames over the router network. A typical example would be an SDLC attached IBM 3174 wishing to connect to an IBM 3745 Communications Controller as in Figure 49 on page 88. SDLC attached SNA devices need a Token-Ring Network LAA and a SAP. These are configured on the 6611 4-Port SDLC Adapter.

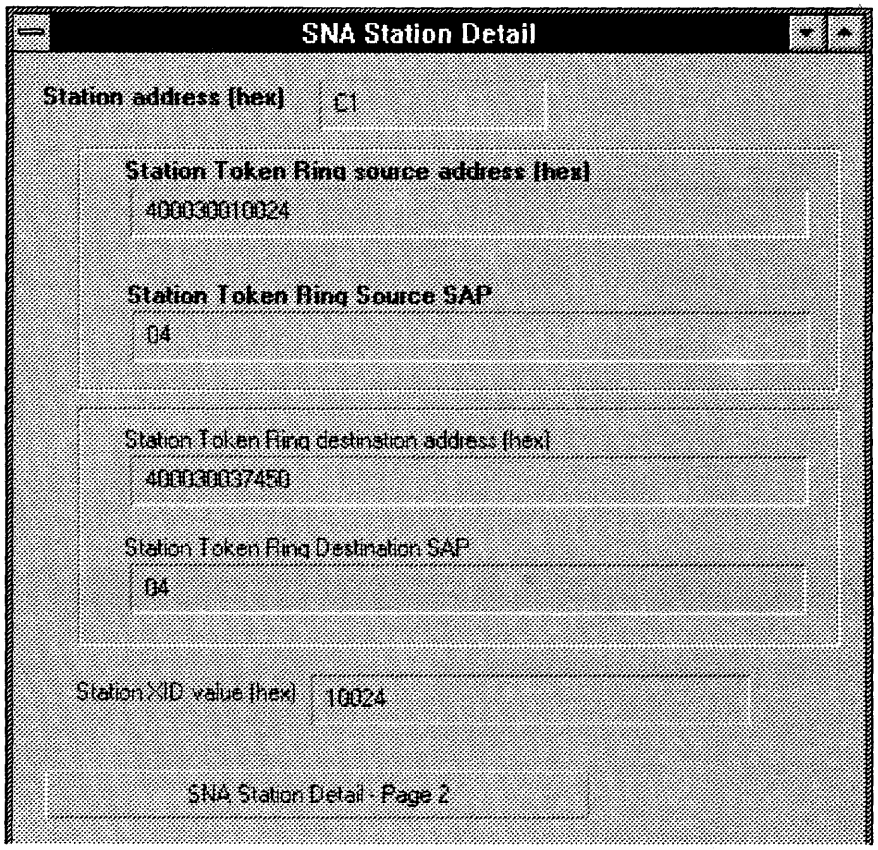


Figure 48. The 4-Port SNA Configuration for DLS

Station address This is the poll address for the station on the SDLC line, for example, *C1*.

Station Token-Ring source address DLS defines a *Virtual Ring Segment*, and all stations attached to it have MAC addresses. The SDLC attached devices have dummy LAA addresses as defined here.

Station Token-Ring Source SAP Together with the LAA defined above, this will define the SDLC attached device to other SNA devices that also use DLS.

Station Token-Ring destination address The LAA of the partner to which the source wants to connect. This is an optional parameter.

Station Token-Ring Destination SAP Will fully define the SNA destination, together with the destination LAA.

Station XID value This is the IDNUM and IDBLOCK needed in an exchange with VTAM.

Optional Parameters These parameters correspond to the VTAM definitions for SDLC lines.

Consider the case as described in Figure 49. The 6611 will get a virtual ring segment of 100, the 3174 will get an LAA of 400031740001 with a SAP of *04*. The 3174 must be known to the 3745 by its *station address* (polling address).

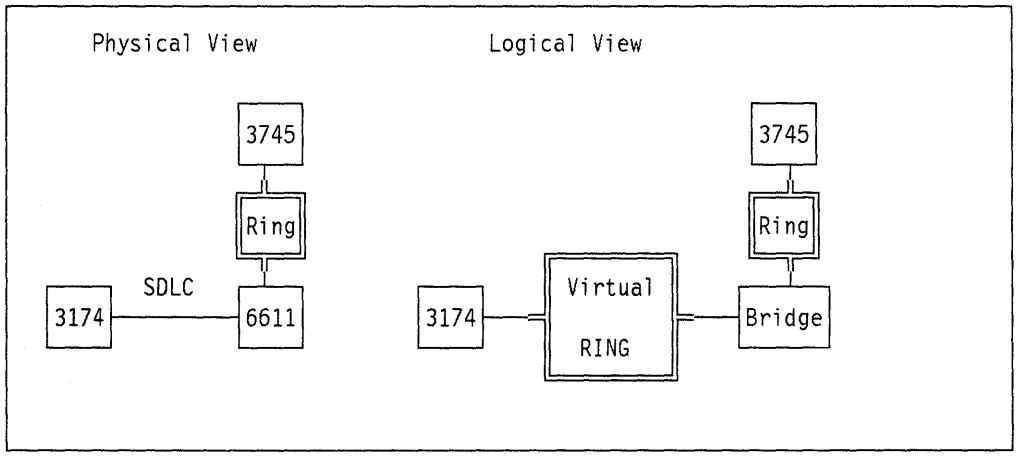


Figure 49. Local DLS from a 3174 to a 3745

Note: The polling address is used in case the 3174 is dialed up. To have a full connection with a 3745, XID exchange is required. Any downstream PU identifies itself to VTAM by an XID exchange.

3.4.3.3 SNA and NetBIOS over Bridged Links

Consider the example as described in Figure 50 on page 89 where a PS/2 connected to LAN segment 500 wants to connect to a 3745 that is Tokne Ring-attached to *routera*. DLS is operational between the two routers over a PPP link (TCP/IP). A PS/2 Remote Bridge connects *routerb* to LAN segment 500.

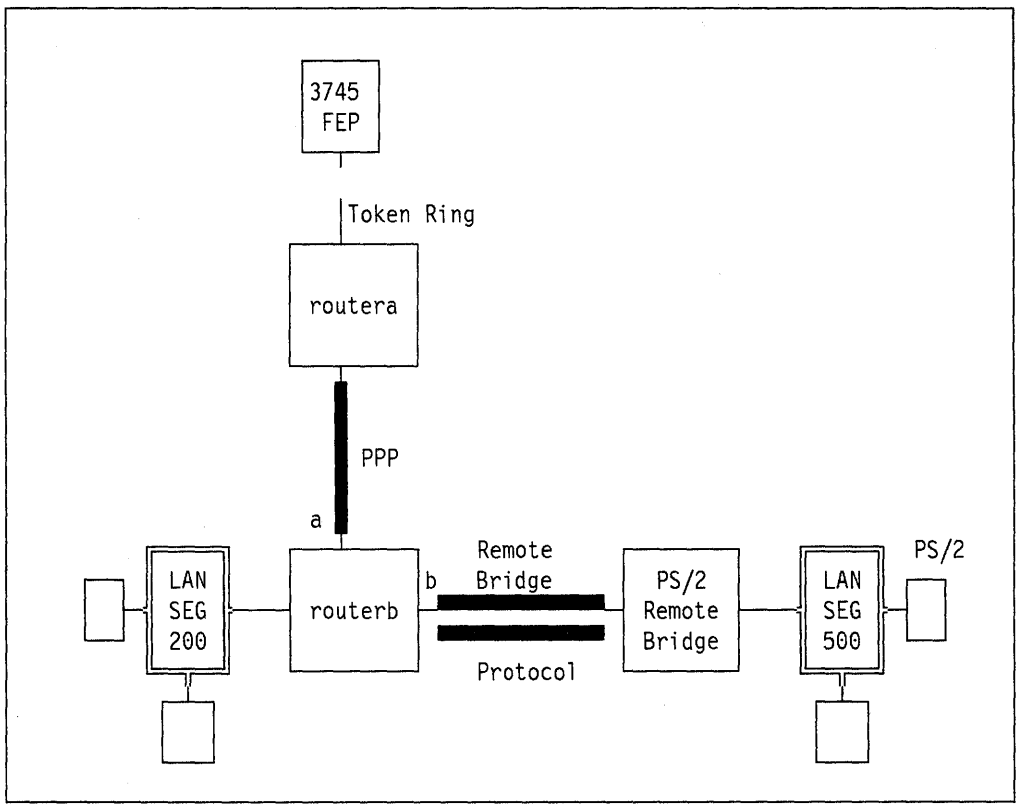


Figure 50. The Case for SNA and NetBIOS over Bridged Links

SNA frames will travel over the bridge and arrive in *routerb* where they will terminate. To transport SNA and NetBIOS frames that come over bridges the port must be configured to forward SNA and NetBIOS frames. In this example, both ports **a** and **b** would be configured for Source Route Bridging and the forwarding of SNA and NetBIOS frames. This is the reason why they can be configured in the panel as shown in Figure 40 on page 77. The same configuration options are available on the serial port where PPP or Frame Relay are defined. See Figure 51 on page 90.

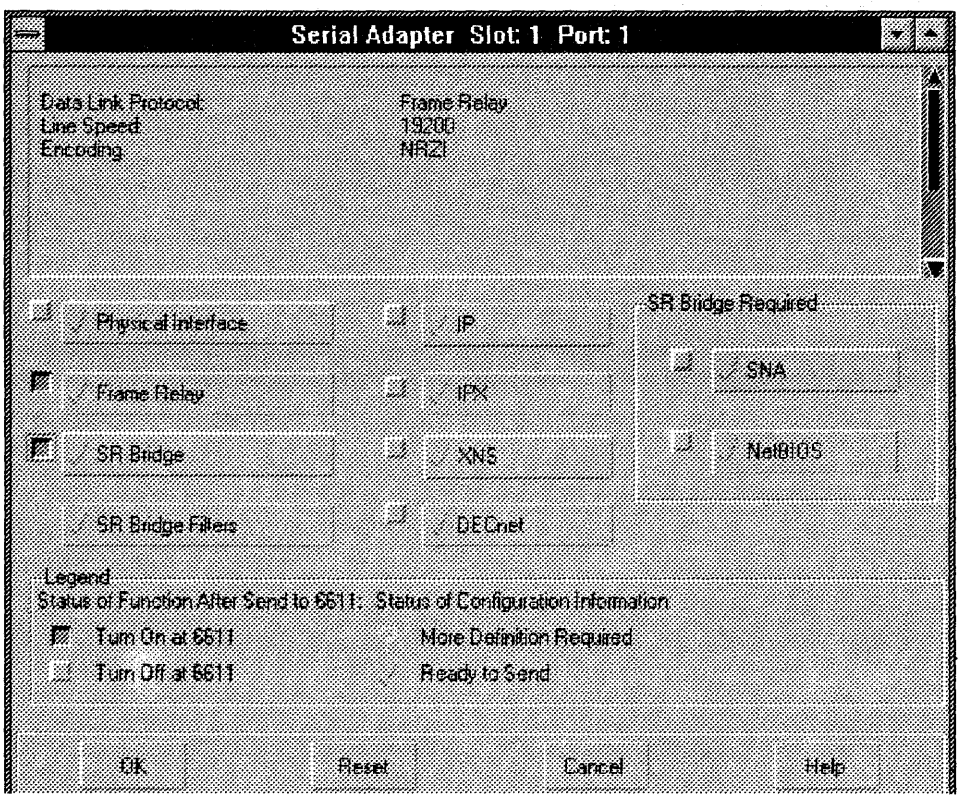


Figure 51. SNA and NetBIOS Definitions over Frame Relay

The SNA and NetBIOS configuration windows are only activated when source route bridging is also active, which is the condition for DLS.

Chapter 4. Managing the 6611

This chapter describes various facilities that can be used to manage 6611 Network Processors.

There are two main categories of management facilities provided by the 6611 Network Processor:

- The System Manager
- TCP/IP-Based Facilities

The facilities in both of these categories will normally be used together to effectively manage networks based on the 6611 Network Processor.

This chapter also describes considerations associated with the use of the 6611 Network Processor with IBM LAN Network Manager.

4.1 System Manager

The System Manager is an interactive user interface to support the management of a network of 6611 Network Processors. The System Manager provides functions that assist in the following tasks:

- Problem management
- Operations management
- Hardware and software maintenance
- Configuration management
- Security management

Either a full-screen or command line user interface is available for the System Manager, and each interface can be accessed via one of several methods. Methods for accessing the System Manager are described further in 4.1.1, "Access Methods, Security and Storage Areas" on page 92. The full-screen user interface provided by the System Manager is illustrated in Figure 52 on page 92.

New users of the System Manager will normally use the full-screen interface. Advanced users can use the command line interface to provide a fast path to System Manager functions.

The command line user interface can also be used in conjunction with a scripting language (executing on a TCP/IP host) to automate the performance of System Manager tasks. This requires that the System Manager be accessed from a TCP/IP host that supports the RSH protocol. The use of RSH is described further in 4.2.2, "Other TCP/IP Facilities" on page 126.

The functions provided by the System Manager are described in the following sections. A more detailed description of the System Manager and its capabilities is provided in the *IBM Multiprotocol Network Program: User's Guide*.

Note: The appearance of screens illustrated in this chapter may differ slightly from those generated by the System Manager. This is because they were captured from an early version of the System Manager.

```
IBM 6611                                                        routera
                                System Manager

Move cursor to desired item and press Enter.

    Performance and Statistics
    Problem Determination Facilities
    Concurrent Hardware Diagnostics

    Resource Control and Management
    System Environment and Configuration
    Remote Accesses to Other Nodes

    Software Installation and Maintenance
    Hardware Vital Product Data

    Configuration Files and Reports
    Adapter and Protocol Configuration

    System Manager Help


F1=Help            F2=Refresh          F3=Previous         F4=SysID
F10=Exit
```

Figure 52. System Manager Main Menu

4.1.1 Access Methods, Security and Storage Areas

The 6611 Network Processor System Manager can be accessed by several different methods. Each method falls into one of two categories:

- The method makes use of the 6611 Network Processor serial ports
- The method makes use of a TCP/IP network connection

4.1.1.1 Access via Serial Ports

Every 6611 Network Processor includes two integrated serial ports. The serial ports are denoted "S1" and "S2," and are located on the back panel of the 6611 Network Processor. Each serial port can be used to access the System Manager either locally or remotely using full-duplex asynchronous protocols.

Note: The S2 port can be used for a network management interface to a Cylink 4201 DSU/CSU. If a Cylink serial number is configured for any serial port the S2 port may not be used for service access.

Local access requires either a suitable ASCII display station, or computer emulating an ASCII display station, to be adjacent to the 6611 Network Processor. This is illustrated in Figure 53.

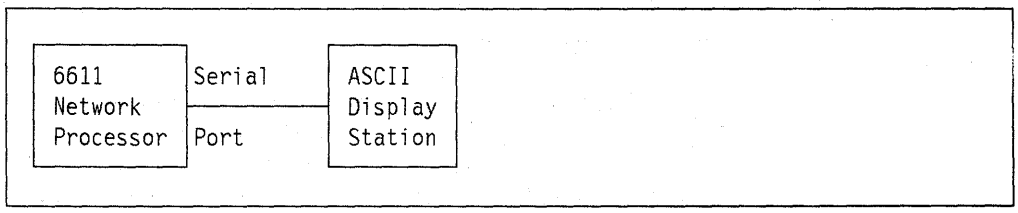


Figure 53. Local Access via Serial Port

Remote access requires a pair of suitable modems in addition to either a suitable ASCII Display Station or computer emulating an ASCII Display Station. This is illustrated in Figure 54 on page 93.

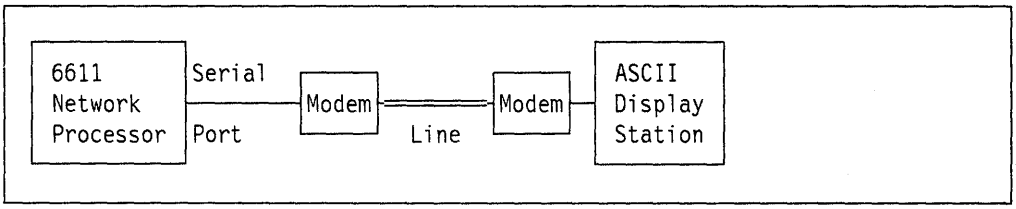


Figure 54. Remote Access via Serial Port

In some countries, an IBM service representative could request remote access to a 6611 Network Processor via the PSTN (Public Switched Telephone Network) to aid in problem resolution. To support this capability, a customer provided modem, and a telephone line are required to attach the 6611 Network Processor to the PSTN. This can be the same modem and line used to provide regular remote access by customer personnel if appropriate. This is illustrated in Figure 55.

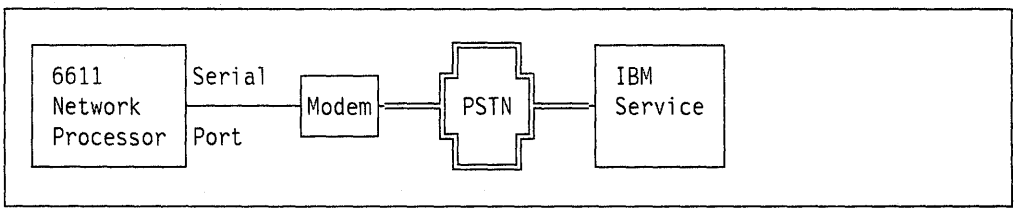


Figure 55. Remote Access for IBM Service via Serial Port

To support remote access by IBM service personnel, a serial port should be configured to operate at 2400 bps. The modem attached to that serial port should support CCITT V.22bis signalling and be configured for auto-answer operation.

A valid System Manager *userid*, password and the telephone number that can be used to reach the 6611 Network Processor, must be provided to IBM service personnel by the customer each time the use of this facility is required. System Manager *userids* and passwords are described further in 4.1.1.3, "Security" on page 95.

Note: The requirements for remote access by IBM service personnel may vary in some countries and should therefore be confirmed by an IBM representative prior to ordering a modem and telephone line for this purpose.

A wide range of ASCII display stations can be used to access the 6611 Network Processor System Manager via the serial ports. A complete list is provided in the *IBM 6611 Network Processor: Introduction and Planning Guide.*. This list includes most IBM ASCII display stations and popular models from other manufacturers.

Whenever a user logs onto the System Manager via a serial port, the user will be able to enter the type of the ASCII display station being used. It is important to enter the correct type of ASCII display station as the System Manager may be become unusable if an incorrect type is selected. If this occurs, the situation can be recovered by one of several methods:

- Logging off the System Manger - this may not be possible if the ASCII display station type entered is vastly different to the terminal type being used.
- Turning off the ASCII display station - this will be detected by the 6611 Network Processor which will then automatically log off the user from the System Manager. This may not be possible if the cable between the ASCII display station and the 6611 Network Processor is wired incorrectly.
- Unplugging the cable from the 6611 Network Processor to the ASCII display station. This should only be used as a last resort.

4.1.1.2 Access via TCP/IP Network

The 6611 Network Processor System Manager can be accessed via a TCP/IP network using either the TELNET, RLOGIN, REXEC or RSH protocols from a TCP/IP host. This is illustrated in Figure 56.

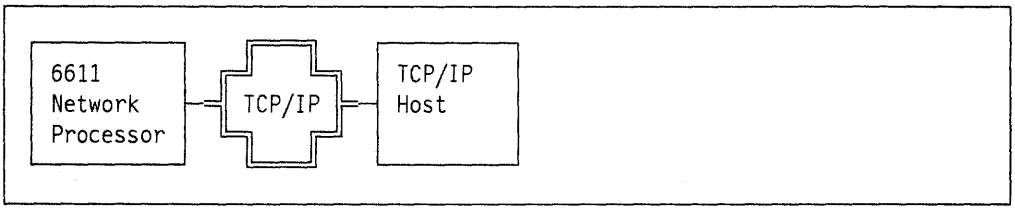


Figure 56. Accessing the System Manager via TCP/IP

The TELNET and RLOGIN protocols can be used to access both the full-screen and command line interfaces provided by the System Manager. The RSH and REXEC protocols can only be used to access the command line interface provided by the System Manager.

A wide variety of TCP/IP hosts can be used to access the 6611 Network Processor System Manager. Examples tested by the authors include:

- IBM RISC System/6000 running IBM AIX Version 3.2
- IBM Personal System/2 running IBM Operating System/2 Version 1.30.2 with IBM TCP/IP Version 1.2 for OS/2
- IBM Personal System/2 running IBM DOS Version 5 with IBM TCP/IP Version 2 for DOS

Note: Not all TCP/IP implementations support RLOGIN, RSH and REXEC. However most TCP/IP implementations (including all those listed above) support TELNET which can be used to access all System Manager functions.

The 6611 Network Processor System Manager can also be used as a TCP/IP host to access the System Manager on other 6611 Network Processors. This enables an ASCII display station attached to a serial port of one 6611 Network Processor to be used to access any other remote 6611 Network Processor via a TCP/IP network. This is illustrated in Figure 57.

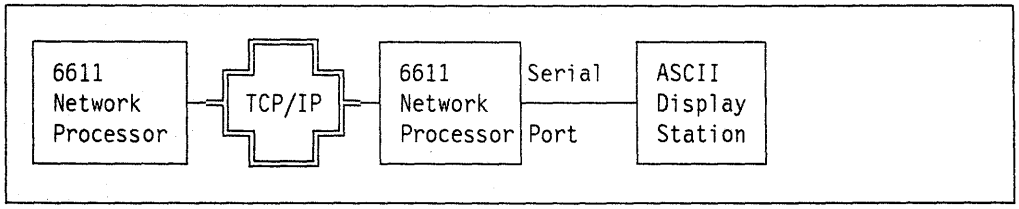


Figure 57. Accessing the System Manager via TCP/IP from another 6611

In some countries this capability can also be used in conjunction with remote access via a serial port by IBM service personnel to aid in problem resolution. The customer need only provide a single modem and telephone line to allow IBM service personnel to remotely access any 6611 Network Processor in the customer's network for problem resolution purposes.

TELNET, RLOGIN, RSH and REXEC can all be used from within the System Manager of a 6611 Network Processor to access the System Manager of any remote 6611 Network Processors. If a full-screen interface to the System Manager on a remote 6611 Network Processor is desired, RLOGIN should be used in preference to TELNET, as only RLOGIN supports direct file transfers from a computer emulating an ASCII display station to the remote 6611 Network Processor via the TCP/IP network.

4.1.1.3 Security

Access to the 6611 Network Processor System Manager is controlled through the use of *userids* and passwords.

When a user attempts to access the System Manager either via a serial port or via a TCP/IP network they will be prompted to enter a valid *userid* and password. If the *userid* is known to the 6611 Network Processor and the password is valid, the user will then be presented with the System Manager main menu.

There are two types of users:

- Controlling users
- Viewing users

Controlling users can access all functions of the System Manager. Viewing users can only access a subset of the System Manager functions that are non-intrusive.

Users of the 6611 Network Processor System Manager and their passwords can be defined either using the 6611 Network Processor configuration program or through menus available within the System Manager.

The 6611 Network Processor is shipped to customers with two users already defined:

- ibm6611c (password ibm6611c) a controlling user
- ibm6611v (password ibm6611v) a viewing user

These *userids* can be used to access the System Manager from a serial port prior to an initial configuration being loaded. Access via TCP/IP is not available until a valid 6611 Network Processor configuration has been loaded that contains the TCP/IP parameters to be used by the 6611 Network Processor.

Note: For security reasons, the passwords for the ibm6611c and ibm6611v *userids* should be changed or the *userids* removed completely prior to using a 6611 Network Processor in a production environment.

4.1.1.4 Storage Areas

The System Manager makes use of two storage areas to support many of its functions. These storage areas are:

- Transfer directory
- Static directory

The transfer directory is used as a temporary storage area for:

- Files produced by System Manager functions that are to be exported to other systems. For example problem determination data is first stored in the transfer directory by the System Manager problem determination functions prior to being exported to other systems.
- Files required by System Manager functions that have been imported from other systems. For example configurations for a 6611 Network Processor first could be stored in the transfer directory prior to being activated on the 6611 Network Processor.

The static directory contains files that may be required by other systems. For example MIB modules that can be loaded by network management systems to aid in the management of 6611 Network Processors are contained in the static directory. The use of MIB modules is described further in 4.2.1.4, "SNMP Client" on page 122.

The contents of the static directory are in general unchanging as the name suggests. However the contents may change when updates to the Multiprotocol Network Program are applied. The application of updates to the Multiprotocol Network Program is described further in 4.1.4.1, "Software Installation and Maintenance" on page 107.

Files can be imported to the transfer directory or exported from either the transfer directory or static directory using any of the following methods:

FTP

Uses the FTP (File Transfer Protocol) across a TCP/IP network to transfer files between the transfer directory (import and export) or static directory (export only) and a remote TCP/IP host. These capabilities are provided by the "Send Files to Another Node" and "Receive Files from Another Node" menu options described in 4.1.3.3, "Remote Accesses to Other Nodes" on page 105.

XMODEM

Uses one of the 6611 Network Processor serial ports to transfer files between the transfer directory (import and export) or static directory (export only) and a computer emulating an ASCII display station. These capabilities are provided by the "Send Files to Another Node" and "Receive Files from Another Node" menu options described in 4.1.3.3, "Remote Accesses to Other Nodes" on page 105.

DOS Diskette

Uses a diskette to transfer files between the transfer directory (import and export) or static directory (export only) and either an IBM DOS or IBM Operating System/2 based system. Diskettes must first be formatted in "DOS" format using an IBM DOS or IBM Operating System/2 based system, or the 6611 Network Processor System Manager. These capabilities are provided by the "Perform Diskette

Operations" menu option described in 4.1.3.2, "System Environment and Configuration" on page 104.

UNIX Diskette

Uses a diskette to transfer files between the transfer directory (import and export) or static directory (export only) and a UNIX** based system. Diskettes must first be formatted in "UNIX" format using a UNIX based system or the 6611 Network Processor System Manager. These capabilities are provided by the "Perform Diskette Operations" menu option described in 4.1.3.2, "System Environment and Configuration" on page 104.

4.1.2 Problem Management

The problem management functions provided by the System Manager are grouped into three areas:

- Performance and Statistics
- Problem Determination Facilities
- Concurrent Hardware Diagnostics

Each group of functions is available on a separate menu within the System Manager full-screen interface.

Note: Most of the problem management functions provided by the 6611 Network Processor are designed for use by IBM service personnel only. For this reason, the *IBM Multiprotocol Network Program: User's Guide* does not describe how the information provided by these functions should be interpreted. However the *IBM Multiprotocol Network Program: User's Guide* does describe how each of these functions is accessed, as IBM service personnel may request customers to access these functions, and export the outputs of these functions to IBM for analysis.

Each group of System Manager functions to support problem management tasks is described in more detail in the following sections.

4.1.2.1 Performance and Statistics

The System Manager can be used to access a wide range of performance and statistical information related to the operation of the 6611 Network Processor. The "Performance and Statistics" menu is illustrated in Figure 58 on page 98.

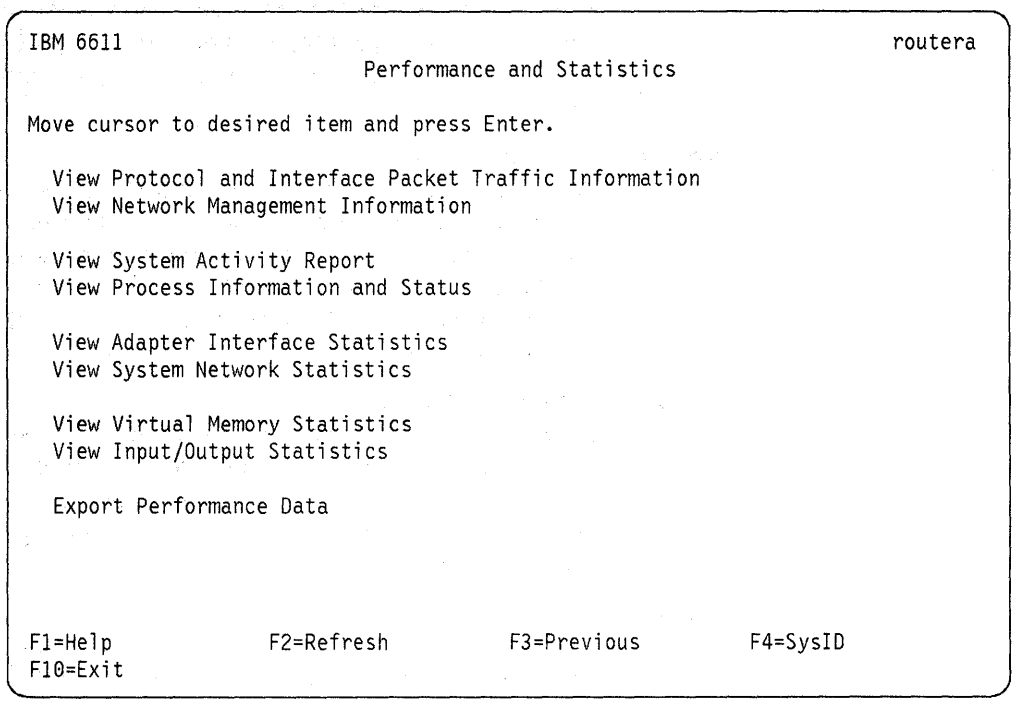


Figure 58. Performance and Statistics Menu

The functions provided by each menu option are:

View Protocol and Interface Packet Traffic Information
Provides a real-time dynamic display of the number of packets processed for each protocol and communication interface. This display is a good "snapshot" of the traffic being processed by the 6611 Network Processor at any particular moment in time.

View Network Management Information
Provides the capability to query any SNMP agent and examine the MIB variables that are accessible via the SNMP agent. Various MIB modules can be loaded to aid in the retrieval of MIB variables from the SNMP agent. The use of this function is described further in 4.2.1.4, "SNMP Client" on page 122.

View System Activity Report
Provides information on the utilization of various system resources. The output of this option can be directed to the transfer directory to allow subsequent export. For example the utilization of the system processor CPU can be obtained using this report.

View Process Information and Status
Provides information on the processes (tasks) executing on the system processor and their status. The output of this option can be directed to the transfer directory to allow subsequent export. The information contained in this report is probably only of interest to IBM service personnel.

View Adapter Interface Statistics
Provides various TCP/IP networking statistics gathered by the communication adapter features that are capable of adapter to adapter transfers (that is, the token-ring, Ethernet and serial adapters). Connection, protocol or packet traffic statistics can be

queried for any interface on these communication adapter features. The information available is similar to that provided by various options of the "netstat" command that is available on many TCP/IP implementations.

View System Network Statistics
Provides various TCP/IP networking statistics gathered by the system processor. Connection, protocol, packet traffic, memory management, route, socket or active internet connection statistics can be queried. The information available is similar to that provided by various options of the "netstat" command that is available on many TCP/IP implementations.

View Virtual Memory Statistics
Provides information on the utilization of virtual memory by processes executing on the system processor. The output of this option can be directed to the transfer directory to allow subsequent export. The information contained in this report is probably only of interest to IBM service personnel.

View Input/Output Statistics
Provides information on the utilization of I/O devices such as the serial ports and fixed disk(s). The output of this option can be directed to the transfer directory to allow subsequent export.

Export Performance Data
Enables performance data to be transferred elsewhere for subsequent analysis, usually by IBM service personnel. To use this capability, performance data must first be collected via one of the other options on the "Performance and Statistics" menu and placed in the transfer directory. Either FTP, XMODEM, DOS diskettes or UNIX diskettes can be used to export the performance data.

4.1.2.2 Problem Determination Facilities

The System Manager can be used to access various functions that aid problem determination. These functions are provided on the "Problem Determination Facilities" menu. Many of these functions will usually only be used at the direction of IBM service personnel.

The "Problem Determination Facilities" menu is illustrated in Figure 59 on page 100.

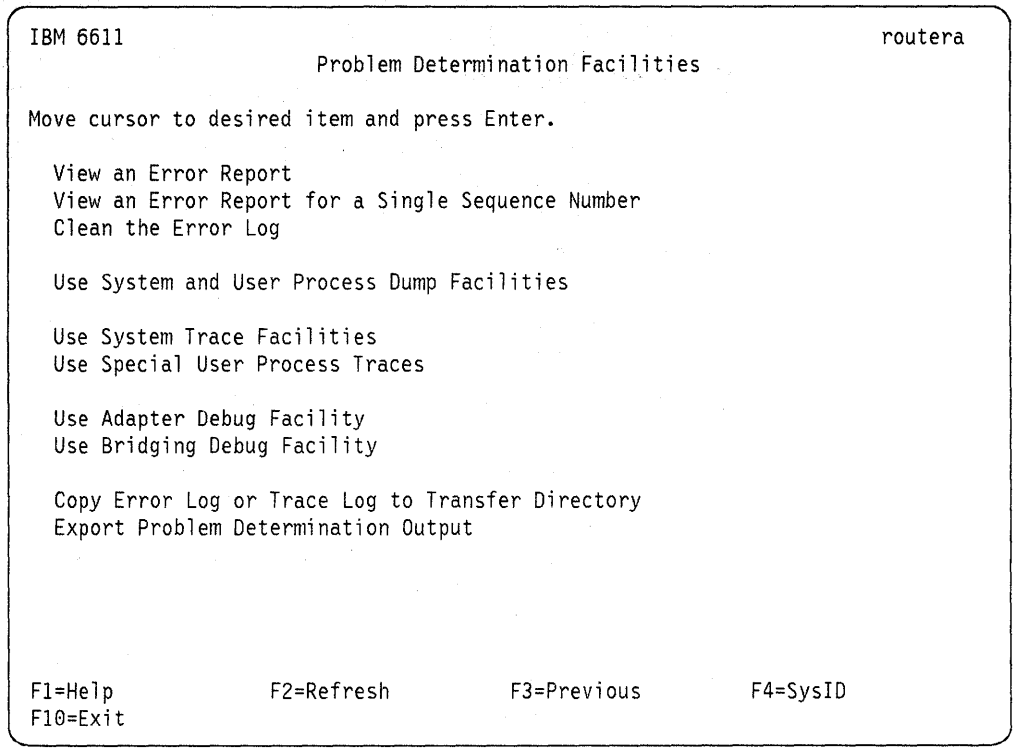


Figure 59. Problem Determination Facilities Menu

The functions provided by each menu option are:

View an Error Report (for a Single Sequence Number)
Provides information on errors logged by the Multiprotocol Network Program. Errors which require a user response are automatically converted to SNMP traps. The use of SNMP traps is described further in 4.2.1.2, "SNMP Traps" on page 120. The output of these options can be directed to the transfer directory to allow subsequent export.

Clean the Error Log
Provides the capability to remove entries from the error log based on age, resource class, resource name or error ID.

Use System and User Process Dump Facilities
Provides the capability to dump the memory used by various components of the Multiprotocol Network Program. A formatted version of the system dump is available.

Use System Trace Facilities
Provides the capability to trace various components of the Multiprotocol Network Program and view a report of the data captured by such traces. The output of this option can be directed to the transfer directory to allow subsequent export.

Use Special User Process Traces
Provides the capability to trace functions that have special purpose traces. The functions that have special purpose traces are:

IP routing protocols
SNMP agent
System monitor
X.25

The output of this option can be directed to the transfer directory to allow subsequent export.

Use Adapter Debug Facility
Provides various debugging aids for the microcode that executes on the 6611 2-Port Serial Adapter, 6611 Token-Ring Network 16/4 Adapter and 6611 Ethernet Adapter. Some of the outputs of this option are placed in the transfer directory to allow subsequent export.

Use Bridging Debug Facility
Provides various debugging aids for the microcode that executes on the 6611 2-Port Serial Adapter and 6611 Token-Ring Network 16/4 Adapter that is used for bridging functions.

Copy Error Log or Trace Log to Transfer Directory
Copies the 6611 Network Processor error log or trace log to the transfer directory so that they can be subsequently exported. The error log is automatically created by the Multiprotocol Network Program. The trace log is created whenever the "Use System Trace Facilities" option is used. Neither of these logs are in a human readable format; however, reports are available through the "View an Error Report" and "Use System Trace Facilities" options.

Export Problem Determination Output
Enables problem determination output to be transferred elsewhere for subsequent analysis, usually by IBM service personnel. To use this capability, problem determination output must first be collected via one of the other options on the "Problem Determination" menu and placed in the transfer directory. Either FTP, XMODEM, DOS diskettes or UNIX diskettes can be used to export the problem determination data.

4.1.2.3 Concurrent Hardware Diagnostics

The 6611 Network Processor provides the capability to execute hardware diagnostics concurrently with operation of the Multiprotocol Network Program. Only those components of the 6611 Network Processor that are being tested are impacted by the use of concurrent hardware diagnostics.

For example, a communication adapter feature can be tested while remaining communication adapter features and the rest of the 6611 Network Processor continues to operate normally.

The functions provided by concurrent hardware diagnostics are illustrated in Figure 60 on page 102.

```
FUNCTION SELECTION                                                  801002

Move cursor to selection, then press Enter.

  Diagnostic Routines
    This selection will test the machine hardware and detect
    any hardware problems.  A problem will be indicated by a
    SRN (Service Request Number).  The SRN will allow a service
    representative to quickly determine what parts are required
    to repair the machine.
  Service Aid
    This selection will look at the machine configuration, exercise
    external interfaces, format media, look at past diagnostic
    results, control what resources are tested, check out media, etc.
  Advanced Diagnostic Routines
    This selection will normally be used by the service representative.




F3=Cancel          F7=Page Up          F8=Page Down        F10=Exit
```

Figure 60. Concurrent Hardware Diagnostics Menu

The 6611 Network Processor also provides stand-alone diagnostics which are described in the *IBM 6611 Network Processor: Installation and Service Guide*.

4.1.3 Operations Management

The operations management functions provided by the System Manager are grouped into three areas:

- Resource Control and Management
- System Environment and Configuration
- Remote Accesses to Other Nodes

Each group of functions is available on a separate menu within the System Manager full-screen interface.

Each group of System Manager functions to support operations management tasks is described in more detail in the following sections.

4.1.3.1 Resource Control and Management

The System Manager provides several functions to control various aspects of 6611 Network Processor operations. These are provided on the "Resource Control and Management" menu.

Note: Great care should be taken in the use of some of these functions as their incorrect use may severely impact the operation of the 6611 Network Processor.

The "Resource Control and Management" menu is illustrated in Figure 61 on page 103.

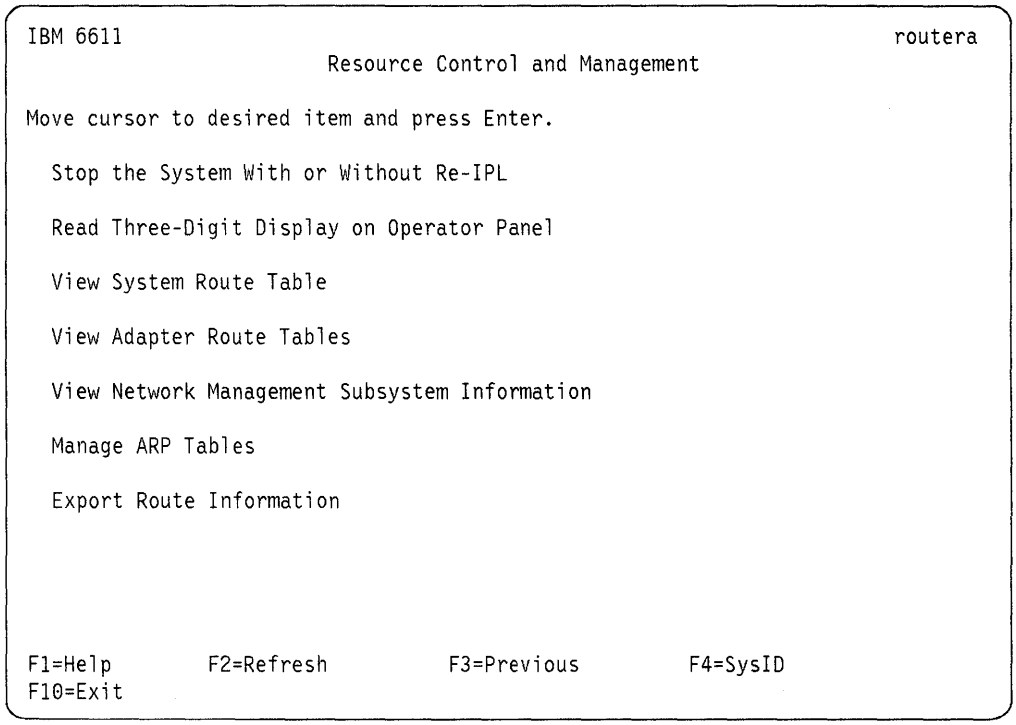


Figure 61. Resource Control and Management Menu

The functions provided by each menu option are:

Stop the System With or Without Re-IPL
Performs an orderly shutdown of the 6611 Network Processor, optionally followed by a restart. This option should always be used before removing power to the 6611 Network Processor prior to relocation or servicing. Any other users of the System Manager will receive a notification message warning them that a shutdown is imminent.

Read Three-Digit Display on Operator Panel
Displays the value that is currently showing on the three-digit display on the front of the 6611 Network Processor. This option will normally be used when accessing the 6611 Network Processor remotely.

View System Route Table
Provides various displays of the routing tables used by the 6611 Network Processor. The output of these displays may be placed in the transfer directory for subsequent export.

View Adapter Route Tables
Provides various displays of the routing tables on the 6611 Token-Ring Network 16/4 Adapter, 6611 Ethernet Adapter and the 6611 2-Port Serial Adapter. The output of these displays may be placed in the transfer directory for subsequent export.

View Network Management Subsystem Information
Provides various detailed information on the configuration of the SNMP-based management subsystem. The output of these displays may be placed in the transfer directory for subsequent export.

Manage ARP Tables

Provides functions to display and update the ARP (Address Resolution Protocol) table that provides for translation between network layer addresses and data link layer addresses for the TCP/IP protocol suite.

This option may be useful after extensive network changes have occurred to remove old ARP table entries that are no longer valid and force new ARP table entries to be discovered by ARP. Entries can also be added manually to the ARP table to eliminate the need for new entries to be discovered using ARP.

Export Route Information

Provides various export methods for exporting route tables. The methods available include FTP, Modem, DOS diskette and UNIX diskette.

4.1.3.2 System Environment and Configuration

The System Manager provides various utility functions which can be used to assist in the management and configuration of management functions for the 6611 Network Processor. These functions are provided on the "System Environment and Configuration" menu.

The "System Environment and Configuration" menu is illustrated in Figure 62.

```
IBM 6611                                                          routera
                    System Environment and Configuration

Move cursor to desired item and press Enter.

  Work with Files in Transfer Directory
  View a File in the Static Directory

  Send AT Command to Modem on Serial Port

  Perform Diskette Operations

  Change Date and Time
  Change Date, Time and Time Zone

  Perform System Configuration Changes




F1=Help          F2=Refresh          F3=Previous          F4=SysID
F10=Exit
```

Figure 62. System Environment and Configuration Menu

The functions provided by each menu option are:

Work with Files in Transfer Directory

Provides the capability to view, rename and delete files stored in the transfer directory. The role of the transfer directory is described further in 4.1.1.4, "Storage Areas" on page 96.

View a File in the Static Directory

Provides the capability to view files stored in the static directory. The role of the static directory is described further in 4.1.1.4, "Storage Areas" on page 96.

Send AT Command to Modem on Serial Port

Provides the capability to configure a modem that is attached to a 6611 Network Processor serial port. For example, this function could be used to configure a modem in auto-answer mode so that it could be used to support remote access to the System Manager.

Perform Diskette Operations

Provides various capabilities for working with diskettes formatted for use with either the IBM Operating System/2 and IBM DOS operating systems (DOS format) or for use with UNIX operating systems (UNIX format). The capabilities provided are:

- Format a diskette (in either DOS or UNIX format)
- List files on a diskette
- Copy files from diskette to the transfer directory
- Copy files from either the transfer or static directories to diskette

Change Date and Time (and Time Zone)

Provides the capability to change the date and time and optionally the time zone used by the 6611 Network Processor. This only changes the date and time on a single 6611 Network Processor.

Perform System Configuration Changes

Provides the capability to change some aspects of the 6611 Network Processor configuration that are related to system management. The functions provided include:

- Configuration of the 6611 Network Processor serial ports.
- Managing the *userids* and passwords that are valid for accessing the System Manager.
- Managing the TCP/IP host name table.
- Managing the use of TCP/IP name servers by the 6611 Network Processor.
- Managing the use of TCP/IP time servers by the 6611 Network Processor.
- Apply, commit or reject changes made to the 6611 Network Processor configuration by any of the above functions.

A more detailed description of the application of many of these functions is described in 4.2.2.4, "Configuration of TCP/IP Facilities" on page 128.

4.1.3.3 Remote Accesses to Other Nodes

The System Manager provides many functions that can be used to access other TCP/IP hosts including other 6611 Network Processors. These functions are provided on the "Remote Accesses to Other Nodes" menu. Many of these facilities are described further in 4.2.2, "Other TCP/IP Facilities" on page 126.

The "Remote Accesses to Other Nodes" menu is illustrated in Figure 63 on page 106.

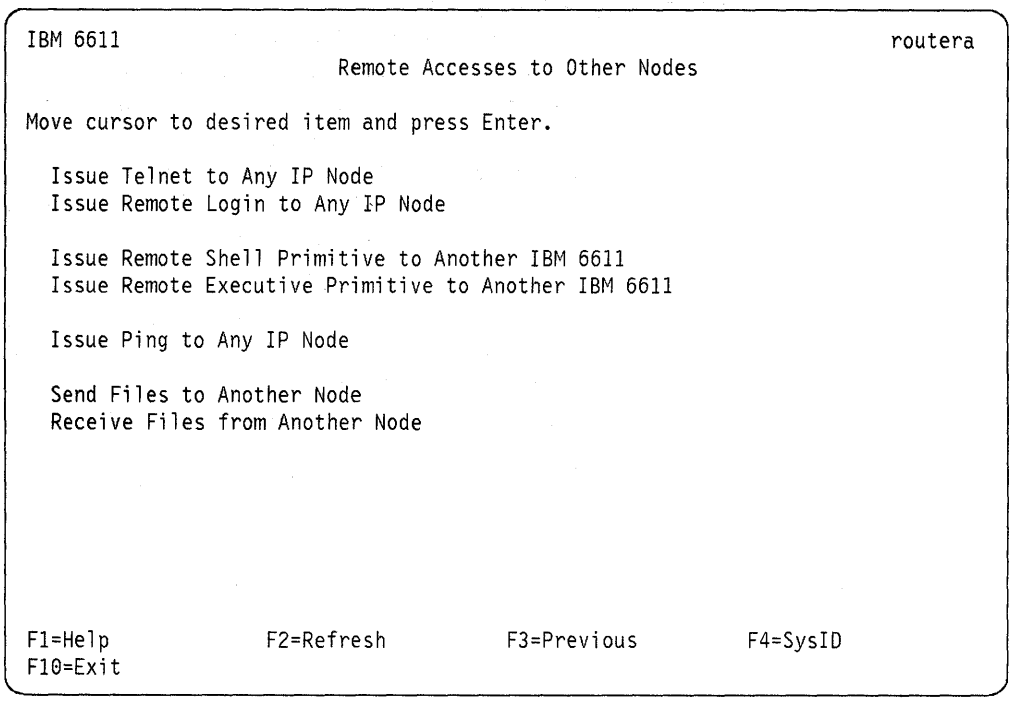


Figure 63. Remote Accesses to Other Nodes Menu

The functions provided by each menu option are:

Issue Telnet to Any IP Node
Provides the capability for the System Manager user to login to other TCP/IP hosts using the TELNET protocol. This option can be used to access the System Manager of another 6611 Network Processor.

Issue Remote Login to Any IP Node
Provides the capability for the System Manager user to login to other TCP/IP hosts using the RLOGIN protocol. This option can be used to access the System Manager of another 6611 Network Processor. It is the preferred method for accessing other 6611 Network Processors when the user has accessed the System Manager via a serial port from a computer emulating an ASCII display station, and a file transfer capability to or from any 6611 Network Processor is required. Such file transfers make use of the XMODEM protocol.

Issue Remote Shell Primitive to Another IBM 6611
Provides the capability for the System Manager user to execute functions on a remote 6611 Network Processor using the RSH protocol.

Issue Remote Executive Primitive to Another IBM 6611
Provides the capability for the System Manager user to execute functions on a remote 6611 Network Processor using the REXEC protocol.

Issue Ping to Any IP Node
Provides the capability to test connectivity with other TCP/IP hosts using PING (Packet InterNet Groper). PING can be used to aid in resolving problems that may occur when trying to use the TCP/IP based management facilities provided by the 6611 Network Processor.

Send Files to Another Node
Provides a file transfer capability to either TCP/IP hosts using the FTP protocol, or to the computer being used to access the System Manager via a serial port. To send files to TCP/IP hosts they must provide an FTP server. To send files to a computer that is being used to access the System Manager via a serial port, that computer must support the XMODEM protocol. Files sent can come from either the transfer directory or the static directory.

Receive Files from Another Node
Provides a file transfer capability from either TCP/IP hosts using the FTP protocol, or to the computer being used to access the System Manager via a serial port. To receive files from TCP/IP hosts they must provide an FTP server. To receive files from a computer that is being used to access the System Manager via a serial port, that computer must support the XMODEM protocol. Files received are placed in the transfer directory.

4.1.4 Maintenance

The maintenance functions provided by the System Manager are grouped into two areas:

- Software Installation and Maintenance
- Hardware Vital Product Data

Each group of functions is available on a separate menu within the System Manager full-screen interface.

Each group of System Manager functions to support maintenance tasks is described in more detail in the following sections.

4.1.4.1 Software Installation and Maintenance

The System Manager provides several functions to assist in the maintenance of the Multiprotocol Network Program. These functions are provided on the "Software Installation and Maintenance" menu.

The "Software Installation and Maintenance" menu is illustrated in Figure 64 on page 108.

```
IBM 6611                                                          routera
                    Software Installation and Maintenance

Move cursor to desired item and press Enter.

  Import Software to Transfer Directory
  List All Software in the Transfer Directory
  List All Problems Fixed by Software Updates in Transfer Directory

  Apply Software Components
  Apply Software Updates
  Restart the System After Applying New Software
  Clean up After a Failed Installation

  List All Applied but Not Committed Software
  Commit Applied Updates (Delete Previous Version)
  Reject Applied Updates (Use Previous Version)
  Reinstate Saved Software Component
  Remove Saved Software Component

  View Software Vital Product Data

F1=Help          F2=Refresh          F3=Previous          F4=SysID
F10=Exit
```

Figure 64. Software Installation and Maintenance Menu

The Multiprotocol Network Program consists of software components with complex interdependencies. Any changes to the software components come in the form of software updates or PTFs. The software installation and maintenance capabilities of the 6611 Network Processor are very comprehensive and include:

- Prerequisite checking
- Automatic backup of previous version
- Backout capability

The software that exists on the 6611 Network Processor is tracked separately and can exist in any one of the following states:

Not Present Not available

Imported Available for installation

Applied Available for use - backout possible

Committed Available for use - backout not possible

The software installation and maintenance process provides several actions that can be applied to each version of each software component. Each of these actions is available through the "Software Installation and Maintenance" menu. The available actions are:

Import Imports a new version of a software component or update to the transfer directory. The software component or update can be imported using either FTP, XMODEM or UNIX diskettes. Once imported to the transfer directory, the software component or update can be installed.

Apply Creates a backup copy of the previous version of the software component or update, and installs the new version of the software component or update from the transfer directory or from the diskette drive of the 6611. After installation software components are in the "committed" state and software updates are in the "applied" state.

Reject Removes the software update and restores the saved files from the backup copy taken during the "Apply" action. The software must be in the "Applied" state to support the "Reject" action.

Commit Deletes the backup copy of the files saved when the software update was installed. A reject of the software update will no longer be possible as the backup files no longer exists. The software update must be in the "Applied" state to support the "Commit" action.

Remove Deletes the previous saved version of a software component to create space.

Reinstate Reverts back to the previously saved version of the software component.

The actions and states provided by the software installation and maintenance process for software updates are illustrated in Figure 65.

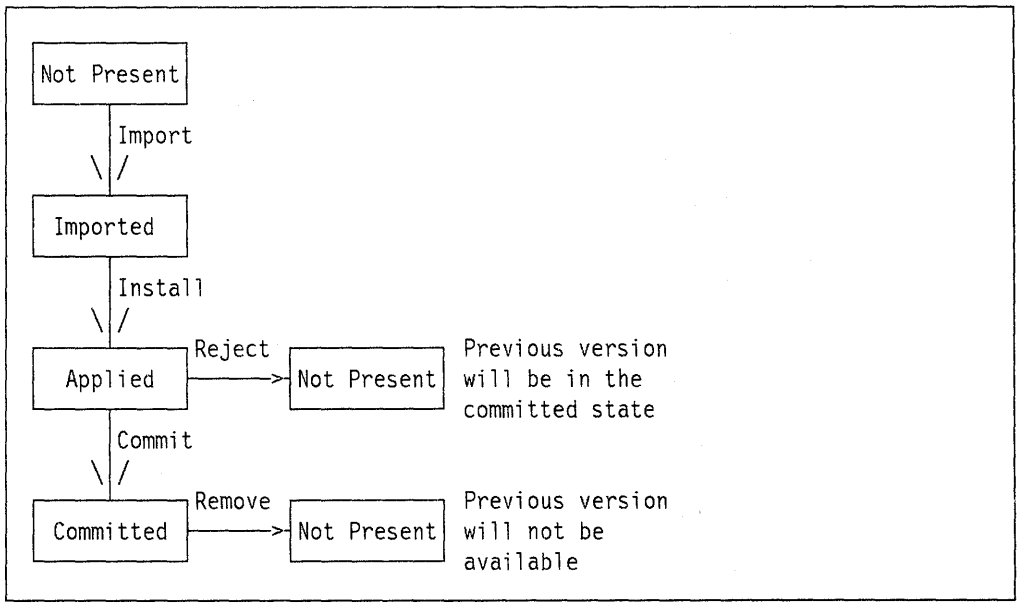


Figure 65. Software Installation and Maintenance Process

4.1.4.2 Hardware Vital Product Data

The System Manager provides several functions to gather information on the hardware components of a 6611 Network Processor. These functions are provided on the "Hardware Vital Product Data" menu.

The "Hardware Vital Product Data" menu is illustrated in Figure 66 on page 110.

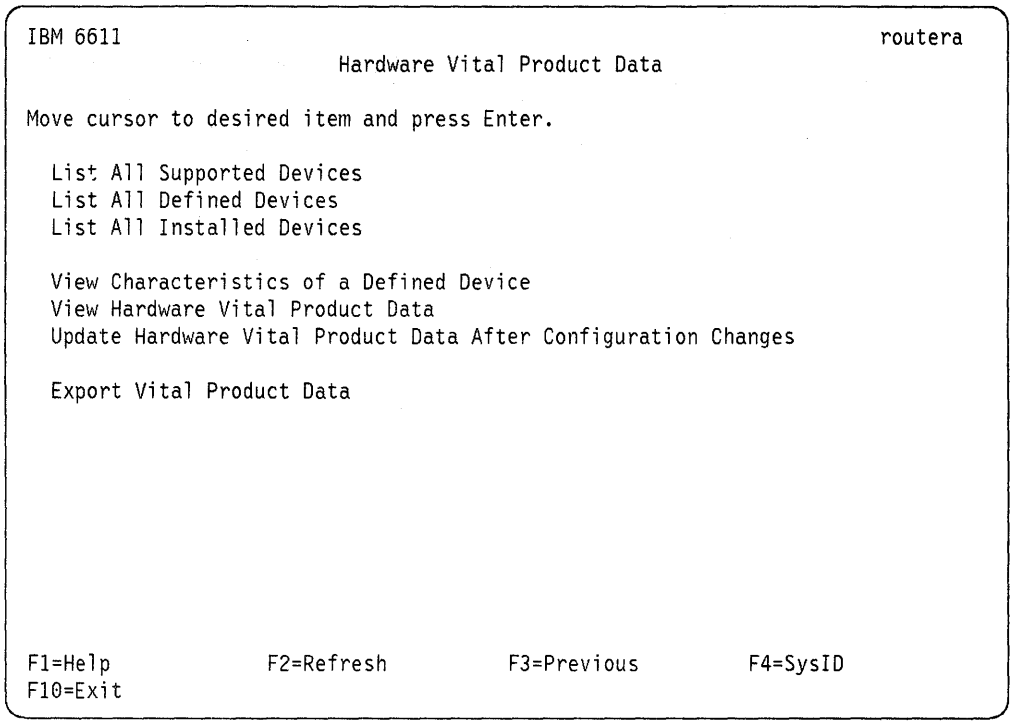


Figure 66. Hardware Vital Product Data

These functions will normally only be used by an IBM service representative when performing hardware upgrades or maintenance to the 6611 Network Processor.

4.1.5 Configuration

The configuration functions provided by the System Manager are grouped into two areas:

- Configuration Files and Reports
- Adapter and Protocol Configuration

Each group of functions is available on a separate menu within the System Manager full-screen interface.

Each group of System Manager functions to support configuration tasks is described in more detail in the following sections.

4.1.5.1 Configuration Files and Reports

The System Manager provides various functions to manage configurations created using the 6611 Network Processor configuration program. These functions are provided on the "Configuration Files and Reports" menu.

The "Configuration Files and Reports" menu is illustrated in Figure 67 on page 111.

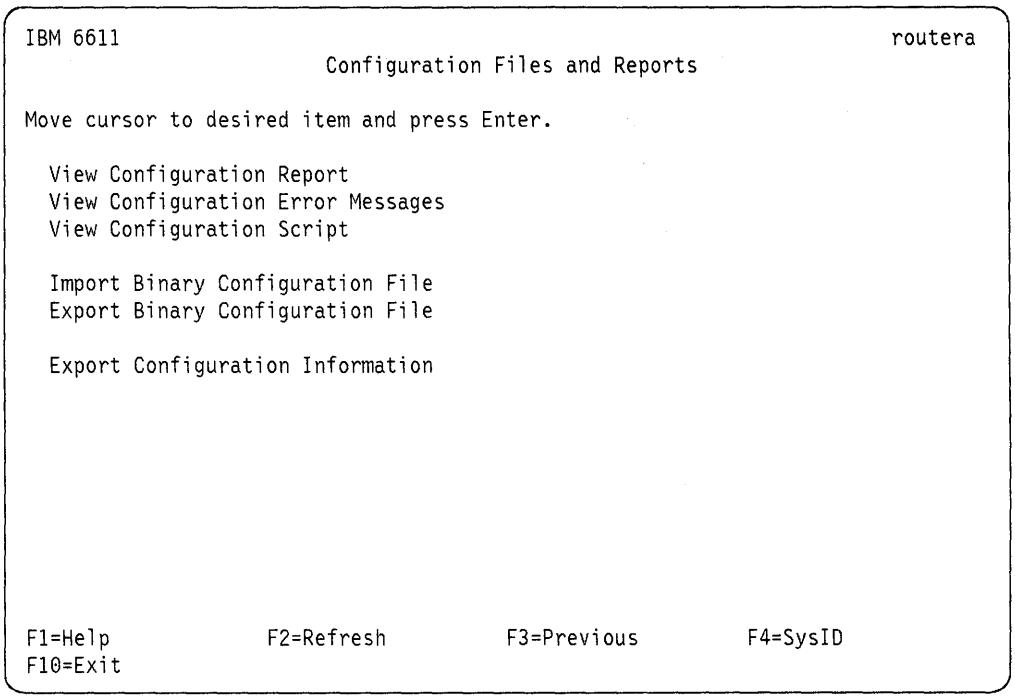


Figure 67. Configuration Files and Reports

The functions provided by each menu option are:

View Configuration Report
Provides a report on the current configuration of the 6611 Network Processor. Either a brief or detailed report can be requested. The reports generated by this option are a very useful aid to resolving configuration problems. The output of this option can be directed to the transfer directory to allow subsequent export.

View Configuration Error Messages
Provides a report of any errors that have occurred while processing configuration files generated by the 6611 Network Processor configuration program or processing changes to the configuration made using the System Manager. The output of this option can be directed to the transfer directory to allow subsequent export.

View Configuration Script
Provides a listing of all the commands that were used by the System Manager to implement any configuration changes requested during the current System Manager session. This listing can be used to develop scripts running on TCP/IP hosts that use RSH to make configuration changes on 6611 Network Processors. The output of this option can be directed to the transfer directory to allow subsequent export.

Import Binary Configuration File
Provides the capability to process a configuration file generated by the 6611 Network Processor configuration program. Once processed, the parameters contained within that configuration file will be those used by the 6611 Network Processor. The configuration file that is to be processed can be located in the transfer directory, on a DOS formatted diskette, or transferred from another system to the 6611 Network Processor using FTP or XMODEM.

Export Binary Configuration File

Provides the capability to generate a configuration file that can be read and possibly modified by the 6611 Network Processor configuration program. The configuration file that is generated reflects the current configuration of the 6611 Network Processor. The configuration file can be placed in the transfer directory, on a DOS formatted diskette, or transferred from the 6611 Network Processor to another system using FTP or XMODEM.

Export Configuration Information

Allows the output of various options of the "Configuration Files and Reports" menu to be transferred to other systems using either FTP, XMODEM, DOS formatted diskettes or UNIX formatted diskettes.

4.1.5.2 Adapter and Protocol Configuration

The System Manager provides various functions to allow the configuration of the 6611 Network Processor to be changed interactively. These functions are provided on the "Adapter and Protocol Configuration" menu.

The "Adapter and Protocol Configuration" menu is illustrated in Figure 67 on page 111.

```
IBM 6611                                                          routera
                      Adapter and Protocol Configuration

Move cursor to desired item and press Enter.

  Show Configuration Values for Single Object
  Set Configuration Values for Single Object

  Add Configuration Element to a List Object
  Delete Configuration Element from a List Object
  List Configuration Elements in a List Object

  Apply Changes to Configuration Data Base
  Commit Changes to Configuration Data Base
  Reject Uncommitted Changes to Configuration Data Base









F1=Help          F2=Refresh          F3=Previous          F4=SysID
F10=Exit
```

Figure 68. Adapter and Protocol Configuration

Note: It is strongly recommended that these functions not be used to alter the configuration of the 6611 Network Processor as they provide little or no dependency checking or error checking. The 6611 Network Processor configuration program provides much more comprehensive error checking and dependency checking and is therefore preferred under most circumstances.

4.2 TCP/IP Based Management

The 6611 Network Processor, when used with the Multiprotocol Network Program, provides several functions to allow one or more 6611 Network Processors to be managed from a network management system of some kind. All of these functions are based on the TCP/IP protocol suite.

To make use of these network management functions all 6611 Network Processors must be configured to support TCP/IP protocols and one or more TCP/IP hosts must be configured to act as the network management system(s) for the 6611 Network Processors. This is illustrated in Figure 69.

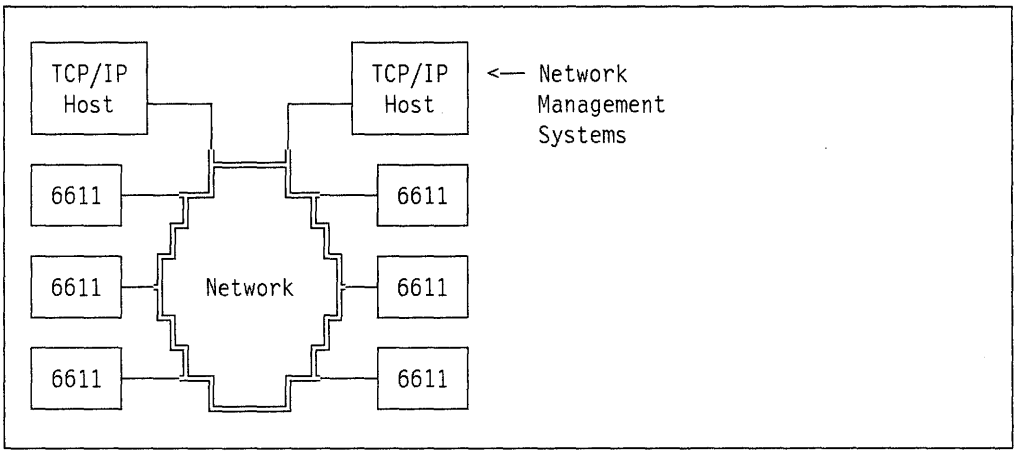


Figure 69. TCP/IP Based Management Configuration

All aspects of the 6611 Network Processor can be managed from a network management system based on a TCP/IP host. This includes those functions of the 6611 Network Processor that are not related to the TCP/IP protocol suite. For example, those aspects of the 6611 Network Processor routing function that relate to the DECnet, XNS, NetWare and AppleTalk protocol suites can all be managed from a network management system based on a TCP/IP host.

The 6611 Network Processor cannot be *directly* managed from a network management system based on a non-TCP/IP host. For example the 6611 Network Processor does not support the network management facilities that are part of the DECnet protocol suite, and therefore cannot be managed directly from a DECnet host using DECnet protocols.

However it is possible to *indirectly* manage the 6611 Network Processor from a network management system based on a non-TCP/IP host. For example the IBM NetView* Program is able to manage 6611 Network Processors indirectly via a suitable service point such as the IBM AIX NetView/6000 with the IBM AIX NetView Service Point. This is illustrated in Figure 70 on page 114.

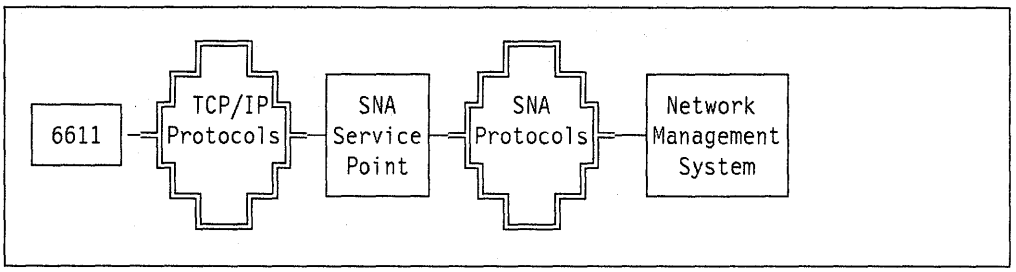


Figure 70. Example of Indirect Management

The capability to manage the 6611 Network Processor indirectly from the IBM NetView Program is described further in 4.2.4, "Using NetView to Manage 6611s via AIX NetView/6000" on page 131.

The TCP/IP capabilities provided by the 6611 Network Processor that can be used for management purposes are:

- SNMP Client and Agent
- TELNET Client and Server
- RLOGIN Client and Server
- REXEC Client and Server
- RSH Client and Server
- FTP Client and Server

Each of these capabilities is described in the following sections.

4.2.1 SNMP

SNMP (Simple Network Management Protocol) is a network management protocol for networks that make use of the TCP/IP protocol suite. SNMP uses a network model that consists of three main elements:

- Managed Objects (things that can be managed)
- Agents (programs that provide an interface to the managed objects)
- Clients (network management systems)

Clients make use of agents to access the managed objects on their behalf. Clients communicate with agents using SNMP.

This is illustrated in Figure 71 on page 115.

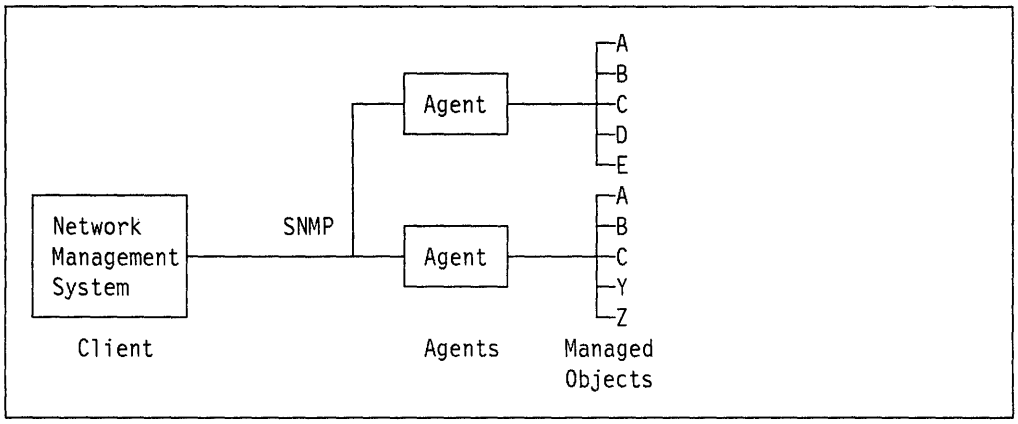


Figure 71. SNMP Network Management Model

The 6611 Network Processor provides an SNMP agent that can be used by SNMP clients to manage objects related to the 6611 Network Processor. The 6611 Network Processor also provides a limited function SNMP client that can be used through the System Manager to access the SNMP agent of the 6611 Network Processor and any other SNMP agents.

4.2.1.1 Management Information Base

Each object that can be managed via an SNMP agent is represented by one or more data values arranged in a data structure called the MIB (Management Information Base). Each data value within the MIB is called a *MIB variable*.

Examples of the types of MIB variables that are supported by the 6611 Network Processor SNMP agent include:

sysContact
: The person responsible for this 6611 Network Processor, together with information on how to contact this person.

sysLocation
: The physical location of this 6611 Network Processor. For example "telephone closet, 3rd floor."

ibmdlsVirtualRingSegmentNumber
: The token-ring segment number used in all frames passed to or from the IBM 6611 Network Processor Data Link Switching function.

A complete list of MIB variable types supported by the 6611 Network Processor SNMP agent is provided in the *IBM 6611 Network Processor: Network Management Reference*.

The structure of the MIB is based on unique *object identifiers*, which are assigned to each type of MIB variable. Object identifiers are specified using ASN.1 (Abstract Syntax Notation One).

Note: ASN.1 is a language developed specifically for the description of data in a manner that is independent of the format used to store that data in a particular device. An understanding of ASN.1 is *not* necessary to make use of the 6611 Network Processor SNMP agent. However some familiarity with object identifiers specified in ASN.1 is necessary to understand the structure of the MIB and configure the 6611 Network Processor SNMP agent.

All valid object identifiers are drawn from the *object identifier namespace*, which is administered by the ISO (International Organization for Standardization) and

CCITT (Comité Consultatif International Télégraphique et Téléphonique). The object identifier namespace is organized in a hierarchical tree structure. A subset of the highest levels of the object identifier namespace tree is illustrated in Figure 72.

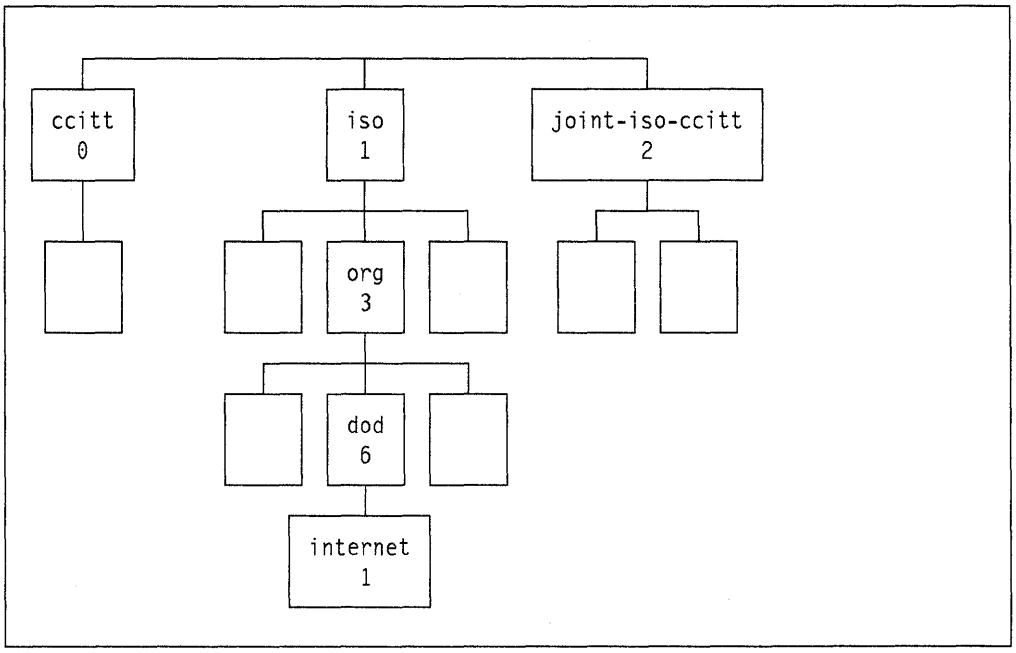


Figure 72. Highest Levels in Object Identifier Namespace Tree

Nodes in the object identifier namespace tree are labeled using both a textual description and a number. These labels are assigned by the administrative authority that is responsible for the *subtree* to which the node belongs.

A *subtree* comprises all nodes beneath a particular node in the tree structure. For example in Figure 72, the "org" node belongs to the subtree beneath the "iso" node, but does not belong to the subtrees beneath the "ccitt" or "joint-iso-ccitt" nodes.

At the highest levels of the object identifier namespace tree, the ISO is responsible for the subtree beneath the "iso" node. The CCITT is responsible for the subtree beneath the "ccitt" node, and they are jointly responsible for the subtree beneath the "joint-iso-ccitt" node.

The ISO has delegated the assignment of labels to the US Department of Defense for the subtree beneath the "dod" node and it, in turn, has delegated the assignment of labels to the Internet Activities Board for the subtree beneath the "internet" node.

All object identifiers assigned to MIB variable types are drawn from the subtree that is beneath the "internet" node. A subset of that subtree is illustrated in Figure 73 on page 117.

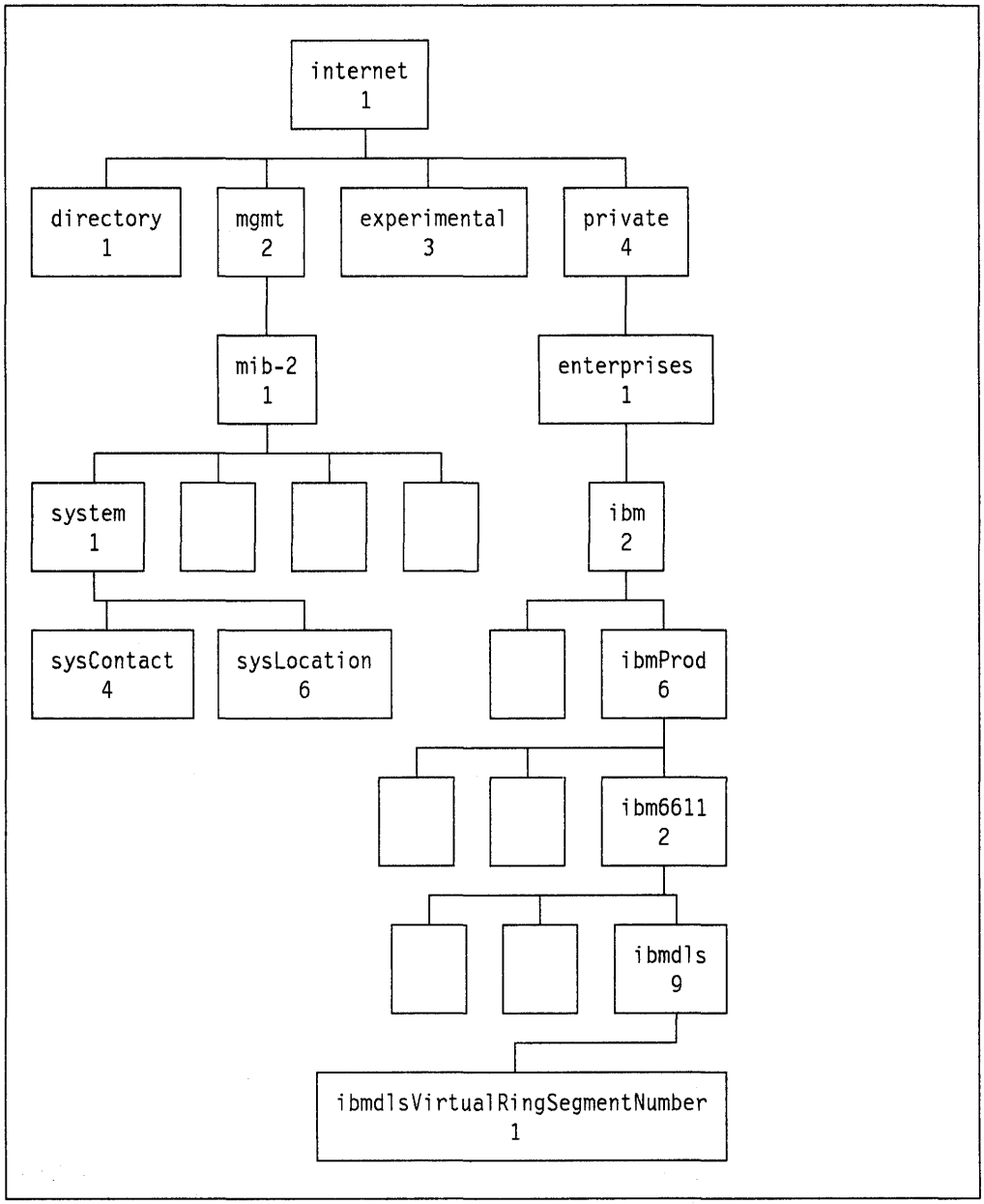


Figure 73. Internet Subtree of Object Identifier Namespace

The Internet Activities Board has delegated the assignment of labels to various other organizations beneath the "enterprises" node in Figure 73. In particular the assignment of labels has been delegated to IBM for the subtree beneath the "ibm" node. It is through this mechanism that object identifiers unique to the 6611 Network Processor can be created without conflicting with any other object identifiers.

Object identifiers are usually written as a series of labels separated by periods, where each label corresponds to a node in the object identifier namespace tree when the tree is traversed from the top of the tree to a node at the bottom of the tree. For example the "sysContact" MIB variable type has an object identifier of:

```
iso.org.dod.internet.mgmt.mib-2.system.sysContact
```

or if written in the more usual form using the numeric labels:

```
1.3.6.1.2.1.1.4
```

All the MIB variable types supported by the 6611 Network Processor have object identifiers that start with either:

iso.org.dod.internet.mgmt.mib-2 (or 1.3.6.1.2.1)

or:

iso.org.dod.internet.private.enterprises.ibm (or 1.3.6.1.4.1.2)

Examples of MIB variable types and their related object identifiers include:

MIB Variable Type	Object Identifier
sysContact	1.3.6.1.2.1.1.4
sysLocation	1.3.6.1.2.1.1.6
ibmdlsVirtualRingSegmentNumber	1.3.6.1.4.1.2.6.2.9.1

The derivation of the object identifiers for all of the above examples can be seen in Figure 72 on page 116 and Figure 73 on page 117.

Each type of MIB variable has one or more instances which can be accessed by SNMP clients via the 6611 Network Processor SNMP agent.

Simple MIB variable types have only a single instance. The object identifier of this single instance is obtained by appending ".0" to the end of the object identifier for the MIB variable type.

For example, the "sysContact" (system contact) MIB variable type is a simple MIB variable type that has only a single instance. The object identifier of the "sysContact" MIB variable type is:

1.3.6.1.2.1.1.4

The object identifier of the single instance is:

1.3.6.1.2.1.1.4.0

Tabular MIB variable types can have multiple instances. Each instance corresponds to an entry in a table. The object identifier for a particular instance is obtained by appending the index for the desired table entry to the end of the object identifier for the MIB variable type.

For example, the "ifDescr" (interface description) MIB variable type is a tabular MIB variable type that can have multiple instances. Each instance of "ifDescr" provides descriptive information about a different interface on the 6611 Network Processor. Together these instances form a table, with each entry in the table describing a different interface. An interface number is used as the index for entries in this table.

The object identifier for the "ifDesc" MIB variable type is:

1.3.6.1.2.1.2.2.1.2

The object identifier for each instance of the "ifDescr" MIB variable type is formed by appending an interface number to the end of the object identifier for the "ifDescr" MIB variable type. For example, descriptive information about the third communication adapter interface would have an object identifier of:

1.3.6.1.2.1.2.2.1.2.3

Not all tabular MIB variable types use simple integer indices like that illustrated by the previous example. More complex indices are often used.

For example, consider the "ipRouteNextHop" MIB variable type. Each instance of "ipRouteNextHop" is the TCP/IP network layer address of the next hop in a route to reach a different TCP/IP destination. Together these instances form a table which reflects the one used by the 6611 Network Processor TCP/IP routing function. A TCP/IP network layer address is used as the index for entries in this table.

The object identifier for the "ipRouteNextHop" MIB variable type is:

```
1.3.6.1.2.1.4.21.1.7
```

The object identifier for each instance of the "ipRouteNextHop" MIB variable type is formed by appending a TCP/IP network layer address to the end of the object identifier for the "ipRouteNextHop" MIB variable type. For example, the next hop to the TCP/IP destination with a network layer address of "9.38.12.11" would have an object identifier of:

```
1.3.6.1.2.1.4.21.1.7.9.38.12.11
```

Authorized SNMP clients are able to examine and change instances of MIB variable types (or more simply *MIB variables*) using SNMP to communicate with the SNMP agent. The SNMP client does this by sending a request to the SNMP agent which processes the request and then sends a response back to the SNMP client.

Note: The 6611 Network Processor SNMP agent only supports requests to examine MIB variables that represent objects related to the 6611 Network Processor. The 6611 Network Processor SNMP agent does not support requests to change MIB variables.

SNMP clients can issue two different types of requests to examine MIB variables:

- GET requests
- GET-NEXT requests

SNMP "get" requests are used to examine instances of simple MIB variable types. For example, an SNMP client can examine the single instance of the "sysContact" MIB variable type by issuing a "get" request for the object identifier:

```
1.3.6.1.2.1.1.4.0
```

SNMP "get-next" requests are used to examine instances of tabular MIB variable types. For example, an SNMP client would examine the first instance of the "ipRouteNextHop" MIB variable type by issuing a "get-next" request for the "ipRouteNextHop" object identifier:

```
1.3.6.1.2.1.4.21.1.7
```

The SNMP agent would return a response that contained the first instance of the "ipRouteNextHop" MIB variable type. The response would also contain the object identifier of this first instance, which would be of the form:

```
1.3.6.1.2.1.4.21.1.7.A.B.C.D
```

where "A.B.C.D" is the index of the first instance.

The SNMP client could obtain the next instance of the "ipRouteNextHop" MIB variable type by sending a second "GET-NEXT" request that contains the object identifier of the first instance. The SNMP agent would return a response that

included the object identifier of the second instance which could be used in a subsequent "GET-NEXT" request to retrieve the third instance. This process could be repeated to retrieve all instances of the "ipRouteNextHop" MIB variable type.

The SNMP protocol also defines a "SET" request that can be used to change MIB variables. However this request is not supported by the 6611 Network Processor SNMP agent (see previous note).

4.2.1.2 SNMP Traps

In certain situations it may be desirable for an SNMP agent to notify an SNMP client of a condition without requiring the SNMP client to first issue a get request to the SNMP agent to examine a MIB variable. In such situations, the SNMP agent can generate a *trap* which will be sent to the SNMP client.

For example, the 6611 Network Processor SNMP agent will generate a trap to indicate that a beaconing condition exists on a Token-Ring Network attached to the 6611 Network Processor.

The 6611 Network Processor SNMP agent can generate the following traps defined by the SNMP:

coldStart
: Indicates the 6611 Network Processor is reinitializing itself in a way which may change the configuration or implementation of the SNMP agent. Therefore an SNMP client cannot depend on any previous knowledge of the SNMP agent.

warmStart
: Indicates the 6611 Network Processor is reinitializing itself in a way which does not change either the configuration or the implementation of the SNMP agent.

linkDown
: Indicates that a communication interface on the 6611 Network Processor is no longer operational. The trap contains information that identifies the communication interface.

linkUp
: Indicates that a communication interface on the 6611 Network Processor is now operational. The trap contains information that identifies the communication interface.

authenticationFailure
: Indicates that the 6611 Network Processor SNMP agent received an SNMP request from an SNMP client that was not authorized to make the request. Authentication is described further in 4.2.1.3, "SNMP Access Control" on page 122.

egpNeighborLoss
: Indicates that a connection to an EGP (Exterior Gateway Protocol) neighbor is down. The trap contains information that identifies the EGP neighbor.

enterpriseSpecific
: Used to indicate a condition has occurred which cannot be indicated by the other types of SNMP traps.

Each trap contains an *enterprise object identifier* to uniquely identify the type of SNMP agent that generated the trap. Enterprise object identifiers are defined in the same manner as the object identifiers used for MIB variable types using the *object identifier namespace*. This is described in 4.2.1.1, "Management Information Base" on page 115. The 6611 Network Processor SNMP agent uses either:

```
iso.org.dod.internet.private.enterprises.ibm.ibmprod.ibm6611
```

or:

```
iso.org.dod.internet.private.enterprises.ibm.ibmprod.ibm6611.ibmfr
```

as the enterprise object identifier in traps that it generates. When written in the more usual numeric form the two enterprise object identifiers used by the 6611 Network Processor SNMP agent are:

```
1.3.6.1.4.1.2.6.2 (iso.org  ...  ibmprod.ibm6611)
```

and:

```
1.3.6.1.4.1.2.6.2.8 (iso.org  ... ibmprod.ibm6611.ibmfr)
```

The "enterpriseSpecific" trap also contains a *specific trap number*. The specific trap number and the enterprise object identifier, when used together, distinguish between the many possible conditions that can be indicated by the "enterpriseSpecific" trap. The "enterpriseSpecific" trap conditions that can be generated by the 6611 Network Processor SNMP agent are listed below. The last part of the enterprise object identifier ("ibm6611" or "ibm6611.ibmfr") and the specific trap number are listed in parenthesis after each trap:

DSU/CSU: Link alarm (ibm6611 1)
DSU/CSU: Test improperly requested at DSU/CSU (ibm6611 2)
DSU/CSD: Loss of signal (ibm6611 3)
DSU/CSU: Out of frame error (ibm6611 4)
DSU/CSU: Errored seconds threshold exceeded (ibm6611 5)
DSU/CSU: Loss of clock (ibm6611 6)
DSU/CSU: Unknown error code (ibm6611 7)
DSU/CSU: Equipment failure (ibm6611 8)
SDLC Adapter: Transmit failsafe timeout (ibm6611 9)
X.21: Unexpected clear during call establishment (ibm6611 10)
X.21: Unexpected clear during data transfer (ibm6611 11)
SNMP: Configuration file open error (ibm6611 15)
SNMP: Bad configuration parameter (ibm6611 16)
SNMP: TCP/IP failure (ibm6611 17)
SNMP: Kernel resource problem (ibm6611 18)
SNMP: MIB-related problem (ibm6611 19)
SNMP: SNMP agent or subagent terminated by user (ibm6611 20)
Token Ring: Beaconing (ibm6611 21)
2-Port Serial Adapter: Clear to Send Inactive (ibm6611 22)
Frame Relay: DLCI State Change (ibm6611.ibmfr 1)

When the 6611 Network Processor SNMP agent generates a trap, more detailed information is logged in the 6611 Network Processor error log. The System Manager can be used to access this information if it is required to resolve a condition that has been indicated by a trap.

The "enterpriseSpecific" traps generated by the 6611 Network Processor SNMP agent contain a reference to the error log entry that provides more information on the condition that caused the trap to be generated. This reference can be

used with the "View an Error Report for a Single Sequence Number" option of the "Problem Determination Facilities" System Manager menu to retrieve the correct error log entry. Traps other than "enterpriseSpecific" do not contain this reference as there is no provision within SNMP to provide this capability.

Additionally, the "enterpriseSpecific" traps generated by the 6611 Network Processor SNMP agent contain information that is compatible with the IBM SNA Management Services architecture. The enables "enterpriseSpecfic" traps to be converted into SNA MSUs (Management Services Units) by an SNA service point for forwarding to an SNA Management Services focal point such as the IBM NetView Program. This is described further in 4.2.4, "Using NetView to Manage 6611s via AIX NetView/6000" on page 131.

4.2.1.3 SNMP Access Control

The SNMP provides a simple access control capability that can be used to limit the access SNMP clients have to SNMP agents.

Each request sent from an SNMP client to an SNMP agent contains a *community name*. The SNMP agent verifies that the community name contained within the request is authorized to make the request before processing the request. If the request is not authorized, an "authenticationFailure" trap is generated by the SNMP agent and the request is not processed.

The 6611 Network Processor SNMP agent performs several checks based on the community name before granting a request from an SNMP client. These include:

- That the community name is known to the 6611 Network Processor SNMP agent.
- That the TCP/IP network layer address of the SNMP client that sent the request matches that specified for this community name. A mask capability is provided to allow a range of addresses to match the address specified. Only those bits set in the mask are used for the comparison.
- That a sufficient access level has been specified for this community name. The access levels supported by the 6611 Network Processor SNMP agent are "readOnly" and "none." SNMP get or get-next requests will only be granted if "readOnly" access has been specified for the community name. SNMP set requests will always be rejected by the 6611 Network Processor.
- That the MIB variable required by the request is contained within the *view* specified for this community name. A *view* is a subset of the MIB.

A community name is also included in any trap generated by the 6611 Network Processor agent. A different community name can be specified for each SNMP client to which traps are sent by the 6611 Network Processor SNMP agent.

Community names, and the access capabilities associated with each name are defined when the 6611 Network Processor is configured. This is described further in 4.2.1.5, "Configuration of SNMP" on page 125.

4.2.1.4 SNMP Client

The 6611 Network Processor provides an SNMP client capability which can be accessed through the System Manager. The SNMP client can be used to examine the MIB variables for a 6611 Network Processor using the services of its SNMP agent.

The SNMP client can also be used to examine MIB variables of many other devices that provide an SNMP agent.

The SNMP client makes use of MIB modules to make it easier for a System Manager user to examine MIB variables. MIB modules are the ASN.1 definitions for the MIB variable types supported by SNMP agents. A System Manager user can use symbolic labels to request groups of MIB variables without requiring a detailed knowledge of ASN.1.

The 6611 Network Processor provides a wide range of MIB modules that can be used in conjunction with the 6611 Network Processor agent. Each MIB module contains definitions for MIB variables that are contained within a subtree of the object identifier namespace. MIB modules are provided that can be used with both IBM and non-IBM SNMP agents.

The following example illustrates the use of the SNMP client provided by the 6611 Network Processor. To access the SNMP client from within the System Manager the "View Network Management Information" option should be selected from the "Performance and Statistics Menu." The screen illustrated in Figure 74 will be displayed.

```
                                                                routera
                          Performance and Statistics
Mo┌──────────────────────────────────────────────────────────────────┐
  │                          MIB module to be viewed                 │
  │                                                                  │
  │ Move cursor to desired item and press Enter.                     │
  │                                                                  │
  │ [TOP]                                                            │
  │   IBM_6611 Complete MIB                                          │
  │   ACC MIB                                                        │
  │   Cabletron_EMM MIB                                              │
  │   Cabletron_HUB MIB                                              │
  │   Chipcom MIB                                                    │
  │   Cisco_R8.0 MIB                                                 │
  │   HP MIB                                                         │
  │   Novell MIB                                                     │
  │   Proteon MIB                                                    │
  │   Synoptics MIB                                                  │
  │ [MORE...9]                                                       │
  │                                                                  │
  │ F1=Help                 F2=Refresh              F3=Previous      │
  │ F7=Page Up              F8=Page Down            F10=Exit         │
F1└──────────────────────────────────────────────────────────────────┘
```

Figure 74. MIB Module Selection

The screen illustrated in Figure 74 lists the MIB modules that can be used by the SNMP agent. In this example the "IBM 6611 Complete MIB" module has been selected. When "Enter" is pressed the "View Network Management Information" screen is displayed as illustrated in Figure 75 on page 124.

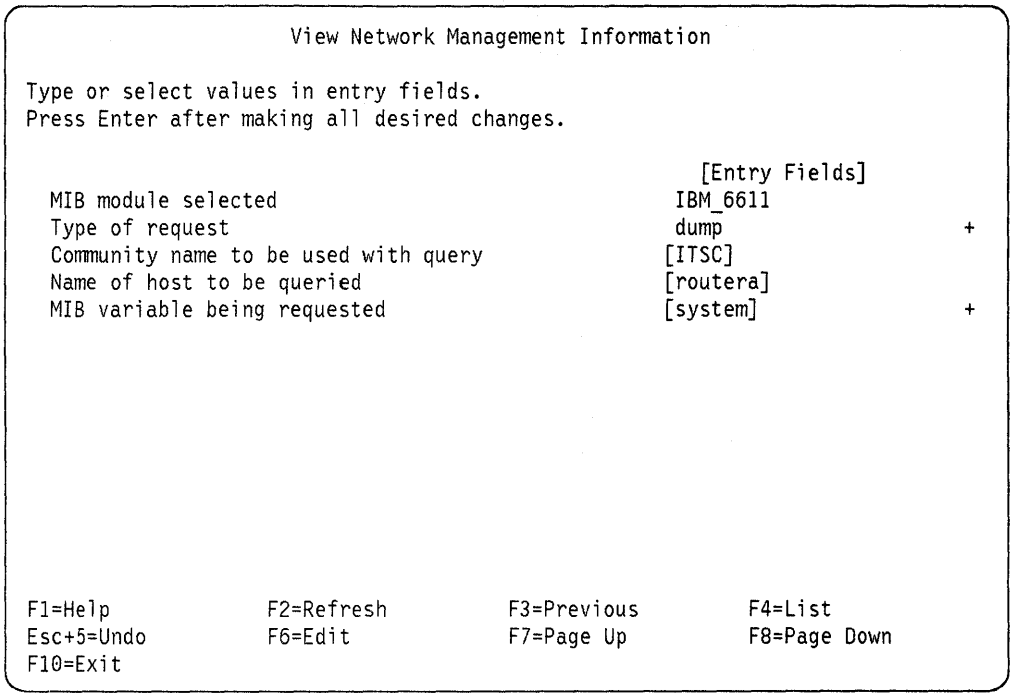


Figure 75. View Network Management Information Screen

The SNMP client provides three types of requests:

get Returns a single MIB variable using an SNMP "GET" request containing the object identifier for the MIB variable specified in the "MIB variable being requested" field.

next Returns a single MIB variable using an SNMP "GET-NEXT" request containing the object identifier for the MIB variable specified in the "MIB variable being requested" field.

dump Returns all MIB variables that are in the subtree below the object identifier specified in the "MIB variable being requested" field. The dump is obtained by the SNMP client from the SNMP agent by issuing a repeated sequence of SNMP "get-next" requests.

A list of valid MIB variables that are contained in the MIB module that is being used is available using the "List" function key (function key F4 in the example illustrated in Figure 75).

In this example a dump has been requested of all MIB variables contained within the "system" MIB subtree. The "system" MIB subtree comprises all MIB variables that have object identifiers that start with "1.3.6.1.2.1.1." The SNMP agent to which the request is to be sent is "routera" and the community name to be sent in the request is "ITSC." The use of community names is described further in 4.2.1.3, "SNMP Access Control" on page 122.

The output produced by the request sent to the SNMP agent of "routera" is illustrated in Figure 76 on page 125.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

sysDescr.0 = "IBM 6611 Network Processor 170 Serial Number: 26-06620
Software: Multiprotocol Network Program (5648016) 01.01.15"
sysObjectID.0 = ibm6611 (1.3.6.1.4.1.2.6.2)
sysUpTime.0 = 19 hours, 21 minutes, 53.99 seconds (6971399 timeticks)
sysName.0 = "routera.itsc.raleigh.ibm.com"
sysLocation.0 = "ITSC Raleigh LAB"
sysServices.0 = 0xe<datalink/subnetwork,internet,transport>




F1=Help             F2=Refresh          F3=Previous         F7=Page Up
F8=Page Down        F10=Exit
```

Figure 76. Dump of System MIB Subtree

The 6611 Network Processor provides MIB modules that can be used by other SNMP clients to aid in accessing the 6611 Network Processor SNMP agent. These MIB modules are contained in the static directory and can be transferred to the network management system using either FTP, XMODEM, DOS diskettes or UNIX diskettes.

4.2.1.5 Configuration of SNMP

The 6611 Network Processor SNMP agent must be configured before it can be used by SNMP clients. To configure the 6611 Network Processor SNMP agent the following information should be defined that is specific to SNMP:

System contact
: The person responsible for the 6611 Network Processor along with information on how to contact this person. This value will be accessible via the "sysContact" MIB variable (1.3.6.1.2.1.1.4.0).

System location
: The physical location of the 6611 Network Processor. This value will be accessible via the "sysLocation" MIB variable (1.3.6.1.2.1.1.6.0).

System name
: A name for this 6611 Network Processor. By convention this is usually made the same as the TCP/IP fully qualified domain name. This value will be accessible via the "sysName" MIB variable (1.3.6.1.2.1.1.5.0).

Enterprise specific trap throttle time
: Controls the throttling of "enterpriseSpecific" traps. The SNMP agent will not generate consecutive "enterpriseSpecific" traps that have the same enterprise object identifier and specific trap number within the time period specified by this configuration parameter.

Router serial number
: The serial number of this 6611 Network Processor. This value will be accessible as part of the "sysDescr" MIB variable (1.3.6.1.2.1.1.1.0).

Define traps

Defines where to send traps. This comprises a list of SNMP clients to which traps should be sent. The types of traps that should be sent to each SNMP client can also be specified along with a community name to be placed in each trap sent.

Define views

Defines subsets of the MIB which can be used to limit access by SNMP clients. Each view is defined by a list of object identifier prefixes which are called *MIB subtrees*. The view comprises all MIB variables that have object identifiers that contain one of the object identifier prefixes.

Define communities

Defines the communities that can use the SNMP agent of this 6611 Network Processor. The access of each community is limited to MIB variables that are contained within a view that is defined using "Define views."

Configuration of the 6611 Network Processor is described further in Chapter 3, "Configuring the 6611" on page 55. The SNMP configuration parameters are described further in *IBM Multiprotocol Network Program: User's Guide*.

4.2.2 Other TCP/IP Facilities

The 6611 Network Processor provides several other TCP/IP facilities in addition to the SNMP agent that can be used for management purposes. Both a client and server are provided for each of these facilities.

The servers can be used to support remote access by a network management system (running on a TCP/IP host) to a 6611 Network Processor. The clients can be used from the 6611 Network Processor System Manager to allow it to remotely access other 6611 Network Processors or TCP/IP hosts that are operating the corresponding servers. Each of these facilities is described in the following sections.

4.2.2.1 TELNET and RLOGIN

The 6611 Network Processor provides TELNET and RLOGIN (Remote Login) servers. These servers (also known as TELNETD and RLOGIND) allow a TELNET or RLOGIN client running on a TCP/IP host to remotely access the full-screen or command-line interfaces of the 6611 Network Processor System Manager.

The 6611 Network Processor also provides TELNET and RLOGIN clients. Either client can be started while using the System Manager and each client enables a user of the System Manager to remotely access applications on other TCP/IP hosts that provide TELNET or RLOGIN servers. These other TCP/IP hosts could be 6611 Network Processors.

TELNET and RLOGIN provide very similar capabilities; however, RLOGIN can eliminate the need to enter a *userid* and password under some circumstances.

When using a serial port of a 6611 Network Processor to access the System Manager from a computer emulating an ASCII display station, RLOGIN is the preferred method for accessing other 6611 Network Processors via the System Manager of the first 6611 Network Processor. This is because RLOGIN will support file transfers using XMODEM directly from remote 6611 Network

Processors to the computer emulating an ASCII display station, whereas TELNET will not.

4.2.2.2 REXEC and RSH

The 6611 Network Processor provides REXEC (Remote Execution) and RSH (Remote Shell) servers. These servers (also known as REXECD and RSHD) allow a REXEC or RSH client running on a TCP/IP host to remotely access the command-line interface of the 6611 Network Processor System Manager.

For example a 6611 Network Processor ("routera") could be shut down remotely from a TCP/IP host and then restarted using a REXEC command of the form:

```
rexec routera shutdown_soon_ipl 0
```

The user would be prompted to enter a valid 6611 Network Processor *userid* and password before the shutdown command was executed.

Alternatively the following RSH command could be used to achieve the same result:

```
rsh routera -l kellyjp bart shutdown_soon_ipl 0
```

When using RSH a valid 6611 Network Processor *userid* (for example "kellyjp") and password (for example "bart") must be specified with the RSH command.

If the current *userid* being used to issue the RSH command on the TCP/IP host is the same as a valid 6611 Network Processor *userid*, the 6611 Network Processor *userid* need not be specified on the RSH command as illustrated by the following example:

```
rsh routera bart shutdown_soon_ipl 0
```

Note: The syntax used to access a 6611 Network Processor using RSH is different from that used when accessing other TCP/IP hosts using RSH. Specifically the 6611 Network Processor syntax includes a password immediately before the command to be executed whereas the syntax normally used by RSH has no password. This is because TCP/IP hosts use a different authentication scheme for RSH that is based on entries in configuration files.

The 6611 Network Processor also provides REXEC and RSH clients. Either client can be started while using the System Manager and each client enables a user to remotely access the System Manager command-line interface on other 6611 Network Processors.

RSH and REXEC provide very similar capabilities. The main difference between RSH and REXEC is REXEC will prompt for a *userid* and password, whereas RSH expects that a *userid* and password are provided as part of the RSH command.

Therefore REXEC is preferred when issuing commands interactively and RSH is preferred when issuing commands from within scripting languages.

4.2.2.3 FTP

The 6611 Network Processor provides a FTP (File Transfer Protocol) server. This server (also known as FTPD) allows an FTP client running on a TCP/IP host to transfer files to and from the 6611 Network Processor.

For example a configuration for a 6611 Network Processor can be transferred to a 6611 Network Processor from a TCP/IP host via this facility. Alternatively the

output of a 6611 Network Processor problem determination facility can be transferred from a 6611 Network Processor to a TCP/IP host.

The 6611 Network Processor also provides an FTP client. The client can be started while using the System Manager and enables a user of the System Manager to transfer files to and from other TCP/IP hosts that provide an FTP server. These other TCP/IP hosts could be 6611 Network Processors.

4.2.2.4 Configuration of TCP/IP Facilities

To make use of the TCP/IP based management facilities provided by the 6611 Network Processor, various parameters must first be configured.

Many of these configuration parameters make use of TCP/IP host names. TCP/IP host names provide a convenient way of referring to the TCP/IP network layer addresses of TCP/IP hosts.

When setting up a network that uses TCP/IP protocols, it is usual to assign a host name to each device that participates in TCP/IP protocols. It therefore follows that devices such as the 6611 Network Processor would be assigned a host name.

These host names can be used by the various TCP/IP based management facilities wherever a TCP/IP network layer address for a TCP/IP host could normally be used. For example, to initiate a TELNET connection to a 6611 Network Processor that has a TCP/IP network layer address of "9.67.38.78" the following command could be used:

```
TELNET 9.67.38.78
```

If this 6611 Network Processor had been assigned a host name of "routerb," the following command could be used instead:

```
TELNET routerb
```

Large networks that use TCP/IP protocols use more complex host names. Such networks are divided into many administrative domains. Each administrative domain is responsible for the assignment of host names for TCP/IP hosts under their control.

Each administrative domain has a domain name, which can be added to the end of the name of a TCP/IP host to produce a fully qualified host name. For example, if the name "routerb" used in the previous example was assigned by the administrative domain named "itsc.raleigh.ibm.com," the fully qualified name would be:

```
routerb.itsc.raleigh.ibm.com
```

In order to make effective use of the TCP/IP based management facilities provided by the 6611 Network Processor the following parameters should be configured:

Host Name
: The name that will be used for this 6611 Network Processor, for example, "routerb."

Domain Name
: The name of the administrative domain which was responsible for issuing the host name assigned to this 6611 Network Processor, for example, "itsc.raleigh.ibm.com."

SNMP

Various parameters required for the correct operation of the SNMP agent. These have been described in 4.2.1.5, "Configuration of SNMP" on page 125.

Users of System Manager

userids and passwords that can be used to access the System Manager via TELNET, RLOGIN, RSH or REXEC.

Configuration Hosts

Defines TCP/IP hosts that can update the configuration of the 6611 Network Processor using the 6611 Network Processor configuration program. This capability is only available when the configuration program is used on an IBM RISC System/6000.

Remote Host Names

Defines various TCP/IP host names and their corresponding TCP/IP network layer addresses. Host names can be used in place of TCP/IP network layer addresses for many 6611 Network Processor System Manager functions.

Name Servers

Defines name servers that can be used by the 6611 Network Processor to resolve TCP/IP names. Name servers translate TCP/IP names into TCP/IP network layer addresses. Name servers can be used as an alternative to defining remote host names. The 6611 Network Processor will query the name server whenever it needs to translate a host name into TCP/IP network layer addresses if it can not find the host name in the remote host name table.

Time Servers

Defines time servers that can be used by the 6611 Network Processor to update its internal clock. Time servers provide an accurate time service which can be used by many TCP/IP hosts including the 6611 Network Processor. If the time is changed on the time server (for example to change to summer time), the internal clock in 6611 Network Processors using the time server will automatically be updated to reflect the time change.

Configuration of the 6611 Network Processor is described further in Chapter 3, "Configuring the 6611" on page 55.

4.2.3 Using AIX NetView/6000 to Manage 6611s

IBM AIX NetView/6000 (5765-077) is a program for the IBM RISC System/6000 to facilitate the management of networks that make use the TCP/IP protocol suite. AIX NetView/6000 provides SNMP client functions that can be used to manage various SNMP agents, including the SNMP agent that is implemented by the 6611 Network Processor. This is illustrated in Figure 77 on page 130.

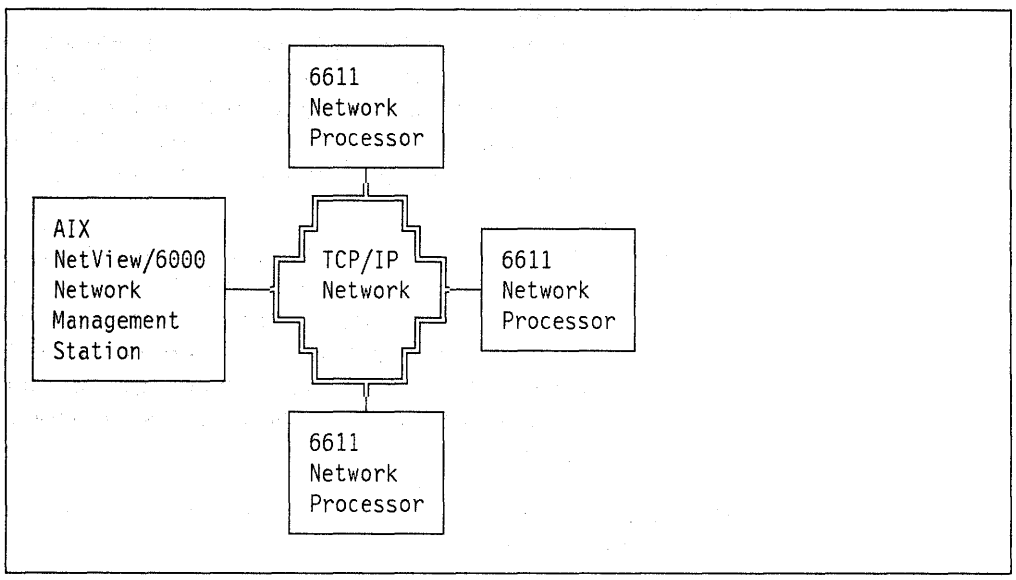


Figure 77. Using AIX NetView/6000 to Manage 6611s via TCP/IP Network

AIX NetView/6000 features a graphical, object-oriented user interface which provides a highly productive environment for the management of networks based on the 6611 Network Processor and other devices that implement SNMP agents. Other features of AIX NetView/6000 include:

Dynamic Network Discovery and Mapping

The TCP/IP network and its resources are automatically discovered and monitored by AIX NetView/6000. This information is presented as graphical maps which are automatically generated by AIX NetView/6000 for viewing by network operators. The maps indicate the type and status of each component of the network using icons of various shapes and colors respectively. Further information about any network component is readily available by selecting the icon representing that component using the mouse and selecting the information required using pull-down menus.

MIB Loader

Various MIB modules (such as those provided with the 6611 Network Processor) can be loaded by AIX NetView/6000 to provide easy access to, and interpretation of, the MIB variables managed by any SNMP agent.

MIB Browser

The MIB variables of any SNMP agent can be interactively browsed using the MIB browser component of AIX NetView/6000 which makes use of MIB modules that have been loaded previously by the MIB loader. The MIB browser allows network operators to quickly locate the information they need.

MIB Application Builder

Tabular and graphical displays of particular MIB variables can be developed without programming using the MIB application builder component of AIX NetView/6000. Once defined, these displays can be accessed using the AIX NetView/6000 pull-down menus for any network component. For example, a graphical display of the t ffic being processed by a 6611 Network Processor can be developed in just a few minutes using this facility.

MIB Data Collector

MIB variables can be periodically retrieved by AIX NetView/6000 from network components (such as the 6611 Network Processor) and collected in a file for comparison with user definable thresholds. If the thresholds have been exceeded, AIX NetView/6000 can generate an *event* (see below) indicating that a problem exists.

Event Configurator

SNMP traps received by AIX NetView/6000 and various other situations create an *event*. The AIX NetView/6000 event configurator allows network administrators to specify the actions that should be taken when events occur. For example, the network administrator can specify what text is displayed, how the status of the network component should be effected and what automation routines should be run for each type of event.

For further information on AIX NetView/6000 refer to *AIX Netview/6000 at a Glance* (GC31-6175).

4.2.4 Using NetView to Manage 6611s via AIX NetView/6000

The IBM NetView Program can be used in conjunction with AIX NetView/6000 to centrally manage a network of 6611 Network Processors. This is illustrated in Figure 78.

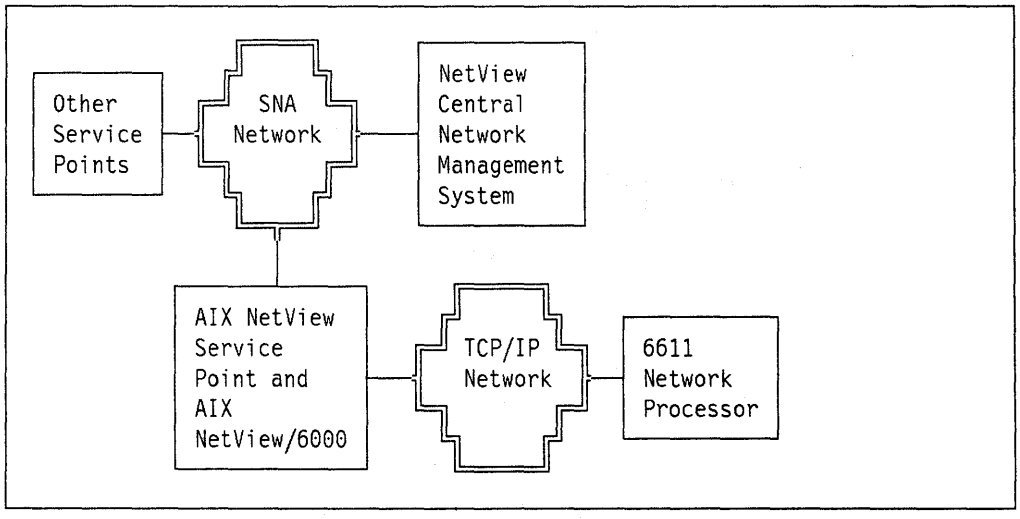


Figure 78. Using NetView to Manage 6611s Via AIX NetView/6000

To support this configuration, an SNA network connection must exist between the NetView system and the IBM RISC System/6000 running AIX NetView/6000. Additionally the IBM AIX NetView Service Point must be installed on the IBM RISC System/6000 to support communication between NetView and AIX NetView/6000.

AIX NetView/6000 can be configured to translate *events* into *alerts* which will then be forwarded via the AIX NetView Service Point to NetView. Upon receipt of these alerts, NetView can display them to network operators or evoke automation routines.

For example, when a 6611 Network Processor generates an SNMP trap and sends it to AIX NetView/6000 an event will be created. A network operator using

NetView will see this event if AIX NetView/6000 has been configured to convert the event into an alert for forwarding to NetView.

NetView automation routines or network operators using NetView can send commands back to AIX NetView/6000 via the AIX NetView Service Point using the NetView *RUNCMD* facility. These commands can be used to control TCP/IP network devices such as the 6611 Network Processor.

For example, a network operator using NetView can access the 6611 Network Processor System Manager command-line interface using the NetView RUNCMD facility to issue a RSH command. This is illustrated by the following example which shuts down a 6611 Network Processor and then immediately restarts it:

```
RUNCMD SP=puname,APPL=spappl,rsh routera -l kellyjp bart shutdown_soon_ipl 0
```

In this example "puname" is the SNA PU name of the IBM RISC System/6000 running AIX NetView Service Point, and "spappl" is the name assigned to the AIX NetView/6000 service point application.

4.3 IBM LAN Network Manager (LNM) Considerations

This section describes the implications and possibilities of managing LANs that have 6611 Network Processors.

The IBM LAN Network Manager V1.0 is an OS/2-based LAN management product. The LAN can be comprised of many segments bridged together. Up to 255 segments can be managed by the IBM LAN Network Manager V 1.0. The IBM LAN Network Manager links to the different bridges to build its view of the whole LAN.

With the IBM 6611 Network Processor, source route bridging is supported locally, remotely to another 6611 Network Processor and to an IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R).

The 6611 Network Processor does not have any network management server components; Configuration Report Server (CRS), Ring Error Monitor (REM), Ring Parameter Server (RPS), LAN Reporting Mechanism (LRM) and LAN Bridging Server (LBS) available as are present in the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R).

LAN Network Manager cannot link to a 6611 Network Processor, when it is operating as part of a 6611 Network Processor-to-6611 Network Processor native bridge configuration, or when it is part of a 6611 Network Processor-to-IBM Token-Ring Network Bridge Program Version 2.2 (compatibility mode). However, the IBM LAN Network Manager Version 1.0 can link to the IBM Token-Ring Network Bridge Program Version 2.2 half when the 6611 Network Processor is operating in compatibility mode. In order for the IBM LAN Network Manager to manage those remote segments that are bridged to the 6611 Network Processor in bridge compatibility mode, the IBM Token-Ring Network Bridge Program Version 2.2 **must** have PTF UR37051 installed. In addition, the IBM LAN Network Manager **must** have PTF UR37165 installed.

Management of the media cannot be done by the IBM LAN Network Manager for the remote segments that are bridged by the 6611 Network Processor when operating in native bridge mode.

4.3.1 Normal LAN Management of a Bridged LAN

Normal interactions between the IBM LAN Network Manager V1.0 and the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) to manage these bridged segments is as follows:

Bridge Link

When LAN Network Manager activates *Link Bridge* it will send out an All-Routes Broadcast LLC TEST frame to SAP X'00' of the bridge adapter. See Figure 79. The bridge adapter responds also with a TEST frame. At this time the LAN Network Manager will start the link process with a UI frame containing a request to Set Reporting Link. The bridge then sends the SABME (Set Asynchronous Balanced Mode Extended) frame, meaning the bridge has accepted the Reporting Point request of LAN Network Manager. LNM responds with a UA (Unnumbered Acknowledge) frame after which the link is operational. RR (Receive Ready) frames will now travel as link verification tests whenever there is no traffic on the link.

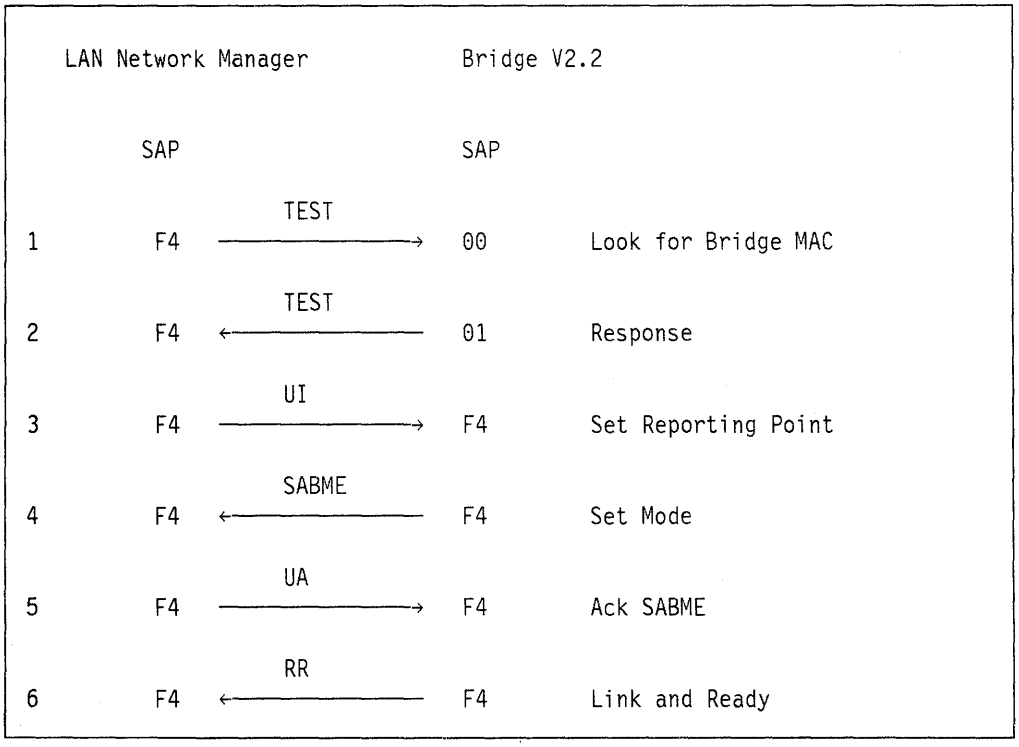


Figure 79. LAN Network Manager Link to a Bridge

Bridge Interaction

Once the link is set up, LAN Network Manager will interact with the Bridge Program and request the *Bridge Status*, the *Ring Error Monitor* (REM) status and set the *Bridge Parameters*. See Figure 80 on page 135. In order to report all these parameters to LNM, the bridge has several management servers:

LRM - LAN Reporting Mechanism

The LAN Reporting Mechanism controls the communication between the LAN Network Manager and the management servers (CRS, REM, RPS, LBS).

CRS - Configuration Report Server

The Configuration Report Server sends notifications about the current active configuration of each LAN segment (a bridge always has two segments) to the LAN Network Manager that requests it. It collects NAUN (Nearest Active Upstream Neighbor) address changes that occur on the LAN segment.

REM - Ring Error Monitor

The Ring Error Monitor receives and analyzes error frames as sent by the adapters on either segment and sends reports to indicate critical problems to the linked-to LAN Network Manager.

RPS - Ring Parameter Server

The Ring Parameter Server provides the LAN segment number to an adapter when the adapter is inserting into the LAN segment.

LBS - LAN Bridge Server

The LAN Bridge Server keeps statistical information about frames forwarded between two or more rings (through a bridge) and sends this information to the appropriate LAN Network Managers.

For a detailed description of these LAN Management servers see *IBM Token-Ring Network Architecture Reference SC30-3374*.

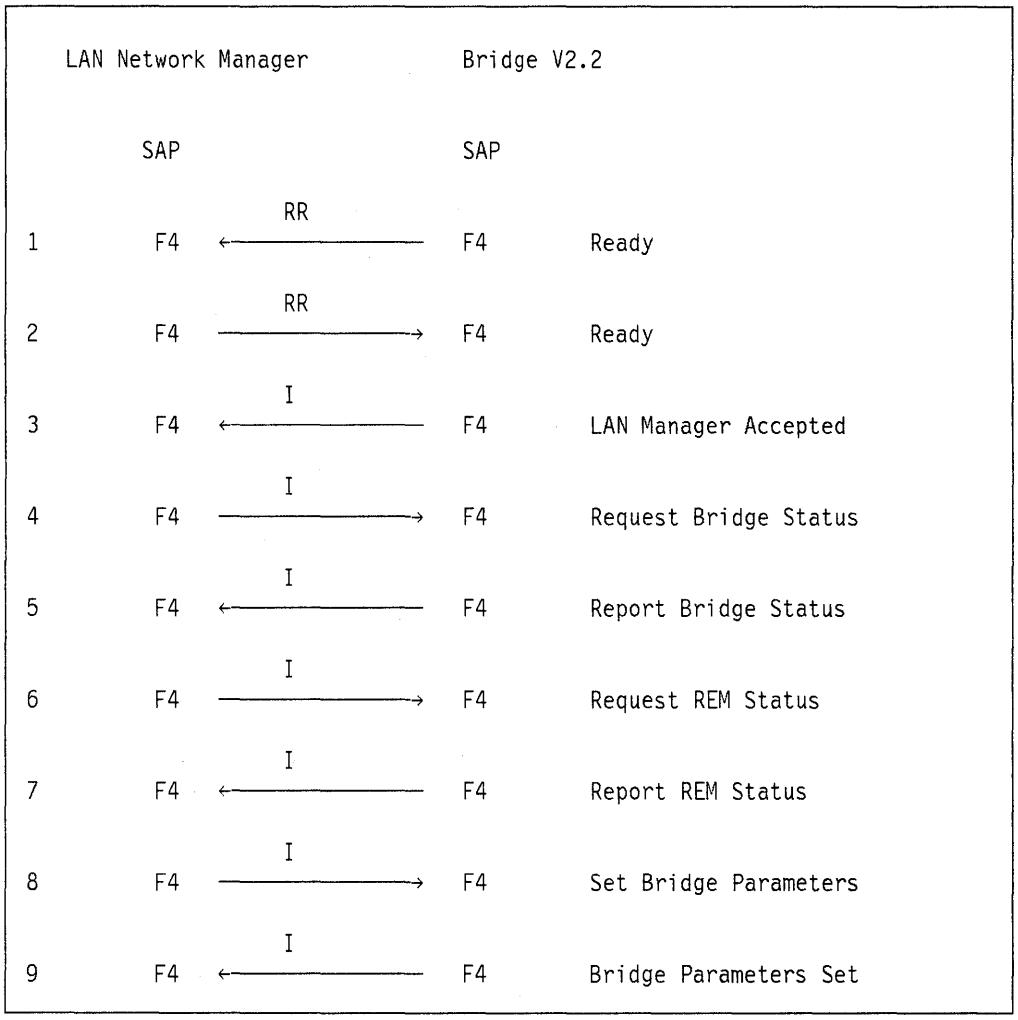


Figure 80. LAN Network Manager Link to a Bridge

8230 Controlled Access Unit Interaction

An IBM 8230 supports registration with one Controlling LAN Network Manager. After the Controlled Access Unit is registered, the LNM can do the following:

- Set the password
- Enable and disable lobe receptacles and attachment modules
- Reset the CAU
- Change the wrap state of the CAU
- Control access to the LAN via the CAU

4.3.2 LNM Support for Local and Remote 6611-to-6611 Bridging

LNM PTF UR 37165 will offer LAN Network Manager support for 8230s and 8220s on the bridged ring segments.

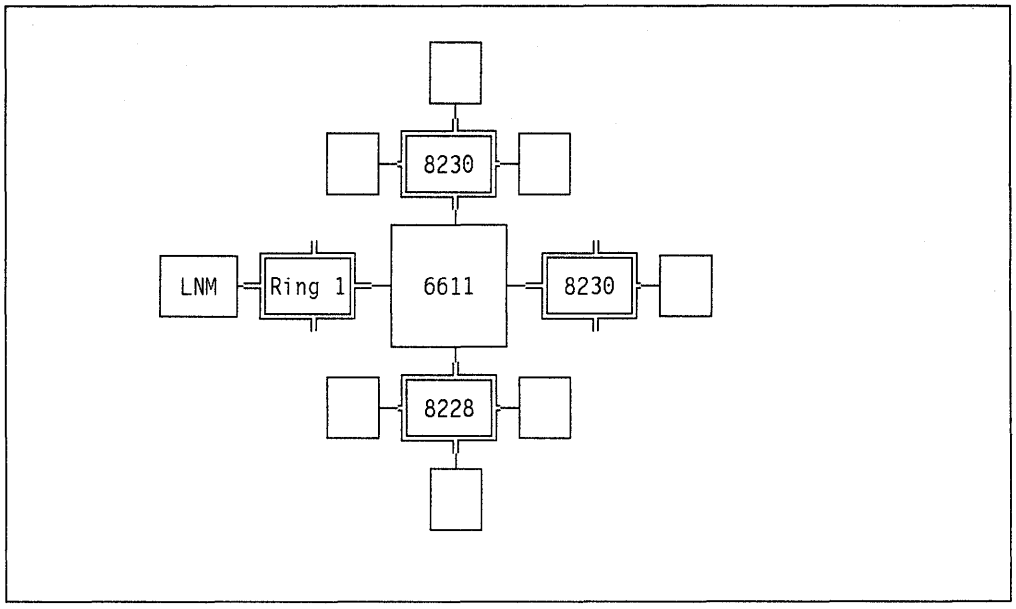


Figure 81. LNM Support of a Local Source Route Bridged LAN

4.3.2.1 LNM Support for 8230s

LAN Network Manager manages 8230s on remote segments by registering with them. To that end, LAN Network Manager must verify that the ring number to which the Controlled Access Units are attached are part of it's **managed domain**. The LAN Network Manager normally discovers the ring numbers by linking to the bridges that connect to them. LAN Network Manager **cannot** link to the 6611 Network Processor bridge function. A new 8230 *Qualifier* has been defined to enable the LNM to manage the Controlled Access Units (CAU) in this 6611 Network Processor native bridging mode. See Figure 82 on page 137. The new qualifier value is the ring number for the token ring segment as defined by the 6611 Network Processor. Also the possibility to *register* and *deregister* a highlighted CAU is available now.

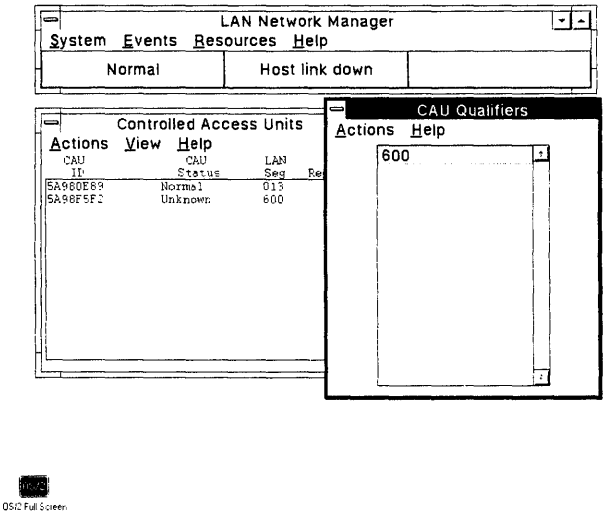


Figure 82. New CAU User Interface on LNM

When LAN Network Manager initializes it will send a CMIP INVOKE ACTION Register Check frame out as a Single-Route Broadcast frame. Inside the CMIP frame will be a field for a segment number. The LAN Network Manager has filled that field in with the segment number of a 'managed' segment. A managed segment is one that is known to the LAN Network Manager, either because it is the local segment that it is on or it is a segment known to a bridge that it is linked to.

This frame will cross all bridges in the network capable of forwarding Single-Route Broadcast frames. The CMIP INVOKE frame is addressed to the X'C000 0000 1000' address which is the Ring Wiring Concentrator functional address. This address is opened by all IBM 8230s and is used to discover all Controlled Access Units. If the CMIP frame that arrives on the segment with an 8230 has a ring number in it for different segment than the segment that the 8230 is on the 8230 will not register with this LAN Network Manager.

When the LAN Network Manager user sets the **qualifier** a CMIP frame will go out that contains the qualified ring segment number. When this new frame is received by the CAU, the segment inside the CMIP frame matches the segment number the CAU knows it is on and the registration process continues. How does the CAU know what segment number it is on if there is no Ring Parameter Server function present on the segment? When the CAU receives the CMIP frame, it examines the Routing Information Field portion of the frame. In that field is the segment number that the CAU is on. See Figure 83 on page 138 below and Figure 84 on page 139 for traces of a frame without, and one with, a qualifier set. The ring number is hidden in the data block and highlighted.

```
Frame number. . . . . 3          Time stamp . . . . .16:26:01.16
Frame length. . . . . 113        Info field length. . . . . 91
Destination address . C00000001000     Source address . . OS2MGR

Access control field. . 10 -> Pri = 0 busy ~mc Res = 0
Frame control field . . 40 -> FMT 1 LLC
Frame status field. . . 00 -> Address not recognized, Frame not copied
Routing information . C810 -> SR BC  Len=8 Dir=0 Max IF=1500
Ring/bridge numbers . 0131 7001 6000
Individual DSAP = D4,  Command SSAP = F2,  Control Field = 03
Unnumbered frame Cmd: UI

0000 D4 F2 03 A1 56 02 02 00-B2 02 01 07 30 4D 80 07
                         .
                         .
                         .

0050 02 04 02 00 30 83 01 F2-84 01 02
```

Figure 83. CMIP INVOKE Frame Without the Qualifier Set

```
Frame number. . . . . 10          Time stamp . . . . .16:26:24.49
Frame length. . . . . 113         Info field length. . . . . 91
Destination address . C00000001000      Source address . . OS2MGR

Access control field. . 10 -> Pri = 0 busy ˜mc Res = 0
Frame control field . . 40 -> FMT 1 LLC
Frame status field. . . 00 -> Address not recognized, Frame not copied
Routing information . C810 -> SR BC  Len=8 Dir=0 Max IF=1500
Ring/bridge numbers . 0131 7001 6000
Individual DSAP = D4,  Command SSAP = F2,  Control Field = 03
Unnumbered frame Cmd: UI

0000 D4 F2 03 A1 56 02 02 00-BA 02 01 07 30 4D 80 07
                         .
                         .
                         .

0050 02 04 02 06 00 83 01 F2-84 01 02



Frame number. . . . . 11          Time stamp . . . . .16:26:24.54
Frame length. . . . . 120         Info field length. . . . . 98
Destination address . OS2MGR            Source address . . CAUPI

Access control field. . 18 -> Pri = 0 busy mc Res = 0
Frame control field . . 40 -> FMT 1 LLC
Frame status field. . . CC -> Address recognized, Frame copied
Routing information . 0890 -> NON BC  Len=8 Dir=1 Max IF=1500
Ring/bridge numbers . 0131 7001 6000
Individual DSAP = F2,  Command SSAP = D4,  Control Field = 03
Unnumbered frame Cmd: UI

0000 F2 D4 03 A2 82 00 5B 02-02 00 BA 30 82 00 53 02
                               .
                               .
                               .
0050 30 10 80 02 01 02 04 02-06 00 04 04 5A 98 F5 F2
0060 A3 00
```

Figure 84. CMIP INVOKE Frame With Qualifier Set and 8230 Response

LAN Network Manager can thus manage segments with Controlled Access Units on segments bridged by 6611 Network Processors but not linked to. The bridged segments will not show up in the *segment* display of the LAN Network Manager. The extent of LAN Network Manager V1.0 ability to manage the IBM 8230 CAUs in this environment is limited to **only** those functions that can be performed with the IBM 8230 Maintenance Facility. LAN Network Manager V1.0 will **not** be able to provide any Access Control of those 8230s managed by the CAU qualifier function.

4.3.2.2 LNM Support for 8220s

The 8220 sends two frames out to the management entity that signify that:

1. the backup path has wrapped to the main path
2. the backup path is beaconing

These frames are always sent to the LNM functional address but were discarded if not coming from a managed segment. The PTF will permit LNM accepting these frames. An **alert** is logged when the condition is reported and an **event** is logged when the condition is resolved. Normally LNM will update the status of the segment from which the wrap report is received. This will not be possible for these 6611 bridged rings.

4.3.3 LNM Support for 6611 Network Processor Compatibility Mode Bridging

The IBM LAN Network Manager with its PTF UR37165 and the IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) with its PTF UR37051 provide more support than that provided for token rings bridged only by 6611s. Since the LAN Network Manager cannot link to the 6611 bridge function there is a PTF for the Token-Ring Bridge Program Version 2.2 to enable LAN Network Manager Version 1.0, with its associated PTF, to link through the 6611 Network Processor to the remote token-ring bridge half.

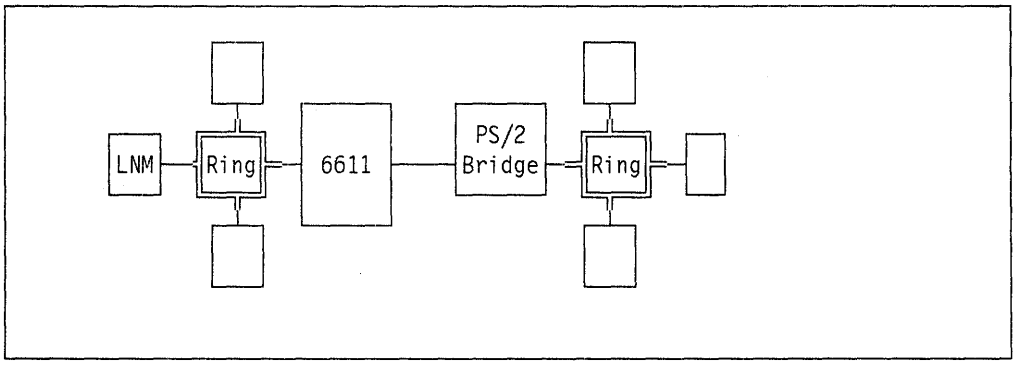


Figure 85. LNM Support for Remote Segment of 6611 Compatibility Mode Bridge

The token-ring management provided is **similar** in content to the management support provided for token-rings connected by linked bridges, and includes:

1. Full CRS and RPS support

   With these two network management server functions, full Access Control support for IBM 8230 CAUs on those linked segments will be possible.

2. Limited REM function

   All token-ring soft errors and temporary beacons will be reported. Hard errors will not be reported by the bridge. The reason that a beaconing condition cannot be reported through the IBM Token-Ring Network Bridge Program Version 2.2 even with the bridge PTF applied is because of the way the PTF allows management of the segment. Since the IBM 6611 Network Processor does not implement the LAN Reporting Mechanism if the bridge was to try and use this mechanism to report error conditions on the managed segment through the 6611, the 6611 would discard the frame.

   In order to resolve this problem the bridge PTF changed the way the bridge communicates to the managing LAN Network Manager. Instead of trying to use the LAN Reporting Mechanism, the bridge will recognize that it is part of

a 6611 in bridge compatibility mode and put the frames normally sent by the LAN Reporting Mechanism to its other half out on it's own local segment. The frame is addressed to the LAN Network Manager's MAC address and bridged across the IBM 6611-to-IBM Token-Ring Network Bridge Program V2.2 link.

When a ring is beaconing, no other traffic can flow on that segment except for the Beacon MAC frame. The bridge cannot put the beaconing notification frame out on its local segment and thus cannot notify the managing LAN Network Manager of the condition.

3. Limited bridge management

   The Token-Ring Bridge Program will:

   - Accept commands from the LNM to set the parameters "Percent frames lost" and "Bridge performance notification interval". These parameters will not be known to the 6611 Network Processor half of the bridge.
   - Report "bridge performance threshold exceeded" alerts and performance notifications to LNM.
   - Report bridge status and performance data upon request from LNM.

LAN Network Manager can now **link** to the bridge and the segments will show up in the segment display.

4.3.4 Critical Resource Support

Although the IBM LAN Network Manager cannot link to rings that are bridged over 6611 Network Processors, it can define stations as *Critical Resources* and monitor them. In that way the system administrator can be informed of the loss of these devices.

Part 3. Example Scenarios

Chapter 5. Basic TCP/IP Example Scenario

This chapter describes a basic TCP/IP scenario that utilizes the 6611 Network Processor. The purpose of this scenario is to illustrate the minimum configuration necessary to provide TCP/IP based management of a network of 6611 Network Processors. This scenario will be used as the basis of other scenarios described in subsequent chapters.

The scenario is illustrated in Figure 86.

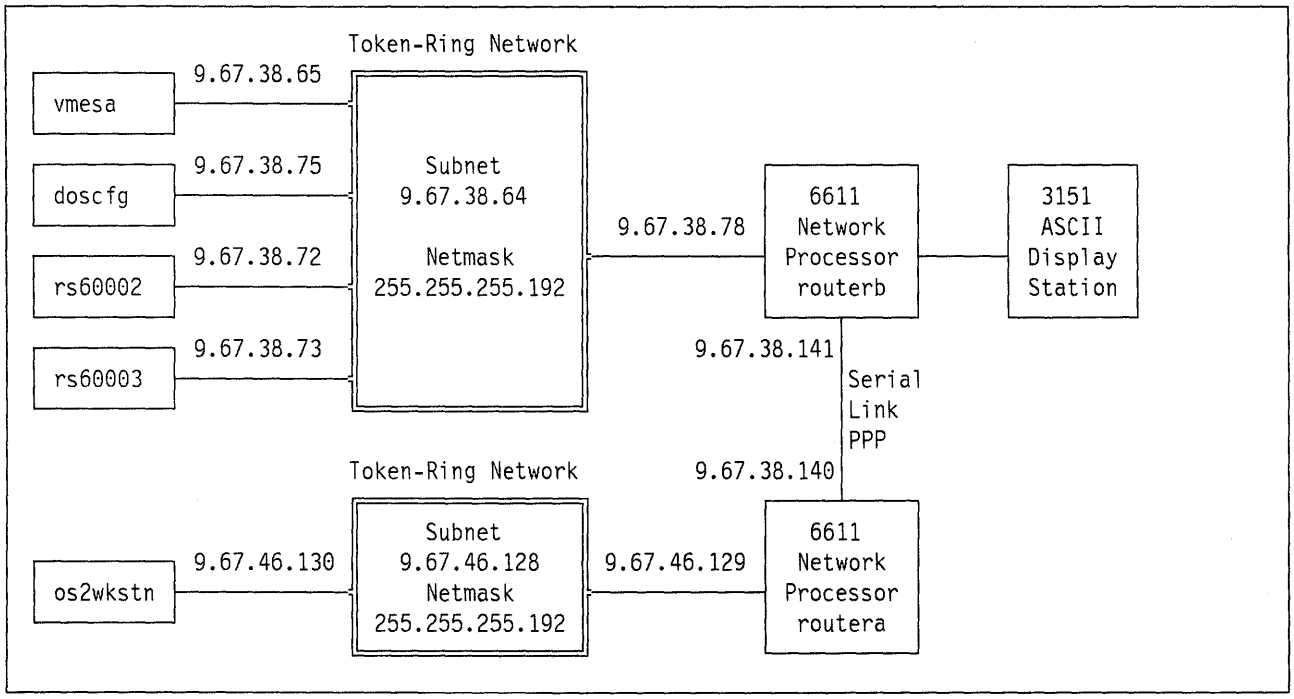


Figure 86. Basic TCP/IP Example Scenario

The scenario consists of two 6611 Network Processors ("routera" and "routerb") interconnected via a high speed serial link (1.536 Mbps) using PPP. Each 6611 Network Processor is attached to a single Token-Ring Network. The 6611 Network Processors are configured to support routing of the TCP/IP protocol suite between the Token-Ring Networks using **static** routes (that is, no routing table maintenance protocol is used).

A IBM 3151 ASCII Display Station is attached to one 6611 Network Processor ("routerb") to provide local access to the System Manager. It can also be used to access the System Manager of the other 6611 Network Processor ("routera") via TCP/IP protocols.

Each Token-Ring Network is a different TCP/IP subnet using a subnet mask of "255.255.255.192." Therefore the *subnet* part of each TCP/IP network layer address comprises 26 bits and the *host* part comprises 6 bits.

Various TCP/IP hosts are attached to each Token-Ring Network to provide facilities to test the functionality of the scenario. These hosts are:

rs60002 A network management system using the IBM AIX NetView/6000 with IBM AIX Version 3.2 running on an IBM RISC System/6000.

rs60003 A network management system using the IBM AIX NetView/6000 with IBM AIX Version 3.2 running on an IBM RISC System/6000.

doscfg A configuration system using IBM TCP/IP Version 2 for DOS with IBM DOS Version 5 running on an IBM Personal System/2.

os2wkstn A test workstation using IBM TCP/IP Version 1.2 for OS/2 with IBM Operating System/2* Version 1.30.2 running on an IBM Personal System/2.

vmesa A test host using IBM TCP/IP Version 2.2 for VM running with IBM VM/ESA* Version 1.1.1 on an IBM Enterprise System/9000*.

The following sections describe the configuration of the various systems that comprise the scenario.

5.1 Configuration of routera

This router is a 6611 Network Processor Model 170. There are three elements of the 6611 Network Processor that are configured to support this scenario:

- System Configuration
- System Management
- Adapter Configuration

The configuration parameters required for each of these elements are described in the following sections.

5.1.1 System Configuration

System configuration comprises many components. Those components that should be configured to implement this scenario are summarized in Table 10.

Table 10. routera - System Configuration Summary

SR Bridge	IP	IPX	XNS	DECnet	DLS
No	**Yes**	No	No	No	No

Only the IP component of system configuration must be configured to support this scenario. It is described further in the following section.

5.1.1.1 IP: The IP component of system configuration is comprised of many sub-components. Those sub-components that should be configured to implement this scenario are listed in Table 11.

Table 11. routera - System Configuration - IP Summary

OSPF	RIP	HELLO	EGP	Static Routes	Packet Filters	Route Exports	IP Over X.25
No	No	No	No	**Yes**	No	No	No

Only the static routes sub-component of IP requires configuration to support this scenario. The configuration parameters for static routes are provided in Table 12. A single static route is defined to reach subnet "9.67.38.64" via the PPP link to "routerb."

Table 12. routera - System Configuration - IP - Static Routes

Destination Address	Destination Mask	Next Hop Router	Preference	Retain Route
9.67.38.64	255.255.255.192	9.67.38.141	50	Yes

5.1.2 System Management

System management comprises many components. Those components that should be configured to implement this scenario are summarized in Table 13 on page 147.

Table 13. routera - System Management Summary	
IBM 6611 Host Name	routera
Domain Name	itsc.raleigh.ibm.com
BAUD Rate for S1 Serial Port	9600
BAUD Rate for S2 Serial Port	2400
Lock Value	Unlock
SNMP	**Yes** (see Table 14)
Users Of System Manager	**Yes** (see Table 17 on page 148)
Configuration Hosts	All hosts
Time to Perform Configuration	Immediately
Remote Host Names	**Yes** (see Table 18 on page 148)
Name Servers	None
Time Servers	None

Those components of system management that require further configuration are described in the following sections.

5.1.2.1 SNMP: The SNMP configuration parameters to implement this scenario are summarized in Table 14.

Table 14. routera - System Management - SNMP Summary	
Enable SNMP	Yes
System Contact	James Kelly or Ivan Van Netelbosch, Room CC-103
System Location	ITSC LAB, Building 657, Raleigh NC USA
System Name	routera.itsc.raleigh.ibm.com
Enterprise Specific Trap Throttle Time	900
Router Serial Number	26-24686
Define Traps	**Yes** (see Table 15)
Define Views	No
Define Communities	**Yes** (see Table 16 on page 148)

The configuration parameters for SNMP traps are provided in Table 15. These parameters specify the network management systems that should be sent SNMP traps by the 6611 Network Processor SNMP agent. In this scenario the "rs60002" and "rs60003" network management systems will be sent SNMP traps.

Table 15 (Page 1 of 2). routera - System Management - SNMP - Traps								
Trap Address	**Trap Community Name**	**Cold Start**	**Warm Start**	**Link Down**	**Link Up**	**Authentication Failure**	**EGP Neighbor Loss**	**Enterprise Specific**
rs60002	ITSC	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 15 (Page 2 of 2). routera - System Management - SNMP - Traps								
Trap Address	**Trap Community Name**	**Cold Start**	**Warm Start**	**Link Down**	**Link Up**	**Authentication Failure**	**EGP Neighbor Loss**	**Enterprise Specific**
rs60003	ITSC	Yes	Yes	Yes	Yes	Yes	Yes	Yes

The configuration parameters for SNMP communities are provided in Table 16. These parameters specify the community names that can be used by network management systems to access the 6611 Network Processor SNMP agent. In this scenario a single community name ("ITSC") is defined that has access to the entire MIB as no "Community View Name" has been specified.

Table 16. routera - System Management - SNMP - Communities				
Community Name	**Community Address**	**Community Address Mask**	**Community Access**	**Community View Name**
ITSC	9.67.0.0	255.255.0.0	read only	

5.1.2.2 Users of System Manager: The users able to access the System Manager in this scenario are listed in Table 17.

Table 17. routera - System Management - Users of System Manager					
Userid	**Password**	**Type**	**Userid**	**Password**	**Type**
kellyjp	bart	Controlling	vannetel	homer	Controlling
collinsr	lisa	Viewing	shogren	maggie	Viewing

5.1.2.3 Remote Host Names: The remote TCP/IP hosts that can be accessed via name from the System Manager in this scenario are listed in Table 18.

Table 18. routera - System Management - Remote Host Names			
IP Address Of Host	**Host Name**	**IP Address Of Host**	**Host Name**
9.67.38.65	vmesa	9.67.38.72	rs60002
9.67.38.73	rs60003	9.67.38.75	doscfg
9.67.38.78	routerb	9.67.46.130	os2wkstn

5.1.3 Adapter Configuration

The communication adapter features installed and interfaces used in this scenario are summarized in Table 19.

Table 19 (Page 1 of 2). routera - Adapter Configuration - Summary					
Slot	**Adapter**	**Port 0**	**Port 1**	**Port 2**	**Port 3**
1	6611 2-Port Serial Adapter	N/A	**PPP**	Not Used	N/A
2	6611 Token-Ring Network 16/4 Adapter	N/A	**Used**	N/A	N/A
3	6611 4-Port SDLC Adapter	Not Used	Not Used	Not Used	Not Used
4	6611 Ethernet Adapter	N/A	Not Used	N/A	N/A
5	Empty Slot				
6	Empty Slot				

Table 19 (Page 2 of 2). routera - Adapter Configuration - Summary					
Slot	**Adapter**	**Port 0**	**Port 1**	**Port 2**	**Port 3**
7	Empty Slot				

The configuration parameters for each communication interface that is used to implement this scenario are described in the following sections.

5.1.3.1 Slot 1, Port 1 (Serial): This communication interface is used to provide the PPP link to the other router ("routerb"). A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 20.

Table 20. routera - Slot 1, Port 1 (Serial) - Summary									
Physical Interface	**PPP**	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	**Yes**	No	No	**Yes**	No	No	No	No	No

The parameters required to configure the physical interface are listed in Table 21.

Table 21. routera - Slot 1, Port 1 (Serial) - Physical Interface			
Enable Interface	Yes	**Cylink Serial Number**	
Serial Line Speed	1536000	**Data Encoding**	NRZI
Locally Administered MAC Address			

The parameters required to configure the PPP data link protocol for this interface are listed in Table 22.

Table 22. routera - Slot 1, Port 1 (Serial) - PPP			
Enable PPP On This Port	Yes	**Maximum Receive Unit**	1500
Enable Link Quality Monitoring	Yes	**Link Quality Monitoring Interval**	10000

The parameters required to configure the IP network layer protocol for this interface are listed in Table 23.

Table 23. routera - Slot 1, Port 1 (Serial) - IP			
Enable IP Routing On This Port	Yes	**IP Address**	9.67.38.140
Subnet Mask	255.255.255.192	**Destination IP Address**	9.67.38.141
Maximum Transmission Unit	1500		

5.1.3.2 Slot 2, Port 1 (Token-Ring): This communication interface is used to provide access to a Token-Ring Network. A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 24.

Table 24. routera - Slot 2, Port 1 (Token Ring) - Summary								
Physical Interface	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	No	No	**Yes**	No	No	No	No	No

The parameters required to configure the physical interface are listed in Table 25 on page 150.

Table 25. routera - Slot 2, Port 1 (Token-Ring) - Physical Interface			
Enable Interface	Yes	**MAC Address**	Use Card MAC Address
MAC Address Format	Non-canonical	**Alternate MAC Address**	
Token-Ring Data Rate	4Mbps	**Broadcast Type**	Non-Local

The parameters required to configure the IP network layer protocol for this interface are listed in Table 26.

Table 26. routera - Slot 2, Port 1 (Token Ring) - IP			
Enable IP Routing On This Port	Yes	**IP Address**	9.67.46.129
Subnet Mask	255.255.255.192	**Maximum Transmission Unit**	1500

5.2 Configuration of routerb

This router is a 6611 Network Processor Model 170. There are three elements of the 6611 Network Processor that are configured to support this scenario:

- System Configuration
- System Management
- Adapter Configuration

The configuration parameters required for each of these elements are described in the following sections.

5.2.1 System Configuration

System configuration comprises many components. Those components that should be configured to implement this scenario are summarized in Table 27.

Table 27. routerb - System Configuration Summary					
SR Bridge	**IP**	**IPX**	**XNS**	**DECnet**	**DLS**
No	**Yes**	No	No	No	No

Only the IP component of system configuration must be configured to support this scenario. It is described further in the following section.

5.2.1.1 IP: The IP component of system configuration is comprised of many sub-components. Those sub-components that should be configured to implement this scenario are listed in Table 28.

Table 28. routerb - System Configuration - IP Summary							
OSPF	**RIP**	**HELLO**	**EGP**	**Static Routes**	**Packet Filters**	**Route Exports**	**IP Over X.25**
No	No	No	No	**Yes**	No	No	No

Only the static routes sub-component of IP requires configuration to support this scenario. The configuration parameters for static routes are provided in Table 29 on page 151. A single static route is defined to reach subnet "9.67.46.128" via the PPP link to "routera."

Table 29. routerb - System Configuration - IP - Static Routes				
Destination Address	**Destination Mask**	**Next Hop Router**	**Preference**	**Retain Route**
9.67.46.128	255.255.255.192	9.67.38.140	50	Yes

5.2.2 System Management

System management comprises many components. Those components that should be configured to implement this scenario are summarized in Table 30.

Table 30. routerb - System Management Summary	
IBM 6611 Host Name	routerb
Domain Name	itsc.raleigh.ibm.com
BAUD Rate for S1 Serial Port	9600
BAUD Rate for S2 Serial Port	2400
Lock Value	Unlock
SNMP	**Yes** (see Table 31)
Users Of System Manager	**Yes** (see Table 34 on page 152)
Configuration Hosts	All hosts
Time to Perform Configuration	Immediately
Remote Host Names	**Yes** (see Table 35 on page 152)
Name Servers	None
Time Servers	None

Those components of system management that require further configuration are described in the following sections.

5.2.2.1 SNMP: The SNMP configuration parameters to implement this scenario are summarized in Table 31.

Table 31. routerb - System Management - SNMP Summary	
Enable SNMP	Yes
System Contact	James Kelly or Ivan Van Netelbosch, Room CC-103
System Location	ITSC LAB, Building 657, Raleigh NC USA
System Name	routerb.itsc.raleigh.ibm.com
Enterprise Specific Trap Throttle Time	900
Router Serial Number	26-06620
Define Traps	**Yes** (see Table 32 on page 152)
Define Views	No
Define Communities	**Yes** (see Table 33 on page 152)

The configuration parameters for SNMP traps are provided in Table 32 on page 152. These parameters specify the network management systems that should be sent SNMP traps by the 6611 Network Processor SNMP agent. In this scenario the "rs60002" and "rs60003" network management systems will be sent SNMP traps.

Table 32. routerb - System Management - SNMP - Traps								
Trap Address	**Trap Community Name**	**Cold Start**	**Warm Start**	**Link Down**	**Link Up**	**Authentication Failure**	**EGP Neighbor Loss**	**Enterprise Specific**
rs60002	ITSC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
rs60003	ITSC	Yes	Yes	Yes	Yes	Yes	Yes	Yes

The configuration parameters for SNMP communities are provided in Table 33. These parameters specify the community names that can be used by network management systems to access the 6611 Network Processor SNMP agent. In this scenario a single community name ("ITSC") is defined that has access to the entire MIB, as no "Community View Name" has been specified.

Table 33. routerb - System Management - SNMP - Communities				
Community Name	**Community Address**	**Community Address Mask**	**Community Access**	**Community View Name**
ITSC	9.67.0.0	255.255.0.0	read only	

5.2.2.2 Users of System Manager: The users able to access the System Manager in this scenario are listed in Table 34.

Table 34. routerb - System Management - Users of System Manager					
Userid	**Password**	**Type**	**Userid**	**Password**	**Type**
kellyjp	bart	Controlling	vannetel	homer	Controlling
collinsr	lisa	Viewing	shogren	maggie	Viewing

5.2.2.3 Remote Host Names: The remote TCP/IP hosts that can be accessed via name in this scenario are listed in Table 35.

Table 35. routerb - System Management - Remote Host Names			
IP Address Of Host	**Host Name**	**IP Address Of Host**	**Host Name**
9.67.38.65	vmesa	9.67.38.72	rs60002
9.67.38.73	rs60003	9.67.46.129	routera
9.67.38.75	doscfg	9.67.46.130	os2wkstn

5.2.3 Adapter Configuration

The communication adapter features installed and interfaces used in this scenario are summarized in Table 36.

Table 36 (Page 1 of 2). routerb - Adapter Configuration - Summary					
Slot	**Adapter**	**Port 0**	**Port 1**	**Port 2**	**Port 3**
1	6611 2-Port Serial Adapter	N/A	**PPP**	Not Used	N/A
2	6611 Token-Ring Network 16/4 Adapter	N/A	**Used**	N/A	N/A
3	Empty Slot				
4	Empty Slot				
5	Empty Slot				

Table 36 (Page 2 of 2). routerb - Adapter Configuration - Summary					
Slot	**Adapter**	**Port 0**	**Port 1**	**Port 2**	**Port 3**
6	Empty Slot				
7	Empty Slot				

The configuration parameters for each communication interface that is used to implement this scenario are described in the following sections.

5.2.3.1 Slot 1, Port 1 (Serial): This communication interface is used to provide the PPP link to the other router ("routera"). A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 37.

Table 37. routerb - Slot 1, Port 1 (Serial) - Summary									
Physical Interface	**PPP**	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	**Yes**	No	No	**Yes**	No	No	No	No	No

The parameters required to configure the physical interface are listed in Table 38.

Table 38. routerb - Slot 1, Port 1 (Serial) - Physical Interface			
Enable Interface	Yes	**Cylink Serial Number**	
Serial Line Speed	1536000	**Data Encoding**	NRZI
Locally Administered MAC Address			

The parameters required to configure the PPP data link protocol for this interface are listed in Table 39.

Table 39. routerb - Slot 1, Port 1 (Serial) - PPP			
Enable PPP On This Port	Yes	**Maximum Receive Unit**	1500
Enable Link Quality Monitoring	Yes	**Link Quality Monitoring Interval**	10000

The parameters required to configure the IP network layer protocol for this interface are listed in Table 40.

Table 40. routerb - Slot 1, Port 1 (Serial) - IP			
Enable IP Routing On This Port	Yes	**IP Address**	9.67.38.141
Subnet Mask	255.255.255.192	**Destination IP Address**	9.67.38.140
Maximum Transmission Unit	1500		

5.2.3.2 Slot 2, Port 1 (Token-Ring): This communication interface is used to provide access to a Token-Ring Network. A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 41.

Table 41. routerb - Slot 2, Port 1 (Token Ring) - Summary								
Physical Interface	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	No	No	**Yes**	No	No	No	No	No

The parameters required to configure the physical interface are listed in Table 42 on page 154.

Table 42. routerb - Slot 2, Port 1 (Token Ring) - Physical Interface			
Enable Interface	Yes	**MAC Address**	Use Card MAC Address
MAC Address Format	Non-canonical	**Alternate MAC Address**	
Token-Ring Data Rate	4Mbps	**Broadcast Type**	Non-Local

The parameters required to configure the IP network layer protocol for this interface are listed in Table 43.

Table 43. routerb - Slot 2, Port 1 (Token Ring) - IP			
Enable IP Routing On This Port	Yes	**IP Address**	9.67.38.78
Subnet Mask	255.255.255.192	**Maximum Transmission Unit**	1500

5.3 Configuration of Other Systems

The other systems in this scenario must also be configured to interoperate correctly with the 6611 Network Processors. The following sections summarize those configuration parameters for the other systems which are relevant to this scenario.

For "rs60002" and "rs60003," most of these parameters can be configured using the SMIT (System Management Interface Tool) program which is part of IBM AIX Version 3.2.

For "os2wkstn" these parameters can be configured using the ICAT (Installation and Configuration Automation Tool) program which is part of IBM TCP/IP Version 1.2 for OS/2.

For "doscfg" most of these parameters can be configured using the CUSTOM program which is part of IBM TCP/IP Version 2 for DOS.

For "vmesa" these parameters can be configured by editing the "PROFILE TCPIP" file.

5.3.1 IP Addresses

Each system that participates in the scenario requires a TCP/IP network layer address or *IP address* and corresponding *subnet mask*. The IP addresses used for each system are listed in Table 44. The subnet mask used for all systems in the scenario is "255.255.255.192."

Table 44. Other Systems - IP Addresses			
System	**IP Address**	**System**	**IP Address**
vmesa	9.67.38.65	rs60002	9.67.38.72
rs60003	9.67.38.73	doscfg	9.67.38.75
os2wkstn	9.67.46.130		

5.3.2 Routes

In this scenario static routing is used; therefore, each system must be configured with routes to the TCP/IP subnets that they can access via the 6611 Network Processors.

Those systems attached to subnet "9.67.38.64" need a route to the subnet "9.67.46.128" via the 6611 Network Processor "routerb" ("9.67.38.78").

For "rs60002" and "rs60003" this can be specified using either the SMIT program or the AIX command:

```
route add net 9.67.46.128 9.67.38.78 netmask 255.255.255.192
```

For "doscfg" this can be specified using the IBM TCP/IP Version 2 for DOS command:

```
ifconfig inet ip route add net 9.67.46.128 9.67.38.78 255.255.255.192
```

For "vmesa" this can be specified under the "GATEWAY" statement in the "PROFILE TCPIP" file. The entry required is:

```
; NETWORK  FIRST_HOP   LINK  P_SIZE  SUBN_MASK      SUBN_VALUE
  9        9.67.38.78  TR1   1500    0.255.255.192  0.67.46.128
```

The system attached to subnet "9.67.46.128" needs a route to subnet "9.67.38.64" via the 6611 Network Processor "routera" ("9.67.46.129").

For "os2wkstn" this can be specified using either the ICAT program, or the IBM TCP/IP Version 1.2 for OS/2 command:

```
route add subnet 9.67.38.64 9.67.46.129
```

Note: *Default routes* could have been used in this scenario; however, the use of default routes would have provided a less interesting example.

5.3.3 Network Management

Those systems that are being used as network management systems ("rs60002" and "rs60003") require additional configuration to effectively manage the 6611 Network Processors.

The IBM AIX NetView/6000 uses a file called "/etc/hosts" to translate TCP/IP hosts names to IP addresses. This file can be modified using SMIT. The 6611 Network Processors are defined in this file using the entries:

```
9.67.46.129   routera  # 6611 Network Processor A
9.67.38.78    routerb  # 6611 Network Processor B
```

Note: In this scenario name servers are not used to resolve TCP/IP host names.

The IBM AIX NetView/6000 uses a file called "/etc/community" to specify the community name that should be used when accessing SNMP agents. The 6611 Network Processors are defined in this file using the entries:

```
routera ITSC
routerb ITSC
```

The IBM AIX NetView/6000 uses files called *MIB modules* when managing SNMP agents. The 6611 Network Processor is shipped with the MIB modules that are required to manage the 6611 Network Processor SNMP agent. These are contained in the *static* directory of the 6611 Network Processor and should be transferred to all network management systems. The IBM AIX NetView/6000 expects these MIB modules to be placed in the directory "/usr/etc/nm/mibs" on the network management system.

The following transcript illustrates the use of FTP to transfer these MIB modules and associated documentation from a 6611 Network Processor ("routerb") to a network management system. Comments have been placed in the transcript using "<" and ">" as delimiters.

```
$ cd /usr/etc/nm/mibs  <Where NetView/6000 looks for MIB modules>
$ ftp routerb  <Connect to a 6611>
Connected to routerb.
220 routerb FTP server (Version 4.1 Wed May 27 23:04:04 EDT 1992) ready.
Name (routerb:root): kellyjp  <Enter a valid system manager user>
331 Password required for kellyjp.
```

```
Password:bart  <Password does not echo>
230 User kellyjp logged in.
ftp> verbose  <To reduce messages generated by FTP>
Verbose mode off.
ftp> cd /static  <MIB modules are stored in the static directory>
ftp> mget *  <Get files from the static directory>
mget README-NM? y  <Instructions>
local: README-NM remote: README-NM
mget config.doc? n  <Not required for network management>
mget dummy? n  <Not required for network management>
mget ibm-6611.mib? y
local: ibm-6611.mib remote: ibm-6611.mib
mget ibm-alert.mib? y
local: ibm-alert.mib remote: ibm-alert.mib
mget ibm-nv6ksubagent.mib? y
local: ibm-nv6ksubagent.mib remote: ibm-nv6ksubagent.mib
mget ibm.mib? y
local: ibm.mib remote: ibm.mib
mget mib-2? y  <Equivalent to smi.mib + mibII.mib>
local: mib-2 remote: mib-2
mget mibII.mib? y
local: mibII.mib remote: mibII.mib
mget rfc1229.mib? y
local: rfc1229.mib remote: rfc1229.mib
mget rfc1231.mib? y
local: rfc1231.mib remote: rfc1231.mib
mget rfc1232.mib? y
local: rfc1232.mib remote: rfc1232.mib
mget rfc1253.mib? y
local: rfc1253.mib remote: rfc1253.mib
mget rfc1284.mib? y
local: rfc1284.mib remote: rfc1284.mib
mget rfc1286.mib? y
local: rfc1286.mib remote: rfc1286.mib
mget rfc1289.mib? y
local: rfc1289.mib remote: rfc1289.mib
mget smi.mib? y
local: smi.mib remote: smi.mib
mget trapd.conf.6611? y  <SNMP traps generated by 6611>
local: trapd.conf.6611 remote: trapd.conf.6611
mget updnv6? y  <Script to update Netview/6000 with 6611 traps>
local: updnv6 remote: updnv6
ftp> close  <Close connection to 6611>
ftp> quit  <Quit FTP>
$  <Done>
```

The IBM AIX NetView/6000 uses a file called "/usr/etc/nm/conf/trapd.conf" to translate SNMP traps received from SNMP agents into a human readable form. The 6611 Network Processor provides updates that can be added to this file to allow the IBM AIX NetView/6000 to translate traps generated by the 6611 Network Processor.

These updates are contained in the file "trapd.conf.6611" and can be added to "/usr/etc/nm/conf/trapd.conf" using a shell script called "updnv6." Both "trapd.conf.6611" and "updnv6" are available in the static directory of all 6611 Network Processors and should be transferred to each network management system using FTP. The previous FTP transcript illustrated the use of FTP to transfer the updates and shell script to a network management system.

Chapter 6. Remote Source Route Bridging Example Scenario

This chapter describes a remote source route bridging scenario that utilizes the 6611 Network Processor. The purpose of this scenario is to illustrate the minimum configuration necessary to implement remote source route bridges based on the 6611 Network Processor.

This scenario is based upon the scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. References will be made to configuration parameters described in that chapter.

The remote source route bridging scenario is illustrated in Figure 87.

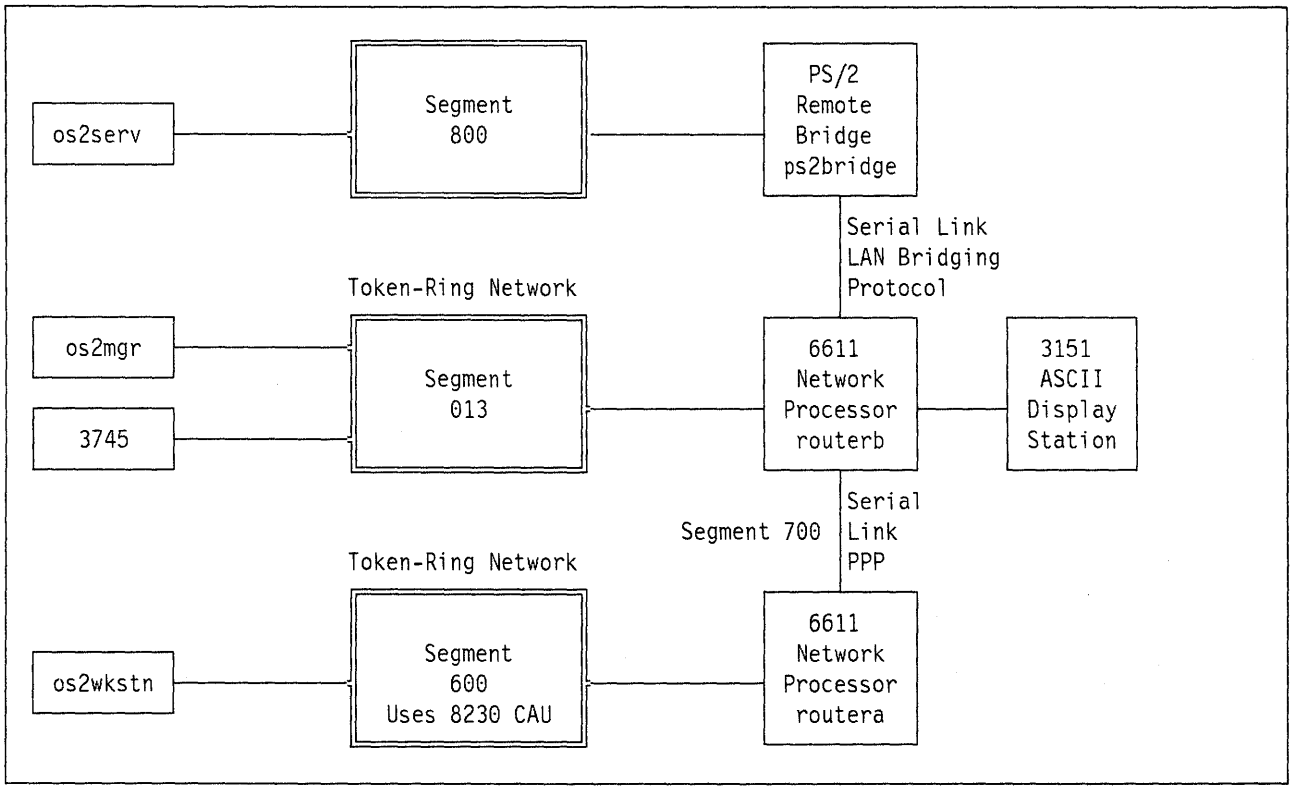


Figure 87. Remote Source Route Bridging Example Scenario

The scenario consists of two 6611 Network Processors ("routera" and "routerb") interconnected via a high speed serial link (1.536 Mbps) using PPP. Each 6611 Network Processor is attached to a single Token-Ring Network. The 6611 Network Processors are configured to provide source route bridging between the two Token-Ring Networks.

Additionally, a PS/2 running IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) ("ps2bridge") is interconnected with one of the 6611 Network Processors ("routerb") via a medium speed serial link (56 Kbps) using the LAN bridging protocol. The PS/2 is attached to a single Token-Ring Network, and both the 6611 Network Processor and the PS/2 are configured to provide source route bridging between the Token-Ring Network attached to the PS/2 and the other Token-Ring Networks in the scenario.

The 6611 Network Processors are also configured to support all the elements of the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. All the TCP/IP connectivity and management facilities provided by the first example scenario will also be provided by this example scenario. Filters will be used to prevent TCP/IP traffic from traversing the remote source

route bridge between the 6611 Network Processors. However, TCP/IP traffic can still make use of the PPP link using the IP routing function.

Each Token-Ring Network has been assigned a different segment number. The high speed serial link that interconnects the 6611 Network Processors has also been assigned a segment number.

Various devices are attached to each Token-Ring Network to provide facilities to test the functionality of the scenario. These devices are:

os2mgr A LAN management station using IBM LAN Network Manager with IBM Operating System/2 Version 1.30.2 running on an IBM Personal System/2.

ps2bridge Half of a remote source route bridge using IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) with IBM DOS Version 5 running on an IBM Personal System/2.

os2wkstn A test workstation using IBM Operating System/2 Version 1.30.2 running on an IBM Personal System/2 configured for 3270 emulation.

os2serv A NetBIOS based LAN server using IBM OS/2 LAN Server Version 1.3 with IBM Operating System/2 Version 1.30.2 running on an IBM Personal System/2.

3745 An SNA gateway to support access to an IBM Enterprise System/9000 by the test workstation.

8230 An active wiring concentrator to be managed by the LAN management station.

This scenario also includes all the other devices that participated in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145.

The following sections describe the configuration of the various systems that comprise this scenario.

6.1 Configuration of routera

This router is a 6611 Network Processor Model 170. There are three elements of the 6611 Network Processor that are configured to support this scenario:

- System Configuration
- System Management
- Adapter Configuration

The system management configuration for this scenario is identical to that for the first scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 13 on page 147 through Table 18 on page 148.

The configuration parameters for the remaining elements are described in the following sections.

6.1.1 System Configuration

System configuration comprises many components. Those components that should be configured to implement this scenario are summarized in Table 45.

Table 45. routera - System Configuration Summary

SR Bridge	IP	IPX	XNS	DECnet	DLS
Yes	Yes	No	No	No	No

The IP component of system configuration is identical to that for the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 11 on page 146 and Table 12 on page 146.

Each of the remaining system configuration components that must be configured to support this scenario are described in the following sections.

6.1.1.1 SR Bridge

Table 46. routera - System Configuration - SR Bridge			
Enable Source Route Bridging	Yes	**Bridge Number**	1
Designated Ring Number	X'600'	**Bridge Priority**	8000
Hello Time	2	**Forward Delay Time**	15
Max Age	20		

6.1.2 Adapter Configuration

The communication adapter features installed and interfaces used in this scenario are summarized in Table 47.

Table 47. routera - Adapter Configuration - Summary					
Slot	**Adapter**	**Port 0**	**Port 1**	**Port 2**	**Port 3**
1	6611 2-Port Serial Adapter	N/A	**PPP**	Not Used	N/A
2	6611 Token-Ring Network 16/4 Adapter	N/A	**Used**	N/A	N/A
3	6611 4-Port SDLC Adapter	Not Used	Not Used	Not Used	Not Used
4	6611 Ethernet Adapter	N/A	Not Used	N/A	N/A
5	Empty Slot				
6	Empty Slot				
7	Empty Slot				

The configuration parameters for each communication interface that is used to implement this scenario are described in the following sections.

6.1.2.1 Slot 1, Port 1 (Serial): This communication interface is used to provide the PPP link to the other router ("routerb"). A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 48.

Table 48. routera - Slot 1, Port 1 (Serial) - Summary									
Physical Interface	**PPP**	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	Yes	**Yes**	**Yes**	Yes	No	No	No	No	No

The physical interface, PPP and IP configuration parameters for this scenario are identical to those used in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 21 on page 149 through Table 23 on page 149.

The parameters required to configure SR bridge are listed in Table 49 on page 160.

Table 49. routera - Slot 1, Port 1 (Serial) - SR Bridge			
Enable SR Bridging On This Port	Yes	**Ring Number**	X'700'
Maximum Transmission Unit	1500	**Spanning Tree Mode**	Automatic
Path Cost	0	**Enable Forwarding Of Spanning Tree Packets**	N/A

The parameters required to configure SR bridge filters are summarized in Table 50.

Table 50. routera - Slot 1, Port 1 (Serial) - SR Bridge Filter Summary			
Inbound MAC Address	Disable	**Outbound MAC Address**	Disable
Inbound Source SAP	Disable	**Outbound Source SAP**	**Enable**
Inbound SNAP Value	Disable	**Outbound SNAP Value**	**Enable**
Inbound Ring Number	Disable	**Outbound Ring Number**	Disable
Hop Count	7	**Frame Type**	Both SRB and ARB

The outbound source SAP filter should be configured to operate as a "Deny" filter on both SRB and ARB frames. No SAPs need be specified as this filter is only being configured to support the use of the outbound SNAP value filter.

The parameters required to configure the outbound SNAP value filter are listed in Table 51. The outbound SNAP value filter should be configured to operate as a "Deny" filter.

Table 51. routera - Slot 1, Port 1 (Serial) - Outbound SNAP Value Filter					
SNAP Value	**SNAP Value Mask**	**SNAP Value**	**SNAP Value Mask**	**SNAP Value**	**SNAP Value Mask**
X'0800'	X'FFFF'	X'0806'	X'FFFF'	X'8035'	X'FFFF'

All TCP/IP traffic is prevented from crossing this interface via the source route bridging function by the outbound SNAP value filter. Any *bridged* frames that contain the SNAP values for IP (X'0800'), ARP (X'0806') or RARP (X'8035') are prevented from crossing this interface.

Note: This filter does not prevent TCP/IP traffic from crossing this interface via the IP routing function.

6.1.2.2 Slot 2, Port 1 (Token Ring): This communication interface is used to provide access to a Token-Ring Network. A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 52.

Table 52. routera - Slot 2, Port 1 (Token Ring) - Summary								
Physical Interface	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	**Yes**	**Yes**	Yes	No	No	No	No	No

The physical interface and IP configuration parameters for this scenario are identical to those used in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 25 on page 150 and Table 26 on page 150.

The parameters required to configure SR bridge are listed in Table 53.

Table 53 (Page 1 of 2). routera - Slot 2, Port 1 (Token Ring) - SR Bridge			
Enable SR Bridging On This Port	Yes	**Ring Number**	X'600'
Maximum Transmission Unit	1500	**Spanning Tree Mode**	Automatic

Table 53 (Page 2 of 2). routera - Slot 2, Port 1 (Token Ring) - SR Bridge			
Path Cost	0	**Enable Forwarding Of Spanning Tree Packets**	N/A

The parameters required to configure SR bridge filters are summarized in Table 54.

Table 54. routera - Slot 2, Port 1 (Token-Ring) - SR Bridge Filter Summary			
Inbound MAC Address	Disable	**Outbound MAC Address**	Disable
Inbound Source SAP	Disable	**Outbound Source SAP**	Disable
Inbound SNAP Value	Disable	**Outbound SNAP Value**	Disable
Inbound Ring Number	Disable	**Outbound Ring Number**	Disable
Hop Count	7	**Frame Type**	Both SRB and ARB

6.2 Configuration of routerb

This router is a 6611 Network Processor model 170. There are three elements of the 6611 Network Processor that are configured to support this scenario:

- System Configuration
- System Management
- Adapter Configuration

The system management configuration for this scenario is identical to that for the first scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 30 on page 151 through Table 35 on page 152.

The configuration parameters for the remaining elements are described in the following sections.

6.2.1 System Configuration

System configuration comprises many components. Those components that should be configured to implement this scenario are summarized in Table 55.

Table 55. routerb - System Configuration Summary					
SR Bridge	**IP**	**IPX**	**XNS**	**DECnet**	**DLS**
Yes	Yes	No	No	No	No

The IP component of system configuration is identical to that for the scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 28 on page 150 and Table 29 on page 151.

Each of the remaining system configuration components that must be configured to support this scenario are described in the following sections.

6.2.1.1 SR Bridge

Table 56 (Page 1 of 2). routerb - System Configuration - SR Bridge			
Enable Source Route Bridging	Yes	**Bridge Number**	1
Designated Ring Number	X'013'	**Bridge Priority**	8000
Hello Time	2	**Forward Delay Time**	15

Table 56 (Page 2 of 2). routerb - System Configuration - SR Bridge			
Max Age	20		

6.2.2 Adapter Configuration

The communication adapter features installed and interfaces used in this scenario are summarized in Table 57.

Table 57. routerb - Adapter Configuration - Summary					
Slot	**Adapter**	**Port 0**	**Port 1**	**Port 2**	**Port 3**
1	6611 2-Port Serial Adapter	N/A	**PPP**	**LAN Bridge**	N/A
2	6611 Token-Ring Network 16/4 Adapter	N/A	**Used**	N/A	N/A
3	Empty Slot				
4	Empty Slot				
5	Empty Slot				
6	Empty Slot				
7	Empty Slot				

The configuration parameters for each communication interface that is used to implement this scenario are described in the following sections.

6.2.2.1 Slot 1, Port 1 (Serial): This communication interface is used to provide the PPP link to the other router ("routera"). A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 58.

Table 58. routerb - Slot 1, Port 1 (Serial) - Summary									
Physical Interface	**PPP**	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	Yes	**Yes**	**Yes**	Yes	No	No	No	No	No

The physical interface, PPP and IP configuration parameters for this scenario are identical to those used in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 38 on page 153 through Table 40 on page 153.

The parameters required to configure SR bridge are listed in Table 59.

Table 59. routerb - Slot 1, Port 1 (Serial) - SR Bridge			
Enable SR Bridging On This Port	Yes	**Ring Number**	X'700'
Maximum Transmission Unit	1500	**Spanning Tree Mode**	Automatic
Path Cost	0	**Enable Forwarding Of Spanning Tree Packets**	N/A

The parameters required to configure SR bridge filters are summarized in Table 60.

Table 60 (Page 1 of 2). routerb - Slot 1, Port 1 (Serial) - SR Bridge Filter Summary			
Inbound MAC Address	Disable	**Outbound MAC Address**	Disable
Inbound Source SAP	Disable	**Outbound Source SAP**	**Enable**
Inbound SNAP Value	Disable	**Outbound SNAP Value**	**Enable**

Table 60 (Page 2 of 2). routerb - Slot 1, Port 1 (Serial) - SR Bridge Filter Summary			
Inbound Ring Number	Disable	**Outbound Ring Number**	Disable
Hop Count	7	**Frame Type**	Both SRB and ARB

The outbound source SAP filter should be configured to operate as a "Deny" filter on both SRB and ARB frames. No SAPs need be specified as this filter is only being configured to support the use of the outbound SNAP value filter.

The parameters required to configure the outbound SNAP value filter are listed in Table 61. The outbound SNAP value filter should be configured to operate as a "Deny" filter.

Table 61. routerb - Slot 1, Port 1 (Serial) - Outbound SNAP Value Filter					
SNAP Value	**SNAP Value Mask**	**SNAP Value**	**SNAP Value Mask**	**SNAP Value**	**SNAP Value Mask**
X'0800'	X'FFFF'	X'0806'	X'FFFF'	X'8035'	X'FFFF'

All TCP/IP traffic is prevented from crossing this interface via the source route bridging function by the outbound SNAP value filter. Any *bridged* frames that contain the SNAP values for IP (X'0800'), ARP (X'0806') or RARP (X'8035') are prevented from crossing this interface.

Note: This filter does not prevent TCP/IP traffic from crossing this interface via the IP routing function.

6.2.2.2 Slot 1, Port 2 (Serial): This communication interface is used to provide the LAN bridging protocol link to the PS/2 bridge ("ps2bridge"). A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 62.

Table 62. routerb - Slot 1, Port 2 (Serial) - Summary					
Physical Interface	**LAN Bridge Port Defaults**	**SR Bridge**	**SR Bridge Filters**	**SNA**	**NetBIOS**
Yes	**Yes**	**Yes**	**Yes**	No	No

The parameters required to configure the physical interface are listed in Table 63.

Table 63. routerb - Slot 1, Port 2 (Serial) - Physical Interface			
Enable Interface	Yes	**Cylink Serial Number**	
Serial Line Speed	56000	**Data Encoding**	NRZI
Locally Administered MAC Address			

The parameters required to configure the LAN bridge port defaults are listed in Table 64.

Table 64. routerb - Slot 1, Port 2 (Serial) - LAN Bridge Port Defaults			
Enable LAN Bridge PPP On This Port	Yes	**Auto Reboot On Error**	Yes
Performance Counter Threshold	10	**Telecommunications Link Error Threshold**	0
Memory Dump On Error	No	**Event Log Drive**	No
Largest Frame Size	1500	**Network Management Parameters**	**Yes**

The network management parameters required to implement this scenario are listed in Table 65 on page 164.

Table 65. routerb - Slot 1, Port 2 (Serial) - Network Management			
Enable Ring Parameter Server	Yes	**Enable Ring Error Monitor**	Yes
Enable Configuration Report Server	Yes		
Link Password 0	00000000	**Link Password 1**	00000000
Link Password 2	00000000	**Link Password 3**	00000000

The parameters required to configure SR bridge are listed in Table 66.

Table 66. routerb - Slot 1, Port 2 (Serial) - SR Bridge			
Enable SR Bridging On This Port	Yes	**Ring Number**	X'800'
Maximum Transmission Unit	1500	**Spanning Tree Mode**	Automatic
Path Cost	0	**Enable Forwarding Of Spanning Tree Packets**	N/A

The parameters required to configure SR bridge filters are summarized in Table 67.

Table 67. routerb - Slot 1, Port 2 (Serial) - SR Bridge Filter Summary			
Inbound MAC Address	Disable	**Outbound MAC Address**	Disable
Inbound Source SAP	Disable	**Outbound Source SAP**	Disable
Inbound SNAP Value	Disable	**Outbound SNAP Value**	Disable
Inbound Ring Number	Disable	**Outbound Ring Number**	Disable
Hop Count	7	**Frame Type**	Both SRB and ARB

6.2.2.3 Slot 2, Port 1 (Token Ring): This communication interface is used to provide access to a Token-Ring Network. A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 68.

Table 68. routerb - Slot 2, Port 1 (Token Ring) - Summary								
Physical Interface	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	**Yes**	**Yes**	Yes	No	No	No	No	No

The physical interface and IP configuration parameters for this scenario are identical to those used in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 42 on page 154 and Table 43 on page 154.

The parameters required to configure SR bridge are listed in Table 69.

Table 69. routerb - Slot 2, Port 1 (Token Ring) - SR Bridge			
Enable SR Bridging On This Port	Yes	**Ring Number**	X'013'
Maximum Transmission Unit	1500	**Spanning Tree Mode**	Automatic
Path Cost	0	**Enable Forwarding Of Spanning Tree Packets**	N/A

The parameters required to configure SR bridge filters are summarized in Table 70.

Table 70 (Page 1 of 2). routerb - Slot 2, Port 1 (Token-Ring) - SR Bridge Filter Summary			
Inbound MAC Address	Disable	**Outbound MAC Address**	Disable
Inbound Source SAP	Disable	**Outbound Source SAP**	Disable

Table 70 (Page 2 of 2). routerb - Slot 2, Port 1 (Token-Ring) - SR Bridge Filter Summary			
Inbound SNAP Value	Disable	**Outbound SNAP Value**	Disable
Inbound Ring Number	Disable	**Outbound Ring Number**	Disable
Hop Count	7	**Frame Type**	Both SRB and ARB

6.3 Configuration of Other Systems

Most of the other systems in this example scenario require no special configuration to make use of the bridged Token-Ring Network environment provided by the 6611 Network Processors. That is, they would be configured in exactly the same manner as if they were all attached to the same Token-Ring Network segment. This applies to the following systems in this example scenario:

- os2wkstn
- os2serv
- 3745
- 8230

However, there are some aspects of the configuration for "os2mgr" and "ps2bridge" that must be configured to interoperate correctly with the 6611 Network Processors. These aspects are described in the following sections.

6.3.1 Configuration of os2mgr

The only configuration considerations for "os2mgr" are the definition of a "Controlled Access Unit Qualifier" for the Token-Ring Network attached to "routera" that contains an 8230 CAU, and the definition of the PS/2 bridge.

A qualifier for the Token-Ring Network segment X'600' must be defined within IBM LAN Network Manager to enable management of the 8230 in this example scenario. The value of the qualifier is the same as the Token-Ring Network segment number (that is, X'600').

Note: To define a "Controlled Access Unit Qualifier" from within IBM LAN Network Manager, PTF UR37041 must first be applied to IBM LAN Network Manager.

To define "ps2bridge" to IBM LAN Network Manager the MAC address of the PS/2 Token-Ring Network Adapter and the MAC address of the 6611 Token-Ring Network 16/4 Adapter attached to the *designated segment* is required. In this example scenario universally administered MAC addresses are used.

The universally administered MAC address of the PS/2 Token-Ring Network Adapter can be obtained using the "Ring Diagnostic" program supplied with the adapter option diskette.

The universally administered MAC address of the 6611 Token-Ring Network 16/4 Adapter can be obtained using the "View Hardware Vital Product Data" option of the "Hardware Vital Product Data" System Manager menu. The MAC address obtained in this way must be converted from *canonical* to *non-canonical* form for use with IBM LAN Network Manager.

For IBM LAN Network Manager to successfully link to "ps2bridge" the "Reporting Link Password" configured in IBM LAN Network Manager much match the appropriate "Link Password" configured for "ps2bridge" on "routerb." In this example scenario, "00000000" was used for all the "Link Passwords" when "routerb" was configured. This corresponds to a null "Reporting Link Password" in IBM LAN Network Manager.

6.3.2 Configuration of ps2bridge

To interoperate with the 6611 Network Processor "routerb," the PS/2 bridge must be configured as the secondary half of a remote bridge configuration. That is, it must not have an "ECCPARMS.BIN" file present in the "R_BRIDGE" directory.

The "Communication Adapter Configuration" parameters for "ps2bridge" (stored in "ECCSBCF.BIN") are listed in Table 71 on page 166.

Table 71. ps2bridge - Communication Adapter Configuration

Link Data Rate	56000	**Electrical Interface**	V.35
Communications Adapter Transmit Buffer Size	0	**Bridge Mode**	Leased

A V.35 to RS-422/RS-449 interface converter and modems with V.35 interfaces were used to attach "ps2bridge" to the slot 1, port 2, RS-422/RS-449 serial interface of "routerb."

Note: PTF UR37051 must be installed on the PS/2 bridge to support connection with the 6611 Network Processor.

Chapter 7. Data Link Switching Example Scenario

This chapter describes a data link switching scenario that utilizes the 6611 Network Processor. The purpose of this scenario is to illustrate the minimum configuration necessary to implement data link switching based on the 6611 Network Processor.

This scenario is based upon the scenarios described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145 and Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. References will be made to configuration parameters described in those chapters.

The data link switching example scenario is illustrated in Figure 88.

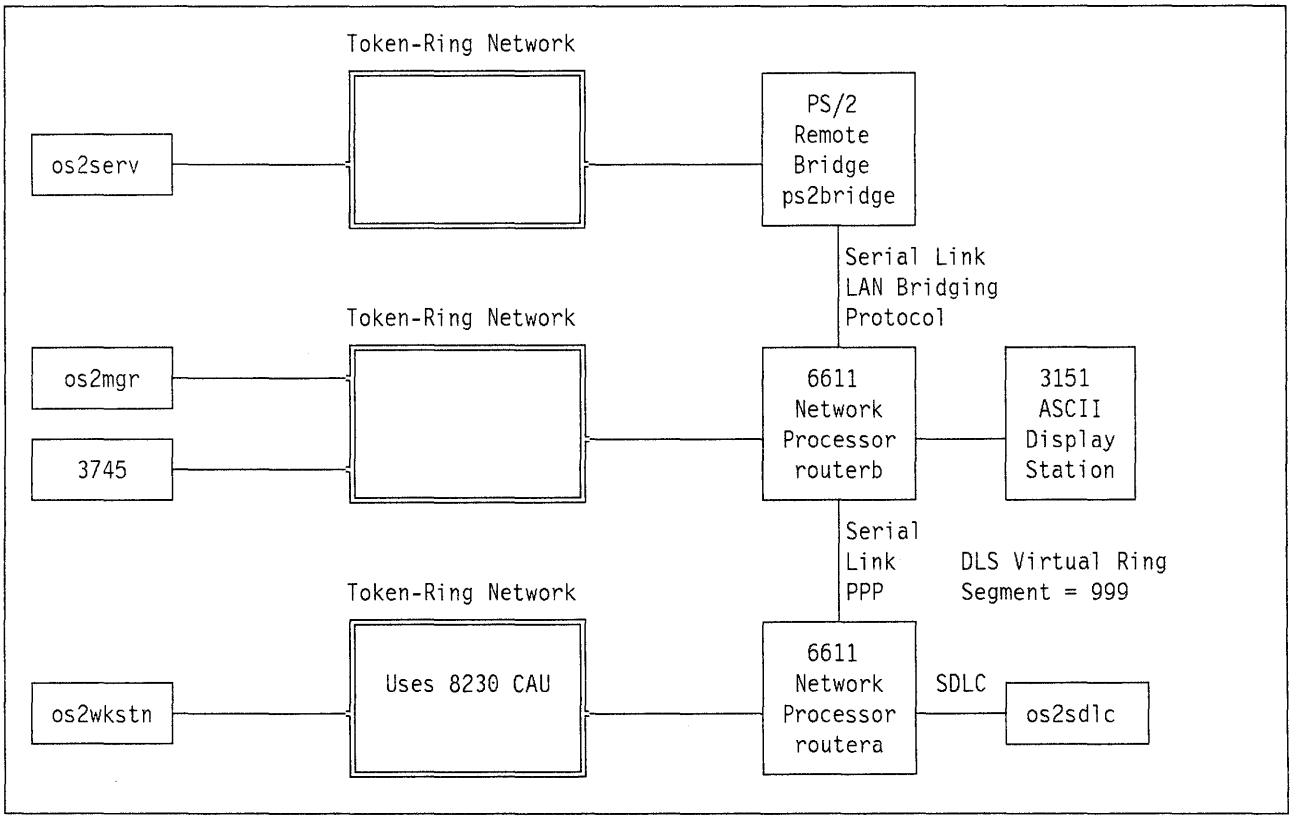


Figure 88. Data Link Switching Example Scenario

The scenario consists of two 6611 Network Processors ("routera" and "routerb") interconnected via a high speed serial link (1.536 Mbps) using PPP. Each 6611 Network Processor is attached to a single Token-Ring Network. The 6611 Network Processors are configured to provide data link switching between the two Token-Ring Networks for SNA and NetBIOS traffic.

Additionally, a PS/2 running IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) ("ps2bridge") is interconnected with one of the 6611 Network Processors ("routerb") via a medium speed serial link (56 Kbps) using the LAN bridging protocol. The PS/2 is attached to a single Token-Ring Network, and the 6611 Network Processor is configured to provide data link switching between the Token-Ring Network attached to the PS/2 and the Token-Ring Network attached to "routera" for SNA and NetBIOS traffic.

Note: SNA and NetBIOS traffic between the Token-Ring Network attached to the PS/2 and the Token-Ring Network attached to "routerb" will not make use of the data link switching function.

The 6611 Network Processors and PS/2 bridge are also configured to support all the elements of the example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. Filters are used to prevent SNA and NetBIOS traffic from traversing the remote source route bridge between the 6611 Network Processors as SNA and NetBIOS traffic across that link will be transported using the data link switching function.

Additionally, the 6611 Network Processors are also configured to support all the elements of the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. All the TCP/IP connectivity and management facilities provided by the first example scenario will also be provided by this example scenario. Filters will be used to prevent TCP/IP traffic from traversing the remote source route bridge. However, TCP/IP traffic can still make use of the PPP link using the IP routing function.

To support the data link switching function, a virtual ring segment number (X'999') has been assigned which will be used by all routers participating in DLS.

Various devices are attached to each Token-Ring Network to provide facilities to test the functionality of the scenario. These devices are:

os2mgr A LAN management station using IBM LAN Network Manager with IBM Operating System/2 Version 1.30.2 running on an IBM Personal System/2.

ps2bridge Half of a remote source route bridge using IBM Token-Ring Network Bridge Program Version 2.2 (5871-A1R) with IBM DOS Version 5 running on an IBM Personal System/2.

os2wkstn A test workstation using IBM Operating System/2 Version 1.30.2 running on an IBM Personal System/2 configured for 3270 emulation and as a LAN Requester.

os2serv A NetBIOS based LAN Server using IBM OS/2 LAN Server Version 1.3 with IBM Operating System/2 Version 1.30.2 running on an IBM Personal System/2.

os2sdlc An SDLC attached test workstation using IBM Operating System/2 Version 1.30.2 running on an IBM Personal System/2 configured for 3270 emulation.

3745 An SNA gateway to support access to an IBM Enterprise System/9000 by the test workstation.

8230 An active wiring concentrator to be managed by the LAN management station.

This scenario also includes all the other devices that participated in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145.

The following sections describe the configuration of the various systems that comprise this scenario.

7.1 Configuration of routera

This router is a 6611 Network Processor Model 170. There are three elements of the 6611 Network Processor that are configured to support this scenario:

- System Configuration
- System Management
- Adapter Configuration

The system management configuration for this scenario is identical to that for the first scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 13 on page 147 through Table 18 on page 148.

The configuration parameters for the remaining elements are described in the following sections.

7.1.1 System Configuration

System configuration comprises many components. Those components that should be configured to implement this scenario are summarized in Table 72 on page 169.

Table 72. routera - System Configuration Summary

SR Bridge	IP	IPX	XNS	DECnet	DLS
Yes	Yes	No	No	No	**Yes**

The IP component of system configuration is identical to that for the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 11 on page 146 and Table 12 on page 146.

The SR bridge component of system configuration is identical to that for the second example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 46 on page 159.

Each of the remaining system configuration components that must be configured to support this scenario are described in the following sections.

7.1.1.1 DLS: The parameters required to configure DLS are summarized in Table 73.

Table 73. routera - System Configuration - DLS Summary

Protocols Forwarded Via DLS - SNA	Yes
SNA - Default Destinations	None
SNA - Source and Destination Frame Filters	Disable
Protocols Forwarded Via DLS - NetBIOS	Yes
NetBIOS - Default Destinations	None
NetBIOS - Source and Destination Name Filters	None
Virtual Ring Segment Number	999
Destination Cache Timeout	8
Default DLS IP Address For This 6611	9.67.46.129
Accept Connections Only From Participating 6611 Routers	Yes
Participating DLS Routers	9.67.38.78

7.1.2 Adapter Configuration

The communication adapter features installed and interfaces used in this scenario are summarized in Table 74.

Table 74 (Page 1 of 2). routera - Adapter Configuration - Summary

Slot	Adapter	Port 0	Port 1	Port 2	Port 3
1	6611 2-Port Serial Adapter	N/A	**PPP**	Not Used	N/A
2	6611 Token-Ring Network 16/4 Adapter	N/A	**Used**	N/A	N/A
3	6611 4-Port SDLC Adapter	**EIA232D**	Not Used	Not Used	Not Used
4	6611 Ethernet Adapter	N/A	Not Used	N/A	N/A
5	Empty Slot				

Table 74 (Page 2 of 2). routera - Adapter Configuration - Summary					
Slot	**Adapter**	**Port 0**	**Port 1**	**Port 2**	**Port 3**
6	Empty Slot				
7	Empty Slot				

The configuration parameters for each communication interface that is used to implement this scenario are described in the following sections.

7.1.2.1 Slot 1, Port 1 (Serial): This communication interface is used to provide the PPP link to the other router ("routerb"). A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 75.

Table 75. routera - Slot 1, Port 1 (Serial) - Summary									
Physical Interface	**PPP**	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	Yes	Yes	**Yes**	Yes	No	No	No	No	No

The physical interface, PPP, and IP configuration parameters for this scenario are identical to those used in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 21 on page 149 through Table 23 on page 149.

The SR bridge configuration parameters for this scenario are identical to those used in the second example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 49 on page 160.

The parameters required to configure SR bridge filters are summarized in Table 76.

Table 76. routera - Slot 1, Port 1 (Serial) - SR Bridge Filter Summary			
Inbound MAC Address	Disable	**Outbound MAC Address**	Disable
Inbound Source SAP	Disable	**Outbound Source SAP**	**Enable**
Inbound SNAP Value	Disable	**Outbound SNAP Value**	Enable
Inbound Ring Number	Disable	**Outbound Ring Number**	Disable
Hop Count	7	**Frame Type**	Both SRB and ARB

The parameters required to configure the outbound SNAP value filter are identical to those used in the second example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 51 on page 160.

The parameters required to configure the outbound source SAP filter are listed in Table 77. The outbound source SAP filter should be configured to operate as a "Deny" filter on both SRB and ARB frames.

Table 77. routera - Slot 1, Port 1 (Serial) - Outbound Source SAP Filter		
Source SAP Value	**Source SAP Value**	**Source SAP Value**
X'04' (SNA)	X'F0' (NetBIOS)	

7.1.2.2 Slot 2, Port 1 (Token Ring): This communication interface is used to provide access to a Token-Ring Network. A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 78 on page 171.

Table 78. routera - Slot 2, Port 1 (Token Ring) - Summary								
Physical Interface	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	Yes	No	Yes	No	No	No	**Yes**	**Yes**

The physical interface and IP configuration parameters for this scenario are identical to those used in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 25 on page 150 and Table 26 on page 150.

The SR bridge and SR bridge filters parameters for this scenario are identical to those used in the second example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 53 on page 160 and Table 54 on page 161.

The parameters required to configure SNA are listed in Table 79.

Table 79. routera - Slot 2, Port 1 (Token Ring) - SNA	
Enable SNA Frame Forwarding On This Port	Yes
SAP Values For Frame Forwarding	X'04'

The parameters required to configure NetBIOS are listed in Table 80.

Table 80. routera - Slot 2, Port 1 (Token Ring) - NetBIOS	
Forward NetBIOS Frames On This Port	Yes
Forward NetBIOS Datagram And Datagram Broadcast Messages On This Port	Yes

7.1.2.3 Slot 3, Port 0 (SDLC): This communication interface is used to provide an SDLC link to "os2sdlc." A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 81.

Table 81. routera - Slot 3, Port 0 (SDLC) - Summary			
Enable Interface	Yes	**Serial Encoding**	NRZ
Request To Send	Continuous	**Bit Clocking**	External
Data Rate Select	Full	**Transmit Rate**	2400
Data Terminal Ready	DTR	**SNA Stations**	See Table 82

The parameters required to configure the SNA station "os2sdlc" are listed in Table 82.

Table 82 (Page 1 of 2). routera - Slot 3, Port 0 (SDLC) - SNA Station os2sdlc	
Station Address	X'C1'
Station Token Ring Source Address	X'4000 3002 0022'
Station Token Ring Source SAP	X'04'
Station Token Ring Destination Address	X'4000 0124 0000'
Station Token Ring Destination SAP	X'04'
Station XID Value	X'05D 20022'
Primary Slow List Timeout	1
Retransmit Count	10
Retransmit Threshold	10

Table 82 (Page 2 of 2). routera - Slot 3, Port 0 (SDLC) - SNA Station os2sdlc	
Primary Repoll Threshold	10
Primary Repoll Count	15
Transmit Window Count	7
Maximum I-Frame Size	265
Force Disconnect Timeout	120
Primary Repoll Timeout	30

7.2 Configuration of routerb

This router is a 6611 Network Processor Model 170. There are three elements of the 6611 Network Processor that are configured to support this scenario:

- System Configuration
- System Management
- Adapter Configuration

The system management configuration for this scenario is identical to that for the first scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 30 on page 151 through Table 35 on page 152.

The configuration parameters for the remaining elements are described in the following sections.

7.2.1 System Configuration

System configuration comprises many components. Those components that should be configured to implement this scenario are summarized in Table 83.

Table 83. routerb - System Configuration Summary					
SR Bridge	**IP**	**IPX**	**XNS**	**DECnet**	**DLS**
Yes	Yes	No	No	No	**Yes**

The IP component of system configuration is identical to that for the scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 28 on page 150 and Table 29 on page 151.

The SR bridge component of system configuration is identical to that for the scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 56 on page 161.

Each of the remaining system configuration components that must be configured to support this scenario are described in the following sections.

7.2.1.1 DLS: The parameters required to configure DLS are summarized in Table 84.

Table 84 (Page 1 of 2). routerb - System Configuration - DLS Summary	
Protocols Forwarded Via DLS - SNA	Yes
SNA - Default Destinations	None
SNA - Source and Destination Frame Filters	Disable
Protocols Forwarded Via DLS - NetBIOS	Yes

Table 84 (Page 2 of 2). routerb - System Configuration - DLS Summary	
NetBIOS - Default Destinations	None
NetBIOS - Source and Destination Name Filters	None
Virtual Ring Segment Number	999
Destination Cache Timeout	8
Default DLS IP Address For This 6611	9.67.38.78
Accept Connections Only From Participating 6611 Routers	Yes
Participating DLS Routers	9.67.46.129

7.2.2 Adapter Configuration

The communication adapter features installed and interfaces used in this scenario are summarized in Table 85.

Table 85. routerb - Adapter Configuration - Summary					
Slot	**Adapter**	**Port 0**	**Port 1**	**Port 2**	**Port 3**
1	6611 2-Port Serial Adapter	N/A	**PPP**	**LAN Bridge**	N/A
2	6611 Token-Ring Network 16/4 Adapter	N/A	**Used**	N/A	N/A
3	Empty Slot				
4	Empty Slot				
5	Empty Slot				
6	Empty Slot				
7	Empty Slot				

The configuration parameters for each communication interface that is used to implement this scenario are described in the following sections.

7.2.2.1 Slot 1, Port 1 (Serial): This communication interface is used to provide the PPP link to the other router ("routera"). A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 86.

Table 86. routerb - Slot 1, Port 1 (Serial) - Summary									
Physical Interface	**PPP**	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	Yes	Yes	**Yes**	Yes	No	No	No	No	No

The physical interface, PPP and IP configuration parameters for this scenario are identical to those used in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 38 on page 153 through Table 40 on page 153.

The SR bridge configuration parameters for this scenario are identical to those used in the second example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 59 on page 162.

The parameters required to configure SR bridge filters are summarized in Table 87 on page 174.

Table 87. routerb - Slot 1, Port 1 (Serial) - SR Bridge Filter Summary			
Inbound MAC Address	Disable	**Outbound MAC Address**	Disable
Inbound Source SAP	Disable	**Outbound Source SAP**	**Enable**
Inbound SNAP Value	Disable	**Outbound SNAP Value**	Enable
Inbound Ring Number	Disable	**Outbound Ring Number**	Disable
Hop Count	7	**Frame Type**	Both SRB and ARB

The parameters required to configure the outbound SNAP value filter are identical to those used in the second example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 61 on page 163.

The parameters required to configure the outbound source SAP filter are listed in Table 88. The outbound source SAP filter should be configured to operate as a "Deny" filter on SRB and ARB frames.

Table 88. routerb - Slot 1, Port 1 (Serial) - Outbound Source SAP Filter		
Source SAP Value	**Source SAP Value**	**Source SAP Value**
X'04' (SNA)	X'F0' (NetBIOS)	

7.2.2.2 Slot 1, Port 2 (Serial): This communication interface is used to provide the LAN bridging protocol link to the PS/2 bridge ("ps2bridge"). A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 89.

Table 89. routerb - Slot 1, Port 2 (Serial) - Summary					
Physical Interface	**LAN Bridge Port Defaults**	**SR Bridge**	**SR Bridge Filters**	**SNA**	**NetBIOS**
Yes	Yes	Yes	No	**Yes**	**Yes**

The physical interface, LAN bridge port defaults, SR bridge and SR bridge filters configuration parameters for this scenario are identical to those used in the example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 63 on page 163 through Table 67 on page 164.

The parameters required to configure SNA are listed in Table 90.

Table 90. routerb - Slot 1, Port 2 (Serial) - SNA	
Enable SNA Frame Forwarding On This Port	Yes
SAP Values For Frame Forwarding	X'04'

The parameters required to configure NetBIOS are listed in Table 91.

Table 91. routerb - Slot 1, Port 2 (Serial) - NetBIOS	
Forward NetBIOS Frames On This Port	Yes
Forward NetBIOS Datagram And Datagram Broadcast Messages On This Port	Yes

7.2.2.3 Slot 2, Port 1 (Token-Ring): This communication interface is used to provide access to a Token-Ring Network. A summary of the parameters that should be configured for this interface to implement this scenario is provided in Table 92 on page 175.

Table 92. routerb - Slot 2, Port 1 (Token Ring) - Summary								
Physical Interface	**SR Bridge**	**SR Bridge Filters**	**IP**	**IPX**	**XNS**	**DECnet**	**SNA**	**NetBIOS**
Yes	Yes	No	Yes	No	No	No	**Yes**	**Yes**

The physical interface and IP configuration parameters for this scenario are identical to those used in the first example scenario described in Chapter 5, "Basic TCP/IP Example Scenario" on page 145. See Table 42 on page 154 and Table 43 on page 154.

The SR bridge and SR bridge filters configuration parameters for this scenario are identical to those used in the second example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See Table 69 on page 164 and Table 70 on page 164.

The parameters required to configure SNA are listed in Table 93.

Table 93. routerb - Slot 2, Port 1 (Token Ring) - SNA	
Enable SNA Frame Forwarding On This Port	Yes
SAP Values For Frame Forwarding	X'04'

The parameters required to configure NetBIOS are listed in Table 94.

Table 94. routerb - Slot 2, Port 1 (Token Ring) - NetBIOS	
Forward NetBIOS Frames On This Port	Yes
Forward NetBIOS Datagram And Datagram Broadcast Messages On This Port	Yes

7.3 Configuration of Other Systems

Many of the other systems in this example scenario require no special configuration to make use of the data link switching environment provided by the 6611 Network Processors. That is, they would be configured in exactly the same manner as if they were all attached to the same Token-Ring Network segment. This applies to the following systems in the example scenario:

- os2wkstn
- os2serv
- 8230

Those aspects of the configuration for "os2mgr" and "ps2bridge" that must be configured to interoperate correctly with the 6611 Network Processors are identical to those used in the second example scenario described in Chapter 6, "Remote Source Route Bridging Example Scenario" on page 157. See 6.3.1, "Configuration of os2mgr" on page 165 and 6.3.2, "Configuration of ps2bridge" on page 166.

Those aspects of the configuration for "os2sdlc" and "3745" that must be configured to interoperate correctly with the 6611 Network Processors are described in the following section.

7.3.1 Configuration of os2sdlc

To attach to "routera," the OS/2 EE Communications Manager for "os2sdlc" must be configured. The only OS/2 EE Communications Manager parameters that must correspond to those configured in "routera" are those in the SDLC DLC profile which is illustrated in Table 95 on page 176.

Table 95. os2sdlc - OS/2 EE Communications Manager SDLC DLC Profile			
Load DLC	Yes	**Free Unused Link**	Yes
Maximum RU Size	256	**Send Window Count**	7
Receive Window Count	7	**Line Type**	Non-Switched
Link Station Role	Secondary	**Line Mode**	Line Turnaround Required
NRZI	No	**Modem Rate**	Full
Local Station Address	X'C1'		

7.3.2 Configuration of 3745

The aspects of the configuration for "3745" that must be configured to interoperate correctly with the 6611 Network Processors are:

- The MAC address of the "3745" TIC must be the same as that configured for the "Station Token Ring Destination Address" parameter for the SNA station "os2sdlc" on "routera." In this example scenario the MAC address of the "3745" TIC is X'4000 0124 0000'.
- The VTAM that owns the "3745" TIC should contain a definition in a VTAM switched major node that corresponds to the "Station XID Value" parameter for the SNA station "os2sdlc" on "routera." In this example scenario the VTAM switched major node definition is for a PU type 2.0 with an IDBLK of X'05D' and a IDNUM of X'20022'.

Part 4. Appendix

Appendix A. TCP/IP Routing Table Maintenance Protocols

This appendix gives an introduction to Routing Table Maintenance Protocols for TCP/IP.

For a full understanding of the routing parameters an in-depth knowledge of TCP/IP routing protocols is needed. Refer to *Internetworking with TCP/IP Volume 1: Principles, Protocols and Architecture, SC31-6144*, and *TCP/IP Tutorial and Technical Overview, GG24-3376-02*.

The goal of routing is to get to a *host*. In the TCP/IP world a host is any computer. Hosts are known by their IP address. IP routing is then based on routing tables that know how to get to these hosts. Hosts that maintain these routing tables and that perform the routing function are called *gateways* (although the term *routers* is being used more and more). Entries in these routing tables are either empty, if the host is on the same physical network as the router, or contain the IP address of a router. These tables are either coded by hand (*static routes*), or they can be built dynamically (*dynamic routes*). Protocols that support the dynamic table updating are called *Routing Table Maintenance Protocols*.

A.1 Internet Addressing

IP addresses are 32 bits long and usually represented in a dotted decimal format. This IP address consists of a network address and a host address. For example:

```
00001001 01000011 00010110 01000000  as the 32 bit address
00001001 01000011 00010110 01000000  the 4 octets
   9        67        38      64    dotted decimal 9.67.38.64
```

The IP address consists of a *network address* and a *host address* on that network. The portion of the address that is used to define either of these is defined by its *class*. The three main classes are A, B and C. Classes D and E are also defined in the standard but will not be discussed here.

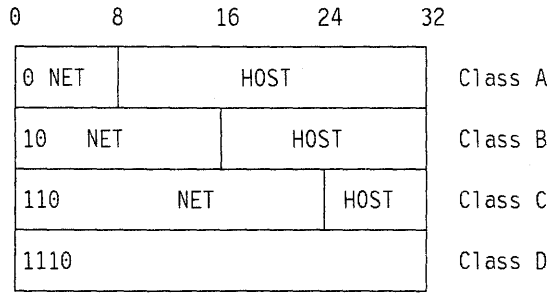


Figure 89. Classes of IP Addresses

Classes can be recognized by their high order bits. Class A starts with a "0," Class B addresses start with a "10," and Class C starts with "110." Class A addresses are allocated to networks with many hosts. For example, IBM uses

Class A IP addresses. Class B addresses are for intermediate size networks and Class C are for small networks. Classes are allocated by a central authority, the *Network Information Center (NIC)*.

To define the class of an address based on its dotted decimal value consider the following:

```
Class A addresses range
00000000.00000000.00000000.00000000 to
01111111.00000000.00000000.00000000

or 0.0.0.0 to 127.0.0.0

Class B addresses range
10000000.00000000.00000000.00000000 to
10111111.11111111.00000000.00000000

or 128.0.0.0 to 191.255.0.0

Class C addresses range
11000000.00000000.00000000.00000000 to
11011111.11111111.11111111.00000000

or 192.0.0.0 to 223.255.255.0
```

An IP address of 9.67.38.54 is thus a Class A address.

The IP addressing scheme defines one address for the whole network. Many networks consist of multiple subnets, for example several token-ring and Ethernet LANs connected to and accessible via one router. Each LAN would like to have its own IP network address. See Figure 90.

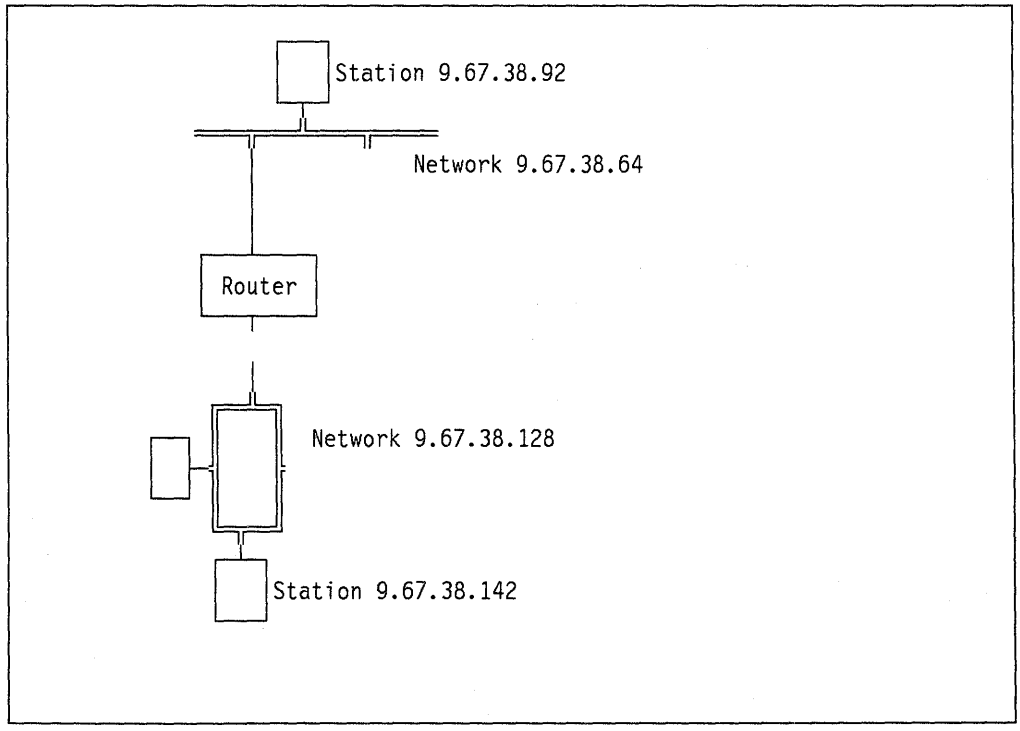


Figure 90. The Need for Subnets

A Class A network can have more than 65536 hosts. Dividing these hosts into subnetworks can be achieved by *subnetting*. Subnetting sets aside part of the host address area as described in Figure 91.

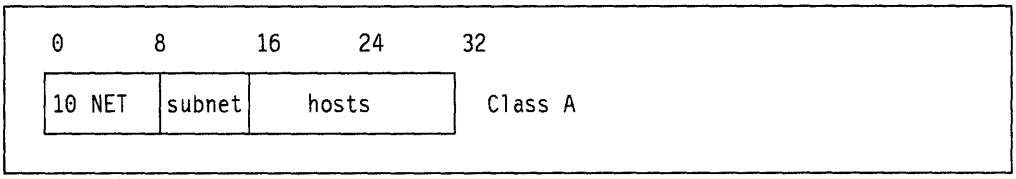


Figure 91. Subnet Mask

Simply stated a subnet mask identifies which part of the IP address represents the network (set to "1") and which part represents the host (set to "0").

The IP address range 9.67.38.0 is split into subnets with a *subnet mask*:

```
IP address 9.67.38.0 or
00001001.01000011.00100110.00000000

with subnet mask 255.255.255.192 or
111111111.11111111.11111111.11000000

gives the following range              subnet        hosts

00001001.01000011.00100110.00xxxxxx  9.67.38.0      0 through 63
00001001.01000011.00100110.01xxxxxx  9.67.38.64     65 through 126
00001001.01000011.00100110.10xxxxxx  9.67.38.128    129 through 190
00001001.01000011.00100110.11xxxxxx  9.67.38.192    192 through 254
```

So when an IP address of 9.67.38.96 with subnet mask of 255.255.255.192 needs to be located, the network that will be routed to will be the result of the logical "AND" between these two, or 9.67.38.64.

A.2 IP Routing

A.2.1 Direct and Indirect Routing

Direct routing can only take place when the two hosts are directly connected on the same physical network. This network can be a physical Token-Ring or an Ethernet, but also a bridged token-ring or Ethernet, or even a token-ring bridged to an Ethernet

Indirect routing takes place when the destination is not on a directly attached network.

A routing table would look something like this:

```
Host A  Address 9.67.38.4

Routing table :

Destination        Gateway
9.67.38.3          9.67.38.4 (host A's network interface)
```

```
9.1.1.2          9.67.38.5 (route added statically to
                           specify router to use to get to
                           9.1.1.2)
```

When Host A receives a datagram for network address 9.67.38.3 it will recognize the network ID and send it through its port with address 9.67.38.4. When Host A receives a datagram for 9.1.1.2 it will route it to the IP address of the gateway as defined in its static route table.

A.3 Routing Table Maintenance Protocols

When networks become large it is no longer possible to maintain static routing tables. Static routes are manually configured in all machines and when a change is made to the network, changes will have to be made in all of the routing tables in all machines.

Note: The definition of a *gateway* in the TCP/IP world is different from the one used in general network terms where it is used to describe the function of a machine that links different network architectures. Refer also to 1.3, "Internetworking and Bridging" on page 11. For the purpose of this introduction the TCP/IP definition of a gateway will be maintained where required, and will be replaced by *router* in other cases.

A.3.1 The Core Architecture

For a detailed description of the core gateway system, please refer to RFC 823 and RFC 1009.

One of the first architectures implemented for large internets used the concept of *core* and *noncore* gateways. The core system has a central group of *core* gateways that exchange all information with each other.

Outside of this central core there are *noncore* gateways that do not exchange routing information with the *core* gateways. These noncore gateways have the routing information about their local network but will not propagate this information to the core gateways. They will have a default route defined to a core gateway through which they will access any hosts they do not know about. See Figure 92 on page 183.

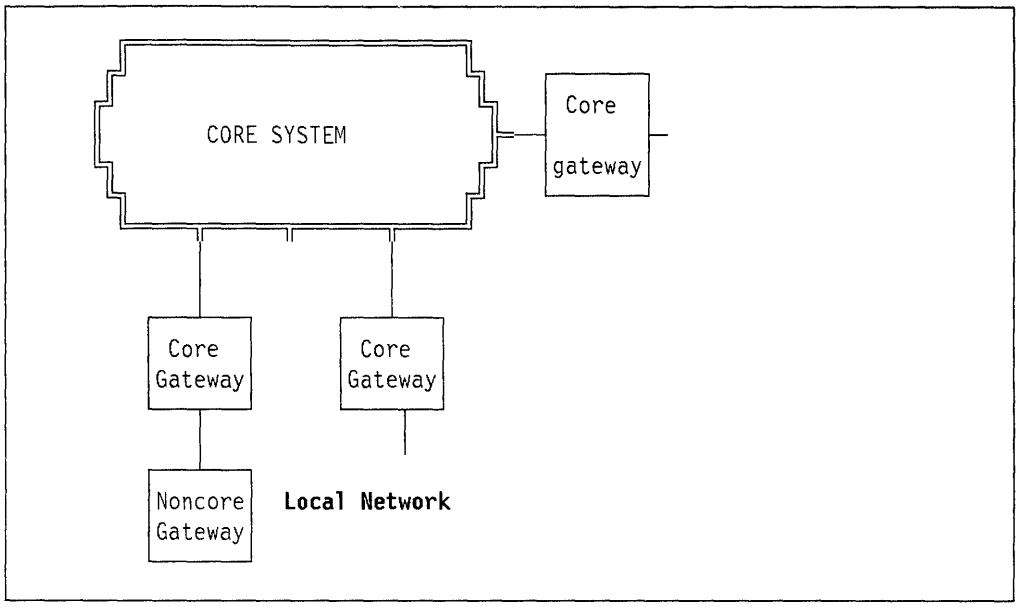


Figure 92. The Core Routing Architecture

A.3.2 The Autonomous System (AS)

In the core architecture, the **Local Networks** use the core system as a default for the hosts they do not know about. A problem arises however when the internets become large and the core system needs to ensure it knows the current routing information about the IP networks within the local networks.

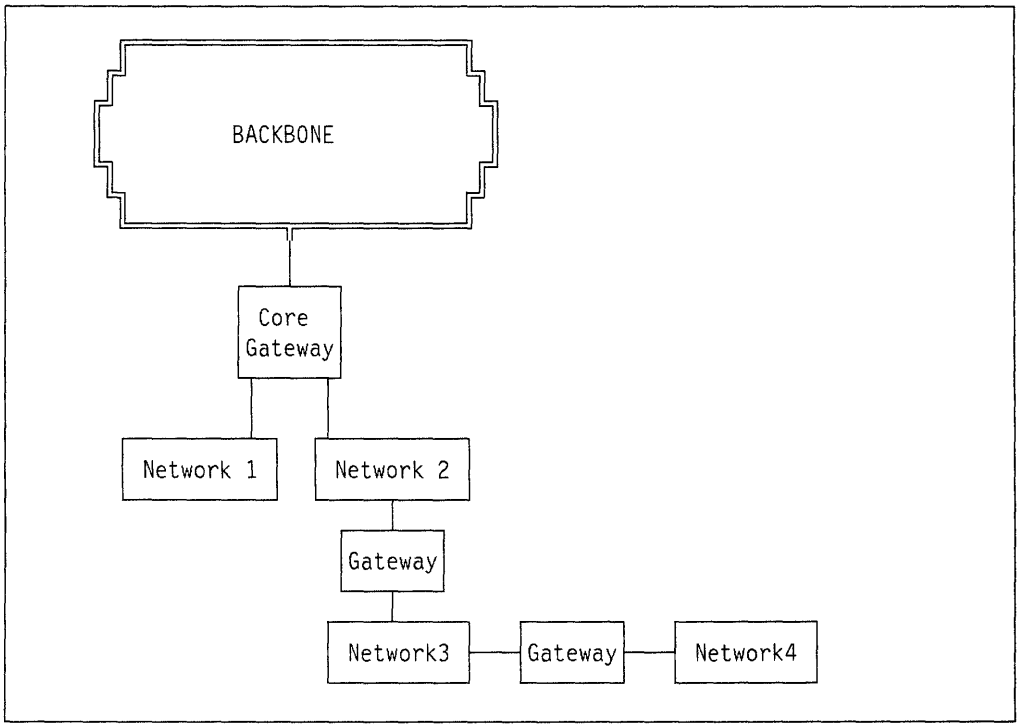


Figure 93. Multiple Networks and Gateways

In Figure 93 the set of Networks 1 to 4 are considered an *Autonomous System* or AS. Each AS is allowed to make its own decisions about routing. They can

decide how routes are propagated and how the routes are maintained. Each AS sends routing information to the other AS.

Based on this definition, the core system is in itself an autonomous system. In a core system this means that the AS will send routing information to the core gateway that connects to the backbone.

Referring to Figure 93 on page 183, Networks 1 through 4 would advertise routing information to the core gateway (which itself forms part of the AS).

The protocols that are used by gateways *inside* an AS are defined as *Interior Gateway Protocols* or *IGPs*. The IGPs supported by the IBM 6611 Network Processor are:

- Hello
- RIP
- OSPF

To advertise routing information between ASs, *Exterior Gateway Protocol* or EGP is used.

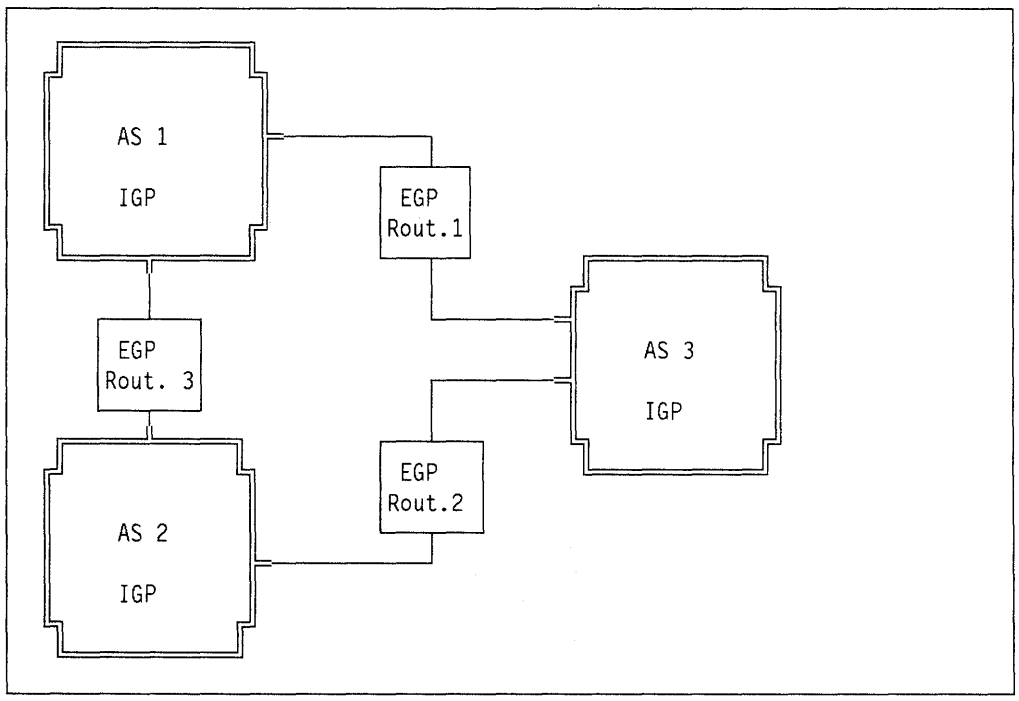


Figure 94. Relationship between EGPs and IGPs

A.3.3 Vector-Distance Routing

Routing tables not only keep information of what router to use to get to a host but also some distance information. *Vector Distance* routing uses the hop count as a measure for the distance. A network that is directly attached to a gateway has a hop count of 0. Each new router adds a hop count of 1 to the distance.

Initially, the Vector-Distance table in a router will show a distance of 0 for every network it attaches to directly. See Figure 95 on page 185.

Destination	Distance
Network 1	0
Network 2	0

Figure 95. Initial Vector-Distance Routing Table

If either Network 1 or Network 2 has other routers on it, it will propagate its routing table. As such, the initial table will grow while it receives information from the other routers.

Route Table I

Destination	Distance	Route
Net 1	0	direct
Net 2	0	direct
Net 4	9	Router 1
Net 17	3	Router 2
Net 24	5	Router 3
Net 30	7	Router 7
Net 42	4	Router 11

Route Table II

Destination	Distance
Net 1	2
Net 4	3
Net 17	6
Net 24	4
Net 24	7
Net 30	13
Net 42	3

Figure 96. Vector-Distance Routing

In Figure 96 Route Table I and Route Table II each in a different router, will exchange information and verify that the path to Net 4 is shorter via router II. Consequently route table I will be updated with a distance to Net 4 of 4.

Using this simple technique all routes within a static environment will be quickly propagated. However this technique has major limitations. One limitation is that the hop count does not make any distinctions between the speed over these hops. For example, a host that is 3 hops away over token-ring can be accessed faster than a host that is 2 hops away over 1200 bps lines. A second limitation is with the changing environment. In a completely static environment, vector-distance algorithms propagate routes to all destinations. When routes change rapidly, however, the computations may not stabilize; this is known as the *Convergence Problem*.

A.3.4 Shortest Path First Routing (SPF)

Shortest Path First or SPF routing is also known as *link-state* routing. SPF algorithms require that participating routers have a complete topology map of the Autonomous Systems. This topology is nothing more than a map, where the routers are the nodes and the connections between them are the links. A link is only defined if two routers can communicate directly. Each participating router has an identical database. Each individual piece of this database is a particular router's local state, for example, the router's usable interfaces and reachable neighbors. The router distributes its local state throughout the Autonomous System by flooding.

All routers run the exact same algorithm in parallel. From the topological database, each router constructs a tree of shortest paths with itself as root. This shortest-path tree gives the route to each destination in the Autonomous System. Externally derived routing information appears on the tree as leaves.

To maintain this map of the internet, routers using SPF algorithms do not send messages containing lists of destinations like the vector-distance protocols, but instead they gather information in the following way:

1. A test is run on the active status of all neighboring routers. A neighbor is defined as a router on a directly attached network. If the neighbor replies to the test message, the link is said to be up. If there is no reply the link in down.
2. The routers then periodically broadcast their link status to all other routers. This information does not contain any routes, merely the status of the link with their neighbor.

In this way, by all routers sending information about their neighbors, all the routers build a complete map of the internet. From this topology map the SPF algorithms can calculate the shortest path to all destinations. When a link status is changed then this information is re-calculated to come up with the next shortest path.

A.3.5 Exterior Gateway Protocol (EGP)

For a detailed description of the EGP protocol, please refer to RFC 904.

EGP gateways forward reachability information only for networks within their AS. As EGP is by definition an exterior gateway protocol it sits on the border of an AS and communicates with other ASs. How the information is gathered within the AS is not specified and is defined by the IGP used in each AS. Refer to Figure 94 on page 184 .

EGP has 3 parts:

Neighbor Acquisition Before an exterior gateway can obtain information from another exterior gateway, it must acquire that gateway as a neighbor. To do this they will use a simple two-way handshake. The commands used to this end are: *Acquisition Request, Confirm, and Refuse* to set up the peer-to-peer relationship and *Cease Request and Confirm* to stop the relationship. The choice of partner is not made by EGP itself. It is up to the system administrator to define the EGP gateways.

The message format is as shown in Figure 97 on page 187. The *Hello Interval* is used to define the time interval for testing whether the neighbor is alive. The *POLL Interval* is used to define the time interval to request routing updates.

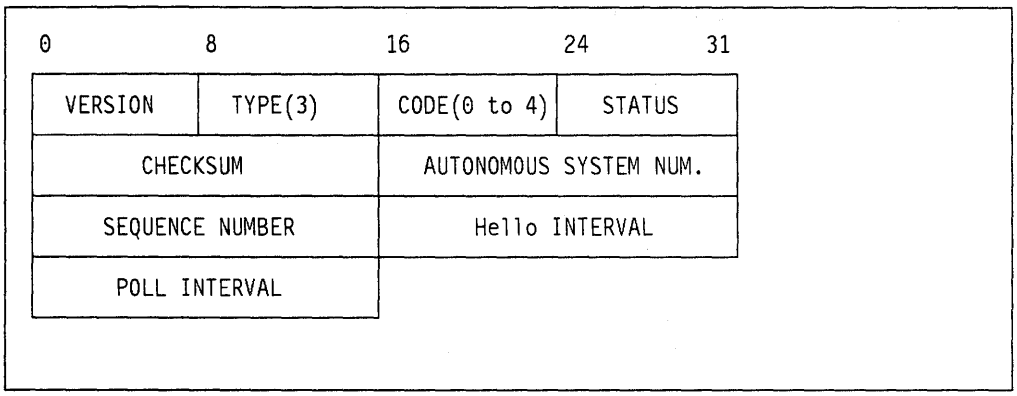


Figure 97. Neighbor Acquisition Message Format

Neighbor Reachability A gateway must have real-time information on the reachability of its neighbors. To achieve this, EGP uses a *Hello* and an *I Hear You* message. As these messages can get lost in the network, leading to a possible false assumption that the neighbor is no longer active, EGP uses a *k-out-of-n* rule. The meaning of this is that at least k out of the last n exchanges must fail before the status update will be accepted.

Network Reachability Neighbors maintain information about the network reachability by using the *Poll Request* and the *Poll Response* messages. Figure 98 gives the format of these messages. The *IP Source Network* refers to the network common to the autonomous systems to which both gateways attach.

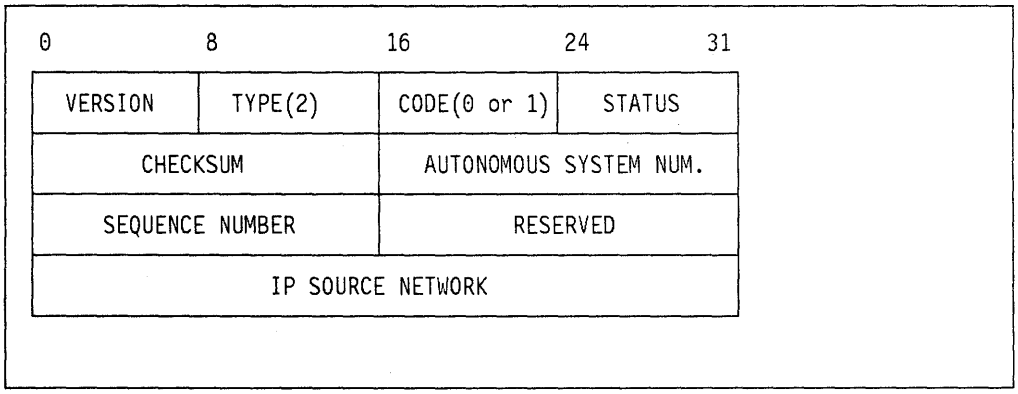


Figure 98. EGP Poll Message Format or NR Message

This *IP Source Network* is the source to which distances are measured. Remember that a gateway connects to two or more physical networks. If EGP is implemented and a Poll Request arrives it would not know over which network it arrived. So if a neighbor receives information about networks that are reachable via a neighbor gateway, the router will assume that this is *the* route to those networks.

The result of a poll request is a *Routing Update* message from the acquired neighbor. Polls from non-neighbors are responded to with an EGP *Error* message.

A.3.6 Routing Information Protocol (RIP)

For a detailed description of RIP, please refer to RFC 1058.

One of the most popular Interior Gateway Protocols (IGPs) is *Routing Information Protocol (RIP)* . RIP is also widely known by the name of the program that implements it, *routed* (pronounced *route D*, after the route daemon).

The full specification for RIP is given by *RFC 1058 Routing Information Protocol.*

RIP is an implementation of the vector-distance routing algorithm, as described in A.3.3, "Vector-Distance Routing" on page 184. RIP has two modes of operation, *active* and *passive* or *silent*. Active gateways advertise their routes to others, passive machines listen and update their routes based on the advertisements of the active gateways. Hosts can be passive gateways supporting RIP.

The active gateways broadcast a message on a regular basis, typically every 30 seconds. Being a vector-distance routing protocol the message contains pairs of IP network addresses together with a distance value. This distance value is measured in *HOP counts*. This is also known as the *Hop Count Metric*. RIP will define a hop count of 1 for a gateway that is directly connected to this gateway. A hop count of 2 means that a second gateway will be passed before reaching the destination.

Several problems exist with this scheme and we will discuss some solutions:

Count to Infinity Take the example as described in Figure 99. Problems arise when both Router 1 and Router 2 believe the other has routing information to Net 1. Router 1 has a connection to Net 1 with hop count 1, Router 2 has hop count 2 and so on. When Router 1 loses its connection to Net 1, it will update its hop count to 16 meaning infinity. Router 1 will receive the routing table information from Router 2 and will update its table's distance to Net 1 from 16 to 3 based on Router 2's hop count of 2. Router 1 will send its routing information to Router 2 at which time Router 2 will update its distance hop count to Net 1 to 4 based on the hop count of 3 as Router 1's distance vector to Net 1. This will go back and forth and will increase until both reach the value of 16, meaning Net 1 cannot be reached. This problem is known as the *Slow Convergence* or *Count to Infinity* problem.

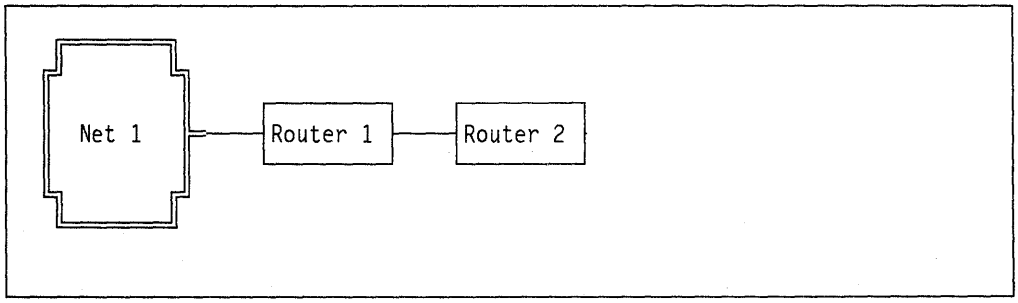


Figure 99. The Slow Convergence - Count to Infinity Problem

Split Horizon Most looping problems arise when all gateways advertise all routes on all network interfaces. The problem can be solved by remembering the interface over which information about a route was received and not sending information on that route back out over that same interface. This is known as *Split Horizon*. In the example of Figure 99 on page 188, Router 2 would not send back to Router 1 information on how to get to Net 1.

Poison Reverse Split horizon will still not prevent an invalid route remaining in the internet due to the time it takes to propagate the information. It could be said that *Good news travels fast, bad news doesn't*. Instead of not returning any information on the same interface the information about a certain route is propagated to all interfaces but with a metric set to infinity (16) for those routes acquired over that interface. This is known as *Poisoned Reverse*.

Triggered Updates To make *Poisoned Reverse* most effective, it must be combined with **Triggered Updates**. Triggered updates force a router to send an immediate broadcast when receiving bad news, instead of waiting for the next periodic broadcast. By sending an update immediately, a router minimizes the time it is vulnerable to believing good news.

RIP messages are sent out using UDP. The format is given in Figure 100 on page 190.

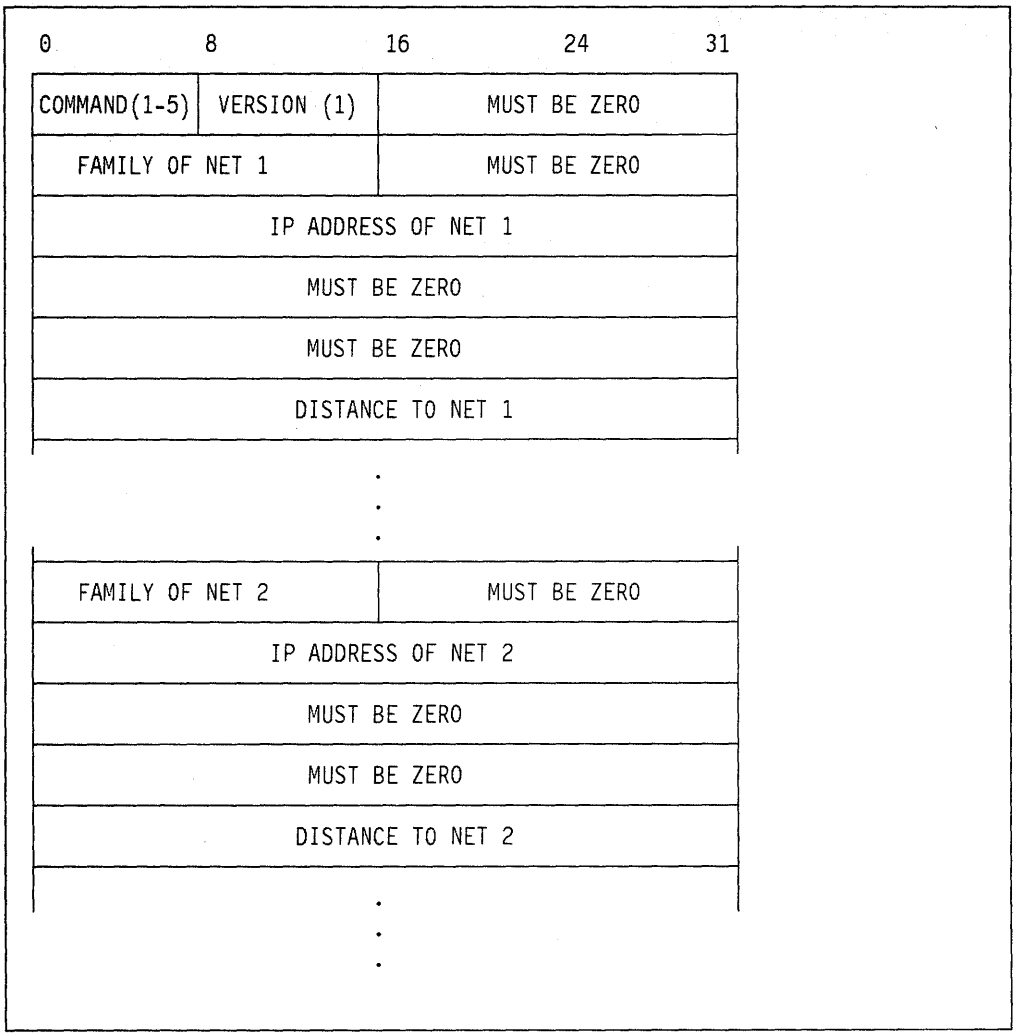


Figure 100. RIP Message Format

Family of Net 1 identifies the protocol family under which the network address should be interpreted. RIP uses values assigned to address families under the 4BSD UNIX operating system. In addition to normal IP addresses, RIP uses the convention that address 0.0.0.0. denotes a *default route*. How a host interprets the IP address supplied within a RIP message will depend on whether or not it knows the subnet mask that applies to the network. This would normally mean that routes to a subnet should not be sent outside the network of which the subnet is a part. *Distance to Net 1* contains an integer value specifying the hop count metric.

The hop count metric of 16, meaning infinity, limits the use of RIP to small networks.

A.3.7 The Hello Protocol

The *Hello* protocol is an IGP that uses a routing metric based on network delay rather than hop count. The Hello protocol is described in *RFC 891 - DCN Local-Network Protocols*.

Hello has two functions:

1. It synchronizes the clocks among a set of machines
2. It allows each machine to compute the shortest delay path to destinations

Each machine contains two tables:

Host Table It contains estimates of round trip delay and logical-clock offset, meaning the difference between the logical clock of this host and the logical clock of the sender's host. It is indexed by the host ID. The Host Table is maintained dynamically using updates generated by periodic (from 1 to 30 seconds) Hello messages.

Net Table It contains an entry for every neighbor network that may be connected to the local network and, in addition. certain other nets that are neighbors. Each entry contains the network number, as well as the host ID of the gateway (located on the local network) to that network. The Net Table is fixed at configuration time for all hosts except those that support an EGP gateway protocol. In these cases the Net Table is updated as part of the gateway operations.

The format of the Hello message is as follows:

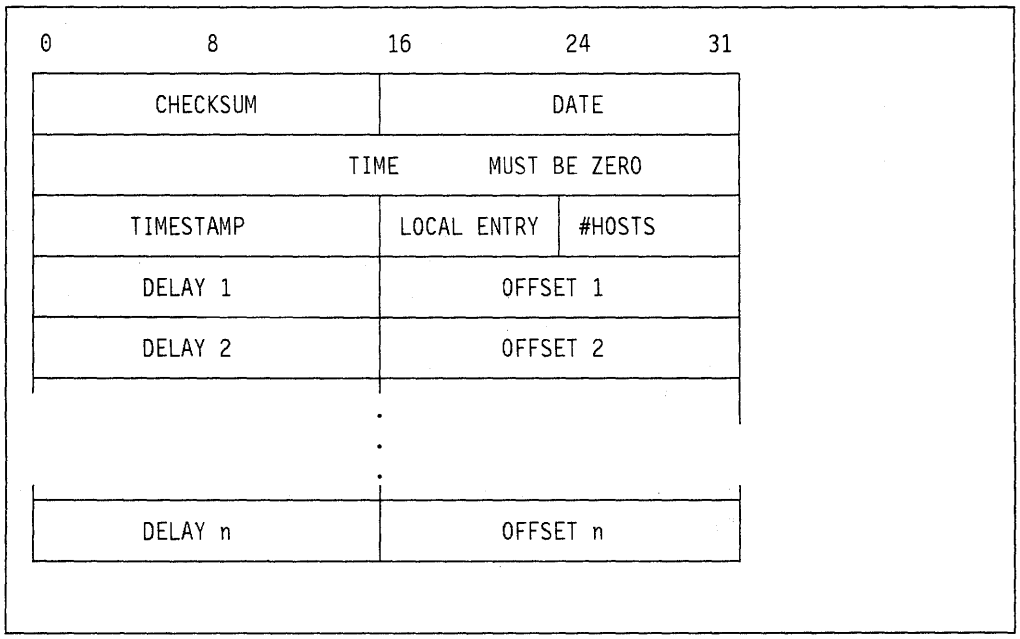


Figure 101. The Format of the Hello Message

The *TIMESTAMP* is used to calculate round trip computation. The field labelled *#HOSTS* specifies how many entries follow in the list of hosts. The field labelled *LOCAL ENTRY* contains the offset of the block of entries of internet addresses

used on the local network. Each entry contains two fields, *DELAY n* and *OFFSET n*, which gives the delay to get to host n and the offset from host n (difference between clocks).

Each machine periodically sends its neighbor a table of estimated delays for all other machines. Suppose Router 1 sends Router 2 a routing table that specifies destinations and delays. Router 2 examines each entry in the table. If Router 2's current delay to reach a given destination, n, is greater than the delay from 1 to n plus the delay from 2 to 1, Router 2 changes its route and sends traffic to Router n via Router 1. That is, Router 2 routes traffic to Router 1 as long as taking that path shortens the delay.

A.3.8 The Open Shortest Path (OSPF) Protocol

OSPF is an IP routing protocol that uses a *Shortest Path First (SPF)* algorithm as described in A.3.4, "Shortest Path First Routing (SPF)" on page 185. OSPF is an all new routing protocol and is the first attempt at a standardized routing table maintenance protocol. The protocol is described fully in *RFC 1131 The OSPF Specification*.

A number a definitions are new and will be described below:

Area Set of networks to be grouped together. The topology of an *area* is hidden from the rest of the AS. Routing within the area is determined only by the area's own topology; that is, each area has a separate topological database. This means that it is no longer true that all routers in the AS have an identical database. A router actually has a separate topological database for each area it is connected to (routers connected to multiple areas are called area border routers).

Multiaccess Network Those physical networks that support the attachment of multiple routers. Each pair of routers on such a network is assumed to be able to communicate directly.

Neighboring Router Two routers that have interfaces to a common network. On a multiaccess network, neighbors are dynamically discovered by the Hello protocol.

Adjacency A relationship formed between selected neighboring routers for the purpose of exchanging routing information. *Not* every pair of neighboring routers become adjacent; that is, *not* every pair of routers will stay synchronized.

Designated Router Each multiaccess network that has at least two attached routers, has a *Designated Router*. The Designated Router generates a link-state advertisement for the multiaccess network. It is elected by the Hello protocol. It becomes adjacent to all other routers on the network. Since the link-state databases are synchronized across adjacencies, the Designated Router plays a central part in the synchronization process.

Backup Designated Router In order to make the transition to a new Designated Router smoother, there is a Backup Designated Router for each multiaccess network. The Backup designated Router is also adjacent to all routers on the network, and

becomes Designated Router when the previous Designated Router fails.

Interfaces The connection between a router and one of its attached networks. An *interface* has state information associated with it which is obtained from the underlying lower-level protocols and the routing protocol itself.

Type of Service (TOS) Metrics In each type of link-state advertisement, different metrics can be advertised for each IP type of service. A metric for TOS 0 (used for OSPF routing protocol packets) must always be specified. OSPF calculates separate routes for each TOS. When several equal-cost routes to a destination exist, traffic is distributed equally among them.

As an example, suppose the point-to-point link between routers RT1 (IP address: 192.1.2.3) and RT6 (IP address: 6.5.4.3) is a satellite link. To encourage the use of this link for high bandwidth traffic, the AS administrator may set an artificially low metric for that TOS.

Link-State Advertisement Refers to the local state of a router or network. This includes the state of the router's interfaces and adjacencies. Each link-state advertisement is flooded throughout the routing domain. The collected link-state advertisement of all routers and networks forms the protocol's topological database.

Topological Database Also called *directed graph* or *Link-State database*. It is pieced together from link-state advertisements generated by the routers. Each router runs the SPF algorithm on its Link-State database resulting in shortest-path tree. The tree gives the entire route to any destination network or host.

Backbone The *backbone* consists of those networks that are not contained in any area, their attached routers, and those that belong to multiple areas. The *backbone* itself has all the properties of an area (its area ID is 0); that is, its topology is invisible to each of the areas, while it knows nothing of the topology of the areas. The backbone must be contiguous.

Virtual Link If areas are defined in such a way that the backbone is no longer contiguous, the system administrator must restore the backbone connectivity by configuring *virtual links*. This is of course because all inter-area traffic traverses the backbone. The two endpoints of a *virtual link* are area border routers. The virtual links must be configured in both routers. The configuration information in each router consists of the other virtual endpoint and the nonbackbone area the two routers have in common, also called the *transit area*.

The sequence performed by OSPF routers is the following:

1. Discovering OSPF neighbors
2. Electing the designated router

3. Bringing up adjacencies
4. Synchronization of databases
5. Calculation of the Routing table

All OSPF protocol exchanges are authenticated. This means that only trusted routers can participate in the Autonomous System's routing. A variety of authentication schemes can be used; a single authentication scheme is configured for each area. This enables some areas to use much stricter authentication than others.

Externally derived routing data, for example, routes learned from EGP, is passed transparently throughout the Autonomous System. This externally derived data is kept separate from the OSPF protocol's link-state data.

A.3.9 Combining RIP, Hello and EGP.

As described earlier in A.3.6, "Routing Information Protocol (RIP)" on page 188, RIP is implemented through a *routed* deamon. A new UNIX program called *gated* (pronounced 'gate' 'd') combines RIP, Hello, and EGP along with a set of rules that constrains how it advertises routes to exterior routers. Gated accepts RIP or Hello messages and modifies the local machine routing tables just like *routed* program, and it advertises routes from within its AS using EGP.

Appendix B. Configuration Reports for Example Scenarios

This appendix provides detailed configuration reports for the 6611 Network Processor configurations that were used to implement the example scenarios described in Part 3, "Example Scenarios" on page 143.

B.1 Basic TCP/IP Example Scenario

Detailed configuration reports for the two 6611 Network Processors used in this scenario are provided in the following sections.

B.1.1 routera

```
Ascii dump of Configuration Data for
Router 'routera' at Thu Jun 18 19:35:39 1992
Configuration: UNNAMED CONFIG

------------------------------------------------------------------------------
Object: Protocol Independent Parameters
     (slot 255, port 255, id 21500, count 1, size 100)

IBM 6611 Host Name: routera
IBM 6611 Domain name: itsc.raleigh.ibm.com
Enable name resolution by remote name servers: no
Enable time service by remote time servers: no

------------------------------------------------------------------------------
Object: List of Static Host to Internet Address Mappings
     (slot 255, port 255, id 21600, count 6, size 228)

IP Address of host: 9.67.38.65
Host name: vmesa

IP Address of host: 9.67.38.72
Host name: rs60002

IP Address of host: 9.67.38.73
Host name: rs60003

IP Address of host: 9.67.38.75
Host name: doscfg

IP Address of host: 9.67.38.78
Host name: routerb

IP Address of host: 9.67.46.130
Host name: os2wkstn

------------------------------------------------------------------------------
Object: Configuration Daemon Parameters
     (slot 255, port 255, id 20200, count 1, size 13)

Type of host access to this IBM 6611 for remote configuration
functions from the Configuration Program.: All hosts
Time period for application of configuration.: Immediately
Year: 0
```

```
Month: 0
Day: 0
Hour: 0
Minute: 0

------------------------------------------------------------------------
Object: Software Lock Parameters
     (slot 255, port 255, id 21200, count 1, size 1)

Lock Value: Unlock

------------------------------------------------------------------------
Object: Serial Line TTY Parameters
     (slot 255, port 255, id 22300, count 1, size 2)

baud rate (bps) for the S1 serial port: 9600
baud rate (bps) for the S2 serial port: 2400

------------------------------------------------------------------------
Object: List of Controlling User Names and Passwords
     (slot 255, port 255, id 22400, count 2, size 40)

User id: kellyjp
Password: *

User id: vannetel
Password: *

------------------------------------------------------------------------
Object: List of Viewing User Names and Passwords
     (slot 255, port 255, id 22401, count 2, size 40)

User id: collinsr
Password: *

User id: shogren
Password: *

------------------------------------------------------------------------
Object: SNMP System Contact
     (slot 255, port 255, id 22200, count 1, size 257)

System contact: Jaems Kelly or Ivan Van Netelbosch, Room CC-103

------------------------------------------------------------------------
Object: SNMP System Name
     (slot 255, port 255, id 22201, count 1, size 257)

System name: routera.itsc.raleigh.ibm.com

------------------------------------------------------------------------
Object: SNMP System Location
     (slot 255, port 255, id 22202, count 1, size 257)

System location: ITSC LAB, Building 657, Raleigh NC USA

------------------------------------------------------------------------
Object: SNMP Parameters
     (slot 255, port 255, id 22203, count 1, size 16)
```

```
Enterprise specific trap throttle time (0 - 3600 seconds): 900
Router Serial Number - Prefix: 26
Router Serial Number - Suffix: 24686
Enable SNMP: yes

------------------------------------------------------------------------------
Object: List of SNMP Communities
     (slot 255, port 255, id 22205, count 1, size 265)

Community IP address or Domain name: 9.67.0.0
Community address mask: 255.255.0.0
Community access: read only
Community name: ITSC
Community view name:

------------------------------------------------------------------------------
Object: List of SNMP Clients for Traps
     (slot 255, port 255, id 22204, count 2, size 276)

Trap IP address or Domain name: rs60002
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

Trap IP address or Domain name: rs60003
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

------------------------------------------------------------------------------
Object: List of IP Static Routes
     (slot 255, port 255, id 21002, count 1, size 17)

Destination IP Host or Network Address: 9.67.38.64
Destination mask: 255.255.255.192
Next hop router: 9.67.38.141
Preference (0 - 255): 50
Retain: yes

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 255, port 255, id 21000, count 1, size 35)

Connection Decay Interval: 10
Status Of All Defined IP Filters: disable

------------------------------------------------------------------------------
Object:
```

```
     (slot 255, port 255, id 20700, count 1, size 6)

------------------------------------------------------------------------
Object: RIP Parameters
     (slot 255, port 255, id 21800, count 1, size 4)

Enable Routing Information Protocol (RIP): no
Broadcast: yes
Zero Reserved Fields: yes
Route preference (0 - 255): 100

------------------------------------------------------------------------
Object: HELLO Parameters
     (slot 255, port 255, id 20800, count 1, size 3)

Enable Hello Protocol: no
Broadcast: yes
Route preference (0 - 255): 90

------------------------------------------------------------------------
Object: Parameters for EGP
     (slot 255, port 255, id 20500, count 1, size 12)

Enable Exterior Gateway Protocol (EGP): no
Preference (0 - 255): 200
Initial maximum packet size (1024 - 65535 bytes): 8192
Loc  Autonomous System Number: 0
Ge  ate default route.: no
Ena e EGP Import Filters: no
Default metric (0 - 255): 1

------------------------------------------------------------------------
Object: OSPF Parameters
     (slot 255, port 255, id 21405, count 1, size 6)

Enable OSPF: no
Router ID: 0.0.0.0

------------------------------------------------------------------------
Object: IPX Parameters
     (slot 255, port 255, id 21100, count 1, size 43)

Enable IPX router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined SAP Filters: enable
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable
SAP Filtering Mode: deny

------------------------------------------------------------------------
Object: XNS Parameters
     (slot 255, port 255, id 22500, count 1, size 41)

Enable XNS router: no
Split Horizon For RIP Filters: On
```

```
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable

------------------------------------------------------------------------------
Object: Protocol Bridging Parameters
     (slot 255, port 255, id 20100, count 1, size 39)

Enable Source Route Bridging: no
Bridge number: 0
Designated ring number (hex): 0x0

------------------------------------------------------------------------------
Object: Bridging Spanning Tree Parameters
     (slot 255, port 255, id 20101, count 1, size 5)

Bridge priority (hex): 0x8000
Hello time (seconds): 2
Forward delay time (seconds): 15
Max Age (seconds): 20

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 255, port 255, id 20300, count 1, size 57)

Enable DECnet router: no
Local address: 0.0
Node type: Routing_IV
Area maximum cost (1 - 1022): 1022
Area maximum hops: 30
Maximum address (1 - 1023): 1023
Maximum area (1 - 63): 63
Maximum cost (1 - 1022): 1022
Maximum hops: 30
Maximum paths: 1
Maximum visits: 63
Path split mode: Normal
Maximum broadcast non-routers (1 - 1022): 1022
Maximum broadcast routers (1 - 1022): 32
Buffer Size (246 - 1486 bytes): 1486

------------------------------------------------------------------------------
Object: Data Link Switch (DLS) Parameters
     (slot 255, port 255, id 20400, count 1, size 45)

Enable SNA frame forwarding: no
Enable NetBIOS frame forwarding: no
Virtual Ring Segment Number: 0x0
Accept connections only from specific 6611 routers: no
Destination cache timeout (minutes): 8
Default DLS IP address. this 6611.: 0.0.0.0

------------------------------------------------------------------------------
Object: SNA Frame Filter Parameters
     (slot 255, port 255, id 22100, count 1, size 37)
```

```
Source Frame Filter Type: permit
Destination Frame Filter Type: permit
Status Of All Defined SNA Source Frame Filters: enable
Status Of All Defined SNA Destination Frame Filters: enable

------------------------------------------------------------------------------
Object: NetBIOS Filter Parameters
     (slot 255, port 255, id 21300, count 1, size 37)

NetBIOS Destination Name Filter Type: permit
NetBIOS Source Name Filter Type: permit
Status Of All Defined NetBIOS Destination Name Filters: enable
Status Of All Defined NetBIOS  Source Name Filters: enable

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 1, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 1536000

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 1, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 1, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 1, id 2804, count 1, size 15)

Enable PPP on this port: yes
Maximum receive unit: 1500
```

```
Enable link quality monitoring: yes
Link quality monitoring interval: 10000

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: no
Ring number (hex): 0x0
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 2052
Hop Count Filter Type: Single route broadcast (SRB)
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: enable
Status of Inbound Ring Number Filters: enable
Status of Inbound MAC Address Filters: enable
Status of Inbound SNAP Filters: enable
Status of Outbound Ring Number Filters: enable
Status of Outbound MAC Address Filters: enable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: List of SAP Input Filters for SRB
     (slot 1, port 1, id 103, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------------
Object: List of SAP Output Filters for SRB
     (slot 1, port 1, id 107, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 180
```

```
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 1, id 1000, count 1, size 52)

IP Address: 9.67.38.140
Subnet mask: 255.255.255.192
Destination IP Address: 9.67.38.141
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 1, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

```
--------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

--------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 2, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 19200

--------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 2, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

--------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 2, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

--------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 2, id 2804, count 1, size 15)

Enable PPP on this port: no
Maximum receive unit: 1500
Enable link quality monitoring: no
Link quality monitoring interval: 10000

--------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 2, id 100, count 1, size 45)
```

```
Enable Source Route Bridging on this port: no
Ring number (hex): 0x0
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 2052
Hop Count Filter Type: Single route broadcast (SRB)
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: enable
Status of Inbound Ring Number Filters: enable
Status of Inbound MAC Address Filters: enable
Status of Inbound SNAP Filters: enable
Status of Outbound Ring Number Filters: enable
Status of Outbound MAC Address Filters: enable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 2, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 600
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 2, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 2, id 1100, count 1, size 32)
```

```
Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 2, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 2, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 2, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: Token-Ring Adapter Parameters
     (slot 2, port 1, id 2900, count 1, size 21)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Token Ring MAC Address: 00-00-00-00-00-00
Token Ring Data Rate: 4 Mbps
MAC Address Format: Non_canonical
Local / Non-local broadcast: Non_local

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 2, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: no
Ring number (hex): 0x0
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
```

```
Path cost (0 - 65535): 0
Maximum transmission unit: 2052
Hop Count Filter Type: Single route broadcast (SRB)
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: enable
Status of Inbound Ring Number Filters: enable
Status of Inbound MAC Address Filters: enable
Status of Inbound SNAP Filters: enable
Status of Outbound Ring Number Filters: enable
Status of Outbound MAC Address Filters: enable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------
Object: List of SAP Input Filters for SRB
     (slot 2, port 1, id 103, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------
Object: List of SAP Output Filters for SRB
     (slot 2, port 1, id 107, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 2, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------
Object: IP Parameters
     (slot 2, port 1, id 1000, count 1, size 52)

IP Address: 9.67.46.129
Subnet mask: 255.255.255.192
```

```
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 2, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 2, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 2, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 2, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 2, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 1, id 2700, count 1, size 18)
```

```
Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 2, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 2, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 3, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 3, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 4, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
```

```
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 4, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Ethernet Adapter Parameters
     (slot 4, port 1, id 2600, count 1, size 19)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Ethernet MAC Address (Canonical format): 00-00-00-00-00-00
Allow Multicasting: no

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 4, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 4, port 1, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 4, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: XNS Parameters
```

```
     (slot 4, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

B.1.2 routerb

```
Ascii dump of Configuration Data for
Router 'routerb' at Thu Jun 18 19:38:19 1992
Configuration: UNNAMED CONFIG

------------------------------------------------------------------------------
Object: Protocol Independent Parameters
     (slot 255, port 255, id 21500, count 1, size 100)

IBM 6611 Host Name: routerb
IBM 6611 Domain name: itsc.raleigh.ibm.com
Enable name resolution by remote name servers: no
Enable time service by remote time servers: no

------------------------------------------------------------------------------
Object: List of Static Host to Internet Address Mappings
     (slot 255, port 255, id 21600, count 6, size 228)

IP Address of host: 9.67.38.65
Host name: vmesa

IP Address of host: 9.67.38.72
Host name: rs60002

IP Address of host: 9.67.38.73
Host name: rs60003

IP Address of host: 9.67.38.75
Host name: doscfg

IP Address of host: 9.67.46.129
Host name: routera

IP Address of host: 9.67.46.130
Host name: os2wkstn

------------------------------------------------------------------------------
Object: Configuration Daemon Parameters
     (slot 255, port 255, id 20200, count 1, size 13)

Type of host access to this IBM 6611 for remote configuration
functions from the Configuration Program.: All hosts
Time period for application of configuration.: Immediately
Year: 0
```

```
Month: 0
Day: 0
Hour: 0
Minute: 0

------------------------------------------------------------------------
Object: Software Lock Parameters
     (slot 255, port 255, id 21200, count 1, size 1)

Lock Value: Unlock

------------------------------------------------------------------------
Object: Serial Line TTY Parameters
     (slot 255, port 255, id 22300, count 1, size 2)

baud rate (bps) for the S1 serial port: 9600
baud rate (bps) for the S2 serial port: 2400

------------------------------------------------------------------------
Object: List of Controlling User Names and Passwords
     (slot 255, port 255, id 22400, count 2, size 40)

User id: kellyjp
Password: *

User id: vannetel
Password: *

------------------------------------------------------------------------
Object: List of Viewing User Names and Passwords
     (slot 255, port 255, id 22401, count 2, size 40)

User id: collinsr
Password: *

User id: shogren
Password: *

------------------------------------------------------------------------
Object: SNMP System Contact
     (slot 255, port 255, id 22200, count 1, size 257)

System contact: James Kelly or Ivan Van Netelbosch, Room CC-103

------------------------------------------------------------------------
Object: SNMP System Name
     (slot 255, port 255, id 22201, count 1, size 257)

System name: routerb.itsc.raleigh.ibm.com

------------------------------------------------------------------------
Object: SNMP System Location
     (slot 255, port 255, id 22202, count 1, size 257)

System location: ITSC LAB, Building 657, Raleigh NC USA

------------------------------------------------------------------------
Object: SNMP Parameters
     (slot 255, port 255, id 22203, count 1, size 16)
```

```
Enterprise specific trap throttle time (0 - 3600 seconds): 900
Router Serial Number - Prefix: 26
Router Serial Number - Suffix: 06620
Enable SNMP: yes

------------------------------------------------------------------------
Object: List of SNMP Communities
     (slot 255, port 255, id 22205, count 1, size 265)

Community IP address or Domain name: 9.67.0.0
Community address mask: 255.255.0.0
Community access: read only
Community name: ITSC
Community view name:

------------------------------------------------------------------------
Object: List of SNMP Clients for Traps
     (slot 255, port 255, id 22204, count 2, size 276)

Trap IP address or Domain name: rs60002
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

Trap IP address or Domain name: rs60003
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

------------------------------------------------------------------------
Object: List of IP Static Routes
     (slot 255, port 255, id 21002, count 1, size 17)

Destination IP Host or Network Address: 9.67.46.128
Destination mask: 255.255.255.192
Next hop router: 9.67.38.140
Preference (0 - 255): 50
Retain: yes

------------------------------------------------------------------------
Object: IP Parameters
     (slot 255, port 255, id 21000, count 1, size 35)

Connection Decay Interval: 10
Status Of All Defined IP Filters: disable

------------------------------------------------------------------------
Object:
```

```
     (slot 255, port 255, id 20700, count 1, size 6)

------------------------------------------------------------------------------
Object: RIP Parameters
     (slot 255, port 255, id 21800, count 1, size 4)

Enable Routing Information Protocol (RIP): no
Broadcast: yes
Zero Reserved Fields: yes
Route preference (0 - 255): 100

------------------------------------------------------------------------------
Object: HELLO Parameters
     (slot 255, port 255, id 20800, count 1, size 3)

Enable Hello Protocol: no
Broadcast: yes
Route preference (0 - 255): 90

------------------------------------------------------------------------------
Object: Parameters for EGP
     (slot 255, port 255, id 20500, count 1, size 12)

Enable Exterior Gateway Protocol (EGP): no
Preference (0 - 255): 200
Initial maximum packet size (1024 - 65535 bytes): 8192
Local Autonomous System Number: 0
Generate default route.: no
Enable EGP Import Filters: no
Default metric (0 - 255): 1

------------------------------------------------------------------------------
Object: OSPF Parameters
     (slot 255, port 255, id 21405, count 1, size 6)

Enable OSPF: no
Router ID: 0.0.0.0

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 255, port 255, id 21100, count 1, size 43)

Enable IPX router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined SAP Filters: enable
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable
SAP Filtering Mode: deny

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 255, port 255, id 22500, count 1, size 41)

Enable XNS router: no
Split Horizon For RIP Filters: On
```

```
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable

------------------------------------------------------------------------------
Object: Protocol Bridging Parameters
     (slot 255, port 255, id 20100, count 1, size 39)

Enable Source Route Bridging: no
Bridge number: 0
Designated ring number (hex): 0x0

------------------------------------------------------------------------------
Object: Bridging Spanning Tree Parameters
     (slot 255, port 255, id 20101, count 1, size 5)

Bridge priority (hex): 0x8000
Hello time (seconds): 2
Forward delay time (seconds): 15
Max Age (seconds): 20

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 255, port 255, id 20300, count 1, size 57)

Enable DECnet router: no
Local address: 0.0
Node type: Routing_IV
Area maximum cost (1 - 1022): 1022
Area maximum hops: 30
Maximum address (1 - 1023): 1023
Maximum area (1 - 63): 63
Maximum cost (1 - 1022): 1022
Maximum hops: 30
Maximum paths: 1
Maximum visits: 63
Path split mode: Normal
Maximum broadcast non-routers (1 - 1022): 1022
Maximum broadcast routers (1 - 1022): 32
Buffer Size (246 - 1486 bytes): 1486

------------------------------------------------------------------------------
Object: Data Link Switch (DLS) Parameters
     (slot 255, port 255, id 20400, count 1, size 45)

Enable SNA frame forwarding: no
Enable NetBIOS frame forwarding: no
Virtual Ring Segment Number: 0x0
Accept connections only from specific 6611 routers: no
Destination cache timeout (minutes): 8
Default DLS IP address. this 6611.: 0.0.0.0

------------------------------------------------------------------------------
Object: SNA Frame Filter Parameters
     (slot 255, port 255, id 22100, count 1, size 37)
```

```
Source Frame Filter Type: permit
Destination Frame Filter Type: permit
Status Of All Defined SNA Source Frame Filters: enable
Status Of All Defined SNA Destination Frame Filters: enable

------------------------------------------------------------------------------
Object: NetBIOS Filter Parameters
     (slot 255, port 255, id 21300, count 1, size 37)

NetBIOS Destination Name Filter Type: permit
NetBIOS Source Name Filter Type: permit
Status Of All Defined NetBIOS Destination Name Filters: enable
Status Of All Defined NetBIOS  Source Name Filters: enable

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 1, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 1536000

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 1, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 1, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 1, id 2804, count 1, size 15)

Enable PPP on this port: yes
Maximum receive unit: 1500
```

```
Enable link quality monitoring: yes
Link quality monitoring interval: 10000

------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: no
Ring number (hex): 0x0
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 2052
Hop Count Filter Type: Single route broadcast (SRB)
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: enable
Status of Inbound Ring Number Filters: enable
Status of Inbound MAC Address Filters: enable
Status of Inbound SNAP Filters: enable
Status of Outbound Ring Number Filters: enable
Status of Outbound MAC Address Filters: enable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------
Object: List of SAP Input Filters for SRB
     (slot 1, port 1, id 103, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------
Object: List of SAP Output Filters for SRB
     (slot 1, port 1, id 107, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 180
```

```
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 1, id 1000, count 1, size 52)

IP Address: 9.67.38.141
Subnet mask: 255.255.255.192
Destination IP Address: 9.67.38.140
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 1, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

```
------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 2, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 19200

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 2, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 2, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 2, id 2804, count 1, size 15)

Enable PPP on this port: no
Maximum receive unit: 1500
Enable link quality monitoring: no
Link quality monitoring interval: 10000

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 2, id 100, count 1, size 45)
```

```
Enable Source Route Bridging on this port: no
Ring number (hex): 0x0
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 2052
Hop Count Filter Type: Single route broadcast (SRB)
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: enable
Status of Inbound Ring Number Filters: enable
Status of Inbound MAC Address Filters: enable
Status of Inbound SNAP Filters: enable
Status of Outbound Ring Number Filters: enable
Status of Outbound MAC Address Filters: enable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 2, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 600
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 2, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 2, id 1100, count 1, size 32)
```

```
Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 2, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 2, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 2, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------
Object: Token-Ring Adapter Parameters
     (slot 2, port 1, id 2900, count 1, size 21)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Token Ring MAC Address: 00-00-00-00-00-00
Token Ring Data Rate: 4 Mbps
MAC Address Format: Non_canonical
Local / Non-local broadcast: Non_local

------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 2, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: no
Ring number (hex): 0x0
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
```

```
Path cost (0 - 65535): 0
Maximum transmission unit: 2052
Hop Count Filter Type: Single route broadcast (SRB)
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: enable
Status of Inbound Ring Number Filters: enable
Status of Inbound MAC Address Filters: enable
Status of Inbound SNAP Filters: enable
Status of Outbound Ring Number Filters: enable
Status of Outbound MAC Address Filters: enable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: List of SAP Input Filters for SRB
     (slot 2, port 1, id 103, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------------
Object: List of SAP Output Filters for SRB
     (slot 2, port 1, id 107, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 2, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 2, port 1, id 1000, count 1, size 52)

IP Address: 9.67.38.78
Subnet mask: 255.255.255.192
```

```
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 2, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 2, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 2, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 2, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 2, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

B.2 Remote Source Route Bridging Example Scenario

Detailed configuration reports for the two 6611 Network Processors used in this scenario are provided in the following sections.

B.2.1 routera

```
Ascii dump of Configuration Data for
Router 'routera' at Thu Jun 18 20:26:10 1992
Configuration: UNNAMED CONFIG

------------------------------------------------------------------------------
Object: Protocol Independent Parameters
     (slot 255, port 255, id 21500, count 1, size 100)

IBM 6611 Host Name: routera
IBM 6611 Domain name: itsc.raleigh.ibm.com
Enable name resolution by remote name servers: no
Enable time service by remote time servers: no

------------------------------------------------------------------------------
Object: List of Static Host to Internet Address Mappings
     (slot 255, port 255, id 21600, count 6, size 228)

IP Address of host: 9.67.38.65
Host name: vmesa

IP Address of host: 9.67.38.72
Host name: rs60002

IP Address of host: 9.67.38.73
Host name: rs60003

IP Address of host: 9.67.38.75
Host name: doscfg

IP Address of host: 9.67.38.78
Host name: routerb

IP Address of host: 9.67.46.130
Host name: os2wkstn

------------------------------------------------------------------------------
Object: Configuration Daemon Parameters
     (slot 255, port 255, id 20200, count 1, size 13)

Type of host access to this IBM 6611 for remote configuration
functions from the Configuration Program.: All hosts
Time period for application of configuration.: Immediately
Year: 0
Month: 0
Day: 0
Hour: 0
Minute: 0

------------------------------------------------------------------------------
Object: Software Lock Parameters
     (slot 255, port 255, id 21200, count 1, size 1)

Lock Value: Unlock

------------------------------------------------------------------------------
Object: Serial Line TTY Parameters
     (slot 255, port 255, id 22300, count 1, size 2)
```

```
baud rate (bps) for the S1 serial port: 9600
baud rate (bps) for the S2 serial port: 2400

------------------------------------------------------------------------------
Object: List of Controlling User Names and Passwords
     (slot 255, port 255, id 22400, count 2, size 40)

User id: kellyjp
Password: *

User id: vannetel
Password: *

------------------------------------------------------------------------------
Object: List of Viewing User Names and Passwords
     (slot 255, port 255, id 22401, count 2, size 40)

User id: collinsr
Password: *

User id: shogren
Password: *

------------------------------------------------------------------------------
Object: SNMP System Contact
     (slot 255, port 255, id 22200, count 1, size 257)

System contact: Jaems Kelly or Ivan Van Netelbosch, Room CC-103

------------------------------------------------------------------------------
Object: SNMP System Name
     (slot 255, port 255, id 22201, count 1, size 257)

System name: routera.itsc.raleigh.ibm.com

------------------------------------------------------------------------------
Object: SNMP System Location
     (slot 255, port 255, id 22202, count 1, size 257)

System location: ITSC LAB, Building 657, Raleigh NC USA

------------------------------------------------------------------------------
Object: SNMP Parameters
     (slot 255, port 255, id 22203, count 1, size 16)

Enterprise specific trap throttle time (0 - 3600 seconds): 900
Router Serial Number - Prefix: 26
Router Serial Number - Suffix: 24686
Enable SNMP: yes

------------------------------------------------------------------------------
Object: List of SNMP Communities
     (slot 255, port 255, id 22205, count 1, size 265)

Community IP address or Domain name: 9.67.0.0
Community address mask: 255.255.0.0
Community access: read only
```

```
Community name: ITSC
Community view name:

------------------------------------------------------------------------------
Object: List of SNMP Clients for Traps
     (slot 255, port 255, id 22204, count 2, size 276)

Trap IP address or Domain name: rs60002
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

Trap IP address or Domain name: rs60003
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

------------------------------------------------------------------------------
Object: List of IP Static Routes
     (slot 255, port 255, id 21002, count 1, size 17)

Destination IP Host or Network Address: 9.67.38.64
Destination mask: 255.255.255.192
Next hop router: 9.67.38.141
Preference (0 - 255): 50
Retain: yes

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 255, port 255, id 21000, count 1, size 35)

Connection Decay Interval: 10
Status Of All Defined IP Filters: disable

------------------------------------------------------------------------------
Object:
     (slot 255, port 255, id 20700, count 1, size 6)

------------------------------------------------------------------------------
Object: RIP Parameters
     (slot 255, port 255, id 21800, count 1, size 4)

Enable Routing Information Protocol (RIP): no
Broadcast: yes
Zero Reserved Fields: yes
Route preference (0 - 255): 100

------------------------------------------------------------------------------
Object: HELLO Parameters
```

```
     (slot 255, port 255, id 20800, count 1, size 3)

Enable Hello Protocol: no
Broadcast: yes
Route preference (0 - 255): 90

------------------------------------------------------------------------------
Object: Parameters for EGP
     (slot 255, port 255, id 20500, count 1, size 12)

Enable Exterior Gateway Protocol (EGP): no
Preference (0 - 255): 200
Initial maximum packet size (1024 - 65535 bytes): 8192
Local Autonomous System Number: 0
Generate default route.: no
Enable EGP Import Filters: no
Default metric (0 - 255): 1

------------------------------------------------------------------------------
Object: OSPF Parameters
     (slot 255, port 255, id 21405, count 1, size 6)

Enable OSPF: no
Router ID: 0.0.0.0

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 255, port 255, id 21100, count 1, size 43)

Enable IPX router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined SAP Filters: enable
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable
SAP Filtering Mode: deny

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 255, port 255, id 22500, count 1, size 41)

Enable XNS router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable

------------------------------------------------------------------------------
Object: Protocol Bridging Parameters
     (slot 255, port 255, id 20100, count 1, size 39)
```

```
Enable Source Route Bridging: yes
Bridge number: 1
Designated ring number (hex): 0x600

------------------------------------------------------------------------------
Object: Bridging Spanning Tree Parameters
     (slot 255, port 255, id 20101, count 1, size 5)

Bridge priority (hex): 0x8000
Hello time (seconds): 2
Forward delay time (seconds): 15
Max Age (seconds): 20

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 255, port 255, id 20300, count 1, size 57)

Enable DECnet router: no
Local address: 0.0
Node type: Routing_IV
Area maximum cost (1 - 1022): 1022
Area maximum hops: 30
Maximum address (1 - 1023): 1023
Maximum area (1 - 63): 63
Maximum cost (1 - 1022): 1022
Maximum hops: 30
Maximum paths: 1
Maximum visits: 63
Path split mode: Normal
Maximum broadcast non-routers (1 - 1022): 1022
Maximum broadcast routers (1 - 1022): 32
Buffer Size (246 - 1486 bytes): 1486

------------------------------------------------------------------------------
Object: Data Link Switch (DLS) Parameters
     (slot 255, port 255, id 20400, count 1, size 45)

Enable SNA frame forwarding: no
Enable NetBIOS frame forwarding: no
Virtual Ring Segment Number: 0x0
Accept connections only from specific 6611 routers: no
Destination cache timeout (minutes): 8
Default DLS IP address. this 6611.: 0.0.0.0

------------------------------------------------------------------------------
Object: SNA Frame Filter Parameters
     (slot 255, port 255, id 22100, count 1, size 37)

Source Frame Filter Type: permit
Destination Frame Filter Type: permit
Status Of All Defined SNA Source Frame Filters: enable
Status Of All Defined SNA Destination Frame Filters: enable

------------------------------------------------------------------------------
Object: NetBIOS Filter Parameters
     (slot 255, port 255, id 21300, count 1, size 37)

NetBIOS Destination Name Filter Type: permit
NetBIOS Source Name Filter Type: permit
```

```
Status Of All Defined NetBIOS Destination Name Filters: enable
Status Of All Defined NetBIOS  Source Name Filters: enable

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 1, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 1536000

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 1, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 1, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 1, id 2804, count 1, size 15)

Enable PPP on this port: yes
Maximum receive unit: 1500
Enable link quality monitoring: yes
Link quality monitoring interval: 10000

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x700
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
```

```
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Both SRB and ARB
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: List of SNAP Output Filters for SRB
     (slot 1, port 1, id 108, count 3, size 15)

SNAP Value (hex): 0x800
SNAP value mask (hex): 0xffff

SNAP Value (hex): 0x806
SNAP value mask (hex): 0xffff

SNAP Value (hex): 0x8035
SNAP value mask (hex): 0xffff

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 180
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 1, id 1000, count 1, size 52)
```

```
IP Address: 9.67.38.140
Subnet mask: 255.255.255.192
Destination IP Address: 9.67.38.141
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 1, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 2, id 2800, count 1, size 28)
```

```
Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 19200

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 2, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 2, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 2, id 2804, count 1, size 15)

Enable PPP on this port: no
Maximum receive unit: 1500
Enable link quality monitoring: no
Link quality monitoring interval: 10000

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 2, id 100, count 1, size 45)

Enable Source Route Bridging on this port: no
Ring number (hex): 0x0
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 2052
Hop Count Filter Type: Single route broadcast (SRB)
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
```

```
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: enable
Status of Inbound Ring Number Filters: enable
Status of Inbound MAC Address Filters: enable
Status of Inbound SNAP Filters: enable
Status of Outbound Ring Number Filters: enable
Status of Outbound MAC Address Filters: enable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 2, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 600
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 2, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 2, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

```
--------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 2, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

--------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 2, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

--------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 2, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

--------------------------------------------------------------------------------
Object: Token-Ring Adapter Parameters
     (slot 2, port 1, id 2900, count 1, size 21)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Token Ring MAC Address: 00-00-00-00-00-00
Token Ring Data Rate: 4 Mbps
MAC Address Format: Non_canonical
Local / Non-local broadcast: Non_local

--------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 2, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x600
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
```

```
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: disable
Status of Outbound Source SAP Filters: disable

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 2, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 2, port 1, id 1000, count 1, size 52)

IP Address: 9.67.46.129
Subnet mask: 255.255.255.192
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 2, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 2, port 1, id 1300, count 1, size 11)
```

```
Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 2, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 2, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 2, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 1, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 2, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
```

```
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 2, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 3, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 3, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 4, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 4, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Ethernet Adapter Parameters
     (slot 4, port 1, id 2600, count 1, size 19)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Ethernet MAC Address (Canonical format): 00-00-00-00-00-00
Allow Multicasting: no

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 4, port 1, id 300, count 1, size 24)
```

```
Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 4, port 1, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 4, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 4, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

B.2.2 routerb

```
Ascii dump of Configuration Data for
Router 'routerb' at Thu Jun 18 20:28:50 1992
Configuration: UNNAMED CONFIG

------------------------------------------------------------------------------
Object: Protocol Independent Parameters
     (slot 255, port 255, id 21500, count 1, size 100)

IBM 6611 Host Name: routerb
IBM 6611 Domain name: itsc.raleigh.ibm.com
Enable name resolution by remote name servers: no
Enable time service by remote time servers: no

------------------------------------------------------------------------------
Object: List of Static Host to Internet Address Mappings
     (slot 255, port 255, id 21600, count 6, size 228)

IP Address of host: 9.67.38.65
Host name: vmesa

IP Address of host: 9.67.38.72
Host name: rs60002

IP Address of host: 9.67.38.73
Host name: rs60003

IP Address of host: 9.67.38.75
Host name: doscfg

IP Address of host: 9.67.46.129
Host name: routera

IP Address of host: 9.67.46.130
Host name: os2wkstn

------------------------------------------------------------------------------
Object: Configuration Daemon Parameters
     (slot 255, port 255, id 20200, count 1, size 13)

Type of host access to this IBM 6611 for remote configuration
functions from the Configuration Program.: All hosts
Time period for application of configuration.: Immediately
Year: 0
Month: 0
Day: 0
Hour: 0
Minute: 0

------------------------------------------------------------------------------
Object: Software Lock Parameters
     (slot 255, port 255, id 21200, count 1, size 1)

Lock Value: Unlock

------------------------------------------------------------------------------
Object: Serial Line TTY Parameters
     (slot 255, port 255, id 22300, count 1, size 2)
```

```
baud rate (bps) for the S1 serial port: 9600
baud rate (bps) for the S2 serial port: 2400

------------------------------------------------------------------------------
Object: List of Controlling User Names and Passwords
     (slot 255, port 255, id 22400, count 2, size 40)

User id: kellyjp
Password: *

User id: vannetel
Password: *

------------------------------------------------------------------------------
Object: List of Viewing User Names and Passwords
     (slot 255, port 255, id 22401, count 2, size 40)

User id: collinsr
Password: *

User id: shogren
Password: *

------------------------------------------------------------------------------
Object: SNMP System Contact
     (slot 255, port 255, id 22200, count 1, size 257)

System contact: James Kelly or Ivan Van Netelbosch, Room CC-103

------------------------------------------------------------------------------
Object: SNMP System Name
     (slot 255, port 255, id 22201, count 1, size 257)

System name: routerb.itsc.raleigh.ibm.com

------------------------------------------------------------------------------
Object: SNMP System Location
     (slot 255, port 255, id 22202, count 1, size 257)

System location: ITSC LAB, Building 657, Raleigh NC USA

------------------------------------------------------------------------------
Object: SNMP Parameters
     (slot 255, port 255, id 22203, count 1, size 16)

Enterprise specific trap throttle time (0 - 3600 seconds): 900
Router Serial Number - Prefix: 26
Router Serial Number - Suffix: 06620
Enable SNMP: yes

------------------------------------------------------------------------------
Object: List of SNMP Communities
     (slot 255, port 255, id 22205, count 1, size 265)

Community IP address or Domain name: 9.67.0.0
Community address mask: 255.255.0.0
Community access: read only
Community name: ITSC
Community view name:
```

```
------------------------------------------------------------------------
Object: List of SNMP Clients for Traps
     (slot 255, port 255, id 22204, count 2, size 276)

Trap IP address or Domain name: rs60002
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

Trap IP address or Domain name: rs60003
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

------------------------------------------------------------------------
Object: List of IP Static Routes
     (slot 255, port 255, id 21002, count 1, size 17)

Destination IP Host or Network Address: 9.67.46.128
Destination mask: 255.255.255.192
Next hop router: 9.67.38.140
Preference (0 - 255): 50
Retain: yes

------------------------------------------------------------------------
Object: IP Parameters
     (slot 255, port 255, id 21000, count 1, size 35)

Connection Decay Interval: 10
Status Of All Defined IP Filters: disable

------------------------------------------------------------------------
Object:
     (slot 255, port 255, id 20700, count 1, size 6)

------------------------------------------------------------------------
Object: RIP Parameters
     (slot 255, port 255, id 21800, count 1, size 4)

Enable Routing Information Protocol (RIP): no
Broadcast: yes
Zero Reserved Fields: yes
Route preference (0 - 255): 100

------------------------------------------------------------------------
Object: HELLO Parameters
     (slot 255, port 255, id 20800, count 1, size 3)
```

```
Enable Hello Protocol: no
Broadcast: yes
Route preference (0 - 255): 90

------------------------------------------------------------------------------
Object: Parameters for EGP
     (slot 255, port 255, id 20500, count 1, size 12)

Enable Exterior Gateway Protocol (EGP): no
Preference (0 - 255): 200
Initial maximum packet size (1024 - 65535 bytes): 8192
Local Autonomous System Number: 0
Generate default route.: no
Enable EGP Import Filters: no
Default metric (0 - 255): 1

------------------------------------------------------------------------------
Object: OSPF Parameters
     (slot 255, port 255, id 21405, count 1, size 6)

Enable OSPF: no
Router ID: 0.0.0.0

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 255, port 255, id 21100, count 1, size 43)

Enable IPX router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined SAP Filters: enable
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable
SAP Filtering Mode: deny

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 255, port 255, id 22500, count 1, size 41)

Enable XNS router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable

------------------------------------------------------------------------------
Object: Protocol Bridging Parameters
     (slot 255, port 255, id 20100, count 1, size 39)

Enable Source Route Bridging: yes
Bridge number: 1
Designated ring number (hex): 0x13
```

```
------------------------------------------------------------------------------
Object: Bridging Spanning Tree Parameters
     (slot 255, port 255, id 20101, count 1, size 5)

Bridge priority (hex): 0x8000
Hello time (seconds): 2
Forward delay time (seconds): 15
Max Age (seconds): 20

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 255, port 255, id 20300, count 1, size 57)

Enable DECnet router: no
Local address: 0.0
Node type: Routing_IV
Area maximum cost (1 - 1022): 1022
Area maximum hops: 30
Maximum address (1 - 1023): 1023
Maximum area (1 - 63): 63
Maximum cost (1 - 1022): 1022
Maximum hops: 30
Maximum paths: 1
Maximum visits: 63
Path split mode: Normal
Maximum broadcast non-routers (1 - 1022): 1022
Maximum broadcast routers (1 - 1022): 32
Buffer Size (246 - 1486 bytes): 1486

------------------------------------------------------------------------------
Object: Data Link Switch (DLS) Parameters
     (slot 255, port 255, id 20400, count 1, size 45)

Enable SNA frame forwarding: no
Enable NetBIOS frame forwarding: no
Virtual Ring Segment Number: 0x0
Accept connections only from specific 6611 routers: no
Destination cache timeout (minutes): 8
Default DLS IP address. this 6611.: 0.0.0.0

------------------------------------------------------------------------------
Object: SNA Frame Filter Parameters
     (slot 255, port 255, id 22100, count 1, size 37)

Source Frame Filter Type: permit
Destination Frame Filter Type: permit
Status Of All Defined SNA Source Frame Filters: enable
Status Of All Defined SNA Destination Frame Filters: enable

------------------------------------------------------------------------------
Object: NetBIOS Filter Parameters
     (slot 255, port 255, id 21300, count 1, size 37)

NetBIOS Destination Name Filter Type: permit
NetBIOS Source Name Filter Type: permit
Status Of All Defined NetBIOS Destination Name Filters: enable
Status Of All Defined NetBIOS  Source Name Filters: enable
```

```
------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 1, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 1536000

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 1, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 1, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 1, id 2804, count 1, size 15)

Enable PPP on this port: yes
Maximum receive unit: 1500
Enable link quality monitoring: yes
Link quality monitoring interval: 10000

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x700
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
```

```
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Both SRB and ARB
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: List of SNAP Output Filters for SRB
     (slot 1, port 1, id 108, count 3, size 15)

SNAP Value (hex): 0x800
SNAP value mask (hex): 0xffff

SNAP Value (hex): 0x806
SNAP value mask (hex): 0xffff

SNAP Value (hex): 0x8035
SNAP value mask (hex): 0xffff

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 180
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 1, id 1000, count 1, size 52)

IP Address: 9.67.38.141
Subnet mask: 255.255.255.192
Destination IP Address: 9.67.38.140
Maximum Transmission Unit: 1500
```

```
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 1, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 2, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
```

```
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 56000

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 2, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: yes
Largest frame size (bytes): 1500
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0: 00000000
Link password 1: 00000000
Link password 2: 00000000
Link password 3: 00000000

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 2, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 2, id 2804, count 1, size 15)

Enable PPP on this port: no
Maximum receive unit: 1500
Enable link quality monitoring: no
Link quality monitoring interval: 10000

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 2, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x800
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
```

```
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: disable
Status of Outbound Source SAP Filters: disable

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 2, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 180
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 2, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 2, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 2, id 2100, count 1, size 1)
```

```
Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------
Object: List of SAP Values
     (slot 1, port 2, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 2, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 2, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------
Object: Token-Ring Adapter Parameters
     (slot 2, port 1, id 2900, count 1, size 21)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Token Ring MAC Address: 00-00-00-00-00-00
Token Ring Data Rate: 4 Mbps
MAC Address Format: Non_canonical
Local / Non-local broadcast: Non_local

------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 2, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x13
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
```

```
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: disable
Status of Outbound Source SAP Filters: disable

------------------------------------------------------------------------------
Object: List of SAP Output Filters for SRB
     (slot 2, port 1, id 107, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 2, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 2, port 1, id 1000, count 1, size 52)

IP Address: 9.67.38.78
Subnet mask: 255.255.255.192
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 2, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
```

```
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 2, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 2, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 2, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 2, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

B.3 Data Link Switching Example Scenario

Detailed configuration reports for the two 6611 Network Processors used in this scenario are provided in the following sections.

B.3.1 routera

```
Ascii dump of Configuration Data for
Router 'routera' at Thu Jun 18 20:41:25 1992
Configuration: UNNAMED CONFIG

------------------------------------------------------------------------------
Object: Protocol Independent Parameters
     (slot 255, port 255, id 21500, count 1, size 100)

IBM 6611 Host Name: routera
IBM 6611 Domain name: itsc.raleigh.ibm.com
```

```
Enable name resolution by remote name servers: no
Enable time service by remote time servers: no

------------------------------------------------------------------------
Object: List of Static Host to Internet Address Mappings
     (slot 255, port 255, id 21600, count 6, size 228)

IP Address of host: 9.67.38.65
Host name: vmesa

IP Address of host: 9.67.38.72
Host name: rs60002

IP Address of host: 9.67.38.73
Host name: rs60003

IP Address of host: 9.67.38.75
Host name: doscfg

IP Address of host: 9.67.38.78
Host name: routerb

IP Address of host: 9.67.46.130
Host name: os2wkstn

------------------------------------------------------------------------
Object: Configuration Daemon Parameters
     (slot 255, port 255, id 20200, count 1, size 13)

Type of host access to this IBM 6611 for remote configuration
functions from the Configuration Program.: All hosts
Time period for application of configuration.: Immediately
Year: 0
Month: 0
Day: 0
Hour: 0
Minute: 0

------------------------------------------------------------------------
Object: Software Lock Parameters
     (slot 255, port 255, id 21200, count 1, size 1)

Lock Value: Unlock

------------------------------------------------------------------------
Object: Serial Line TTY Parameters
     (slot 255, port 255, id 22300, count 1, size 2)

baud rate (bps) for the S1 serial port: 9600
baud rate (bps) for the S2 serial port: 2400

------------------------------------------------------------------------
Object: List of Controlling User Names and Passwords
     (slot 255, port 255, id 22400, count 2, size 40)

User id: kellyjp
Password: *
```

```
User id: vannetel
Password: *

------------------------------------------------------------------------------
Object: List of Viewing User Names and Passwords
     (slot 255, port 255, id 22401, count 2, size 40)

User id: collinsr
Password: *

User id: shogren
Password: *

------------------------------------------------------------------------------
Object: SNMP System Contact
     (slot 255, port 255, id 22200, count 1, size 257)

System contact: Jaems Kelly or Ivan Van Netelbosch, Room CC-103

------------------------------------------------------------------------------
Object: SNMP System Name
     (slot 255, port 255, id 22201, count 1, size 257)

System name: routera.itsc.raleigh.ibm.com

------------------------------------------------------------------------------
Object: SNMP System Location
     (slot 255, port 255, id 22202, count 1, size 257)

System location: ITSC LAB, Building 657, Raleigh NC USA

------------------------------------------------------------------------------
Object: SNMP Parameters
     (slot 255, port 255, id 22203, count 1, size 16)

Enterprise specific trap throttle time (0 - 3600 seconds): 900
Router Serial Number - Prefix: 26
Router Serial Number - Suffix: 24686
Enable SNMP: yes

------------------------------------------------------------------------------
Object: List of SNMP Communities
     (slot 255, port 255, id 22205, count 1, size 265)

Community IP address or Domain name: 9.67.0.0
Community address mask: 255.255.0.0
Community access: read only
Community name: ITSC
Community view name:

------------------------------------------------------------------------------
Object: List of SNMP Clients for Traps
     (slot 255, port 255, id 22204, count 2, size 276)

Trap IP address or Domain name: rs60002
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
```

```
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

Trap IP address or Domain name: rs60003
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

------------------------------------------------------------------------------
Object: List of IP Static Routes
     (slot 255, port 255, id 21002, count 1, size 17)

Destination IP Host or Network Address: 9.67.38.64
Destination mask: 255.255.255.192
Next hop router: 9.67.38.141
Preference (0 - 255): 50
Retain: yes

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 255, port 255, id 21000, count 1, size 35)

Connection Decay Interval: 10
Status Of All Defined IP Filters: disable

------------------------------------------------------------------------------
Object:
     (slot 255, port 255, id 20700, count 1, size 6)

------------------------------------------------------------------------------
Object: RIP Parameters
     (slot 255, port 255, id 21800, count 1, size 4)

Enable Routing Information Protocol (RIP): no
Broadcast: yes
Zero Reserved Fields: yes
Route preference (0 - 255): 100

------------------------------------------------------------------------------
Object: HELLO Parameters
     (slot 255, port 255, id 20800, count 1, size 3)

Enable Hello Protocol: no
Broadcast: yes
Route preference (0 - 255): 90

------------------------------------------------------------------------------
Object: Parameters for EGP
     (slot 255, port 255, id 20500, count 1, size 12)

Enable Exterior Gateway Protocol (EGP): no
Preference (0 - 255): 200
```

```
Initial maximum packet size (1024 - 65535 bytes): 8192
Local Autonomous System Number: 0
Generate default route.: no
Enable EGP Import Filters: no
Default metric (0 - 255): 1

------------------------------------------------------------------------------
Object: OSPF Parameters
     (slot 255, port 255, id 21405, count 1, size 6)

Enable OSPF: no
Router ID: 0.0.0.0

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 255, port 255, id 21100, count 1, size 43)

Enable IPX router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined SAP Filters: enable
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable
SAP Filtering Mode: deny

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 255, port 255, id 22500, count 1, size 41)

Enable XNS router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable

------------------------------------------------------------------------------
Object: Protocol Bridging Parameters
     (slot 255, port 255, id 20100, count 1, size 39)

Enable Source Route Bridging: yes
Bridge number: 1
Designated ring number (hex): 0x600

------------------------------------------------------------------------------
Object: Bridging Spanning Tree Parameters
     (slot 255, port 255, id 20101, count 1, size 5)

Bridge priority (hex): 0x8000
Hello time (seconds): 2
Forward delay time (seconds): 15
Max Age (seconds): 20
```

```
------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 255, port 255, id 20300, count 1, size 57)

Enable DECnet router: no
Local address: 0.0
Node type: Routing_IV
Area maximum cost (1 - 1022): 1022
Area maximum hops: 30
Maximum address (1 - 1023): 1023
Maximum area (1 - 63): 63
Maximum cost (1 - 1022): 1022
Maximum hops: 30
Maximum paths: 1
Maximum visits: 63
Path split mode: Normal
Maximum broadcast non-routers (1 - 1022): 1022
Maximum broadcast routers (1 - 1022): 32
Buffer Size (246 - 1486 bytes): 1486

------------------------------------------------------------------------------
Object: Data Link Switch (DLS) Parameters
     (slot 255, port 255, id 20400, count 1, size 45)

Enable SNA frame forwarding: yes
Enable NetBIOS frame forwarding: yes
Virtual Ring Segment Number: 0x999
Accept connections only from specific 6611 routers: yes
Destination cache timeout (minutes): 8
Default DLS IP address. this 6611.: 9.67.46.129

------------------------------------------------------------------------------
Object: List of Participating DLS Routers
     (slot 255, port 255, id 20401, count 1, size 5)

IP Address Of Remote Router: 9.67.38.78

------------------------------------------------------------------------------
Object: SNA Frame Filter Parameters
     (slot 255, port 255, id 22100, count 1, size 37)

Source Frame Filter Type: permit
Destination Frame Filter Type: permit
Status Of All Defined SNA Source Frame Filters: disable
Status Of All Defined SNA Destination Frame Filters: disable

------------------------------------------------------------------------------
Object: NetBIOS Filter Parameters
     (slot 255, port 255, id 21300, count 1, size 37)

NetBIOS Destination Name Filter Type: permit
NetBIOS Source Name Filter Type: permit
Status Of All Defined NetBIOS Destination Name Filters: disable
Status Of All Defined NetBIOS  Source Name Filters: disable

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 1, id 2800, count 1, size 28)
```

```
Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 1536000

------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 1, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 1, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 1, id 2804, count 1, size 15)

Enable PPP on this port: yes
Maximum receive unit: 1500
Enable link quality monitoring: yes
Link quality monitoring interval: 10000

------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x700
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
```

```
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Both SRB and ARB
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: List of SAP Output Filters for SRB
     (slot 1, port 1, id 107, count 2, size 4)

Source SAP Value (hex): 0x4

Source SAP Value (hex): 0xf0

------------------------------------------------------------------------------
Object: List of SNAP Output Filters for SRB
     (slot 1, port 1, id 108, count 3, size 15)

SNAP Value (hex): 0x800
SNAP value mask (hex): 0xffff

SNAP Value (hex): 0x806
SNAP value mask (hex): 0xffff

SNAP Value (hex): 0x8035
SNAP value mask (hex): 0xffff

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 180
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 1, id 1000, count 1, size 52)
```

```
IP Address: 9.67.38.140
Subnet mask: 255.255.255.192
Destination IP Address: 9.67.38.141
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 1, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 2, id 2800, count 1, size 28)
```

```
Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 19200

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 2, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 2, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes

------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 2, id 2804, count 1, size 15)

Enable PPP on this port: no
Maximum receive unit: 1500
Enable link quality monitoring: no
Link quality monitoring interval: 10000

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 2, id 100, count 1, size 45)

Enable Source Route Bridging on this port: no
Ring number (hex): 0x0
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 2052
Hop Count Filter Type: Single route broadcast (SRB)
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
```

```
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: enable
Status of Inbound Ring Number Filters: enable
Status of Inbound MAC Address Filters: enable
Status of Inbound SNAP Filters: enable
Status of Outbound Ring Number Filters: enable
Status of Outbound MAC Address Filters: enable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 2, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 600
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 2, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 2, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

```
------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 2, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 2, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 2, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: Token-Ring Adapter Parameters
     (slot 2, port 1, id 2900, count 1, size 21)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Token Ring MAC Address: 00-00-00-00-00-00
Token Ring Data Rate: 4 Mbps
MAC Address Format: Non_canonical
Local / Non-local broadcast: Non_local

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 2, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x600
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
```

```
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: disable
Status of Outbound Source SAP Filters: disable

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 2, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 2, port 1, id 1000, count 1, size 52)

IP Address: 9.67.46.129
Subnet mask: 255.255.255.192
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 2, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 2, port 1, id 1300, count 1, size 11)
```

```
Forward NetBIOS frames on this port: yes
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 2, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: yes

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 2, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 2, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 1, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Data terminal ready (DTR)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: List of SNA Stations for Adapter
     (slot 3, port 1, id 2701, count 1, size 45)

Station Address: 0xc1
Station Token Ring Source Address: 40-00-30-02-00-22
Station Token Ring Destination Address: 40-00-01-24-00-00
Transmit window count: 7
Retransmit count (1 - 50 frames): 10
Retransmit Threshold (1 - 100 frames): 10
Force disconnect timeout (1 - 600 seconds): 120
Maximum I-field size (265 - 30729 bytes): 265
Primary repoll timeout (1 - 250 tenths of seconds): 30
Primary Repoll Count (3 - 50): 15
Primary Repoll Threshold (1 - 100%): 10
```

```
Primary slow list timeout (1 - 60 seconds): 1
Station Token Ring Source SAP: 0x4
Station Token Ring Destination SAP: 0x4
Station XID value: 0x5d20022

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 2, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 2, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 3, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 3, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: Multi-Protocol Adapter Parameters
     (slot 3, port 4, id 2700, count 1, size 18)

Enable interface: yes
Serial encoding: NRZ
Request to send: continuous
Data terminal ready (DTR): Connect data set to line (CDSTL)
Bit clocking: external
Data rate select: full
Transmit rate (600 - 38400 bps): 1200
```

```
--------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 3, port 4, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

--------------------------------------------------------------------------------
Object: Ethernet Adapter Parameters
     (slot 4, port 1, id 2600, count 1, size 19)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Ethernet MAC Address (Canonical format): 00-00-00-00-00-00
Allow Multicasting: no

--------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 4, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

--------------------------------------------------------------------------------
Object: IP Parameters
     (slot 4, port 1, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

--------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 4, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

--------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 4, port 1, id 2500, count 1, size 32)
```

```
Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

B.3.2 routerb

```
Ascii dump of Configuration Data for
Router 'routerb' at Thu Jun 18 20:45:37 1992
Configuration: UNNAMED CONFIG

------------------------------------------------------------------------------
Object: Protocol Independent Parameters
     (slot 255, port 255, id 21500, count 1, size 100)

IBM 6611 Host Name: routerb
IBM 6611 Domain name: itsc.raleigh.ibm.com
Enable name resolution by remote name servers: no
Enable time service by remote time servers: no

------------------------------------------------------------------------------
Object: List of Static Host to Internet Address Mappings
     (slot 255, port 255, id 21600, count 6, size 228)

IP Address of host: 9.67.38.65
Host name: vmesa

IP Address of host: 9.67.38.72
Host name: rs60002

IP Address of host: 9.67.38.73
Host name: rs60003

IP Address of host: 9.67.38.75
Host name: doscfg

IP Address of host: 9.67.46.129
Host name: routera

IP Address of host: 9.67.46.130
Host name: os2wkstn

------------------------------------------------------------------------------
Object: Configuration Daemon Parameters
     (slot 255, port 255, id 20200, count 1, size 13)

Type of host access to this IBM 6611 for remote configuration
functions from the Configuration Program.: All hosts
Time period for application of configuration.: Immediately
Year: 0
Month: 0
Day: 0
```

```
Hour: 0
Minute: 0

------------------------------------------------------------------------
Object: Software Lock Parameters
     (slot 255, port 255, id 21200, count 1, size 1)

Lock Value: Unlock

------------------------------------------------------------------------
Object: Serial Line TTY Parameters
     (slot 255, port 255, id 22300, count 1, size 2)

baud rate (bps) for the S1 serial port: 9600
baud rate (bps) for the S2 serial port: 2400

------------------------------------------------------------------------
Object: List of Controlling User Names and Passwords
     (slot 255, port 255, id 22400, count 2, size 40)

User id: kellyjp
Password: *

User id: vannetel
Password: *

------------------------------------------------------------------------
Object: List of Viewing User Names and Passwords
     (slot 255, port 255, id 22401, count 2, size 40)

User id: collinsr
Password: *

User id: shogren
Password: *

------------------------------------------------------------------------
Object: SNMP System Contact
     (slot 255, port 255, id 22200, count 1, size 257)

System contact: James Kelly or Ivan Van Netelbosch, Room CC-103

------------------------------------------------------------------------
Object: SNMP System Name
     (slot 255, port 255, id 22201, count 1, size 257)

System name: routerb.itsc.raleigh.ibm.com

------------------------------------------------------------------------
Object: SNMP System Location
     (slot 255, port 255, id 22202, count 1, size 257)

System location: ITSC LAB, Building 657, Raleigh NC USA

------------------------------------------------------------------------
Object: SNMP Parameters
     (slot 255, port 255, id 22203, count 1, size 16)
```

```
Enterprise specific trap throttle time (0 - 3600 seconds): 900
Router Serial Number - Prefix: 26
Router Serial Number - Suffix: 06620
Enable SNMP: yes

------------------------------------------------------------------------------
Object: List of SNMP Communities
     (slot 255, port 255, id 22205, count 1, size 265)

Community IP address or Domain name: 9.67.0.0
Community address mask: 255.255.0.0
Community access: read only
Community name: ITSC
Community view name:

------------------------------------------------------------------------------
Object: List of SNMP Clients for Traps
     (slot 255, port 255, id 22204, count 2, size 276)

Trap IP address or Domain name: rs60002
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

Trap IP address or Domain name: rs60003
Enable coldStart trap: enable
Enable warmStart trap: enable
Enable linkDown trap: enable
Enable linkUp trap: enable
Enable authenticationFailure trap: enable
Enable egpNeighborLoss trap: enable
Enable enterpriseSpecific trap: enable
Trap community name: ITSC

------------------------------------------------------------------------------
Object: List of IP Static Routes
     (slot 255, port 255, id 21002, count 1, size 17)

Destination IP Host or Network Address: 9.67.46.128
Destination mask: 255.255.255.192
Next hop router: 9.67.38.140
Preference (0 - 255): 50
Retain: yes

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 255, port 255, id 21000, count 1, size 35)

Connection Decay Interval: 10
Status Of All Defined IP Filters: disable

------------------------------------------------------------------------------
Object:
     (slot 255, port 255, id 20700, count 1, size 6)
```

```
------------------------------------------------------------------------------
Object: RIP Parameters
     (slot 255, port 255, id 21800, count 1, size 4)

Enable Routing Information Protocol (RIP): no
Broadcast: yes
Zero Reserved Fields: yes
Route preference (0 - 255): 100

------------------------------------------------------------------------------
Object: HELLO Parameters
     (slot 255, port 255, id 20800, count 1, size 3)

Enable Hello Protocol: no
Broadcast: yes
Route preference (0 - 255): 90

------------------------------------------------------------------------------
Object: Parameters for EGP
     (slot 255, port 255, id 20500, count 1, size 12)

Enable Exterior Gateway Protocol (EGP): no
Preference (0 - 255): 200
Initial maximum packet size (1024 - 65535 bytes): 8192
Local Autonomous System Number: 0
Generate default route.: no
Enable EGP Import Filters: no
Default metric (0 - 255): 1

------------------------------------------------------------------------------
Object: OSPF Parameters
     (slot 255, port 255, id 21405, count 1, size 6)

Enable OSPF: no
Router ID: 0.0.0.0

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 255, port 255, id 21100, count 1, size 43)

Enable IPX router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined SAP Filters: enable
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable
SAP Filtering Mode: deny

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 255, port 255, id 22500, count 1, size 41)

Enable XNS router: no
Split Horizon For RIP Filters: On
Inbound Filtering Mode: deny
```

```
Outbound Filtering Mode: deny
Router Filtering Mode: deny
Status Of All Defined Inbound RIP Filters: enable
Status Of All Defined Outbound RIP Filters: enable
Status Of All Defined RIP Router Filters: enable

------------------------------------------------------------------------
Object: Protocol Bridging Parameters
     (slot 255, port 255, id 20100, count 1, size 39)

Enable Source Route Bridging: yes
Bridge number: 1
Designated ring number (hex): 0x13

------------------------------------------------------------------------
Object: Bridging Spanning Tree Parameters
     (slot 255, port 255, id 20101, count 1, size 5)

Bridge priority (hex): 0x8000
Hello time (seconds): 2
Forward delay time (seconds): 15
Max Age (seconds): 20

------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 255, port 255, id 20300, count 1, size 57)

Enable DECnet router: no
Local address: 0.0
Node type: Routing_IV
Area maximum cost (1 - 1022): 1022
Area maximum hops: 30
Maximum address (1 - 1023): 1023
Maximum area (1 - 63): 63
Maximum cost (1 - 1022): 1022
Maximum hops: 30
Maximum paths: 1
Maximum visits: 63
Path split mode: Normal
Maximum broadcast non-routers (1 - 1022): 1022
Maximum broadcast routers (1 - 1022): 32
Buffer Size (246 - 1486 bytes): 1486

------------------------------------------------------------------------
Object: Data Link Switch (DLS) Parameters
     (slot 255, port 255, id 20400, count 1, size 45)

Enable SNA frame forwarding: yes
Enable NetBIOS frame forwarding: yes
Virtual Ring Segment Number: 0x999
Accept connections only from specific 6611 routers: yes
Destination cache timeout (minutes): 8
Default DLS IP address. this 6611.: 9.67.38.78

------------------------------------------------------------------------
Object: List of Participating DLS Routers
     (slot 255, port 255, id 20401, count 1, size 5)

IP Address Of Remote Router: 9.67.46.129
```

```
--------------------------------------------------------------------------------
Object: SNA Frame Filter Parameters
     (slot 255, port 255, id 22100, count 1, size 37)

Source Frame Filter Type: permit
Destination Frame Filter Type: permit
Status Of All Defined SNA Source Frame Filters: disable
Status Of All Defined SNA Destination Frame Filters: disable

--------------------------------------------------------------------------------
Object: NetBIOS Filter Parameters
     (slot 255, port 255, id 21300, count 1, size 37)

NetBIOS Destination Name Filter Type: permit
NetBIOS Source Name Filter Type: permit
Status Of All Defined NetBIOS Destination Name Filters: disable
Status Of All Defined NetBIOS  Source Name Filters: disable

--------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 1, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 1536000

--------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 1, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: no
Largest frame size (bytes): 2052
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0:
Link password 1:
Link password 2:
Link password 3:

--------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 1, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes
```

```
------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 1, id 2804, count 1, size 15)

Enable PPP on this port: yes
Maximum receive unit: 1500
Enable link quality monitoring: yes
Link quality monitoring interval: 10000

------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x700
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Both SRB and ARB
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: enable
Status of Outbound Source SAP Filters: enable

------------------------------------------------------------------------
Object: List of SAP Output Filters for SRB
     (slot 1, port 1, id 107, count 2, size 4)

Source SAP Value (hex): 0x4

Source SAP Value (hex): 0xf0

------------------------------------------------------------------------
Object: List of SNAP Output Filters for SRB
     (slot 1, port 1, id 108, count 3, size 15)

SNAP Value (hex): 0x800
SNAP value mask (hex): 0xffff
```

```
SNAP Value (hex): 0x806
SNAP value mask (hex): 0xffff

SNAP Value (hex): 0x8035
SNAP value mask (hex): 0xffff

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 180
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 1, id 1000, count 1, size 52)

IP Address: 9.67.38.141
Subnet mask: 255.255.255.192
Destination IP Address: 9.67.38.140
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: no

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 1, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
```

```
     (slot 1, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: no
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: Serial Port Parameters
     (slot 1, port 2, id 2800, count 1, size 28)

Enable interface: yes
Cylink serial number (0 - 99999999): 0
Data Encoding: NRZI
Locally Administered MAC address: 00-00-00-00-00-00
Serial Line Speed (19200 - 1536000 bits per second): 56000

------------------------------------------------------------------------------
Object: IBM Lan Bridge Parameters
     (slot 1, port 2, id 2801, count 1, size 61)

Bridge performance counter threshold: 10
Telecommunications Link error threshold: 0
Auto reboot on error: yes
Memory dump on error: No dumping
Event log drive: No logging
Enable the LAN Bridge Protocol on this port: yes
Largest frame size (bytes): 1500
Enable ring parameter server: yes
Enable ring error monitor: yes
Enable configuration report server: yes
Link password 0: 00000000
Link password 1: 00000000
Link password 2: 00000000
Link password 3: 00000000

------------------------------------------------------------------------------
Object: Frame Relay Parameters
     (slot 1, port 2, id 2802, count 1, size 14)

Enable Frame Relay on this port: no
Polling interval (seconds): 10
Full enquiry interval: 6
LMI option: ANSI T1.617 Annex D
Use Inverse ARP to resolve remote protocol addresses: yes
```

```
--------------------------------------------------------------------------------
Object: Point-to-Point Protocol Parameters
     (slot 1, port 2, id 2804, count 1, size 15)

Enable PPP on this port: no
Maximum receive unit: 1500
Enable link quality monitoring: no
Link quality monitoring interval: 10000

--------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 1, port 2, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x800
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: disable
Status of Outbound Source SAP Filters: disable

--------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 1, port 2, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 180
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable
```

```
------------------------------------------------------------------------------
Object: IP Parameters
     (slot 1, port 2, id 1000, count 1, size 52)

IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: no
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 1, port 2, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 1, port 2, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: yes

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 1, port 2, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 1, port 2, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 1, port 2, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: yes
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes
```

```
------------------------------------------------------------------------------
Object: Token-Ring Adapter Parameters
     (slot 2, port 1, id 2900, count 1, size 21)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Token Ring MAC Address: 00-00-00-00-00-00
Token Ring Data Rate: 4 Mbps
MAC Address Format: Non_canonical
Local / Non-local broadcast: Non_local

------------------------------------------------------------------------------
Object: Source Route Bridging Parameters
     (slot 2, port 1, id 100, count 1, size 45)

Enable Source Route Bridging on this port: yes
Ring number (hex): 0x13
Spanning tree mode: Automatic
Enable forwarding of spanning tree explorer packets: yes
Path cost (0 - 65535): 0
Maximum transmission unit: 1500
Hop Count Filter Type: Both SRB and ARB
Hop Count: 7
Inbound Source SAP Filter Type: deny
Inbound Source SAP Frame Type: Single route broadcast (SRB)
Inbound Ring Number Filter Type: deny
Inbound Ring Number Frame Type: Single route broadcast (SRB)
Inbound MAC Address Filter Type: deny
Inbound MAC Address Frame Type: Single route broadcast (SRB)
Inbound SNAP Filter Type: deny
Outbound Ring Number Filter Type: deny
Outbound Ring Number Frame Type: Single route broadcast (SRB)
Outbound MAC Address Filter Type: deny
Outbound MAC Address Frame Type: Single route broadcast (SRB)
Outbound SNAP Filter Type: deny
Outbound Source SAP Filter Type: deny
Outbound Source SAP Frame Type: Single route broadcast (SRB)
Status of Inbound Source SAP Filters: disable
Status of Inbound Ring Number Filters: disable
Status of Inbound MAC Address Filters: disable
Status of Inbound SNAP Filters: disable
Status of Outbound Ring Number Filters: disable
Status of Outbound MAC Address Filters: disable
Status of Outbound SNAP Filters: disable
Status of Outbound Source SAP Filters: disable

------------------------------------------------------------------------------
Object: List of SAP Output Filters for SRB
     (slot 2, port 1, id 107, count 1, size 2)

Source SAP Value (hex): 0xaa

------------------------------------------------------------------------------
Object: DECnet Parameters
     (slot 2, port 1, id 300, count 1, size 24)

Enable DECnet on this interface: no
Circuit cost (1 - 63): 4
```

```
Hello timer (1 - 8191 seconds): 15
Router priority (0 - 127): 64
Routing timer (seconds): 40
Maximum Routers (1 - 1022): 32
Remote DECnet address: 0.0
Remote DECnet Node Type: Area
Status Of All Defined DECnet Filters On This Port: enable

------------------------------------------------------------------------------
Object: IP Parameters
     (slot 2, port 1, id 1000, count 1, size 52)

IP Address: 9.67.38.78
Subnet mask: 255.255.255.192
Destination IP Address: 0.0.0.0
Maximum Transmission Unit: 1500
Enable IP routing on this port: yes
Ethernet Framing for IP: DIX

------------------------------------------------------------------------------
Object: IPX Parameters
     (slot 2, port 1, id 1100, count 1, size 32)

Network number (hex): 0x0
Enable IPX routing on this port: no
Token-Ring Encapsulation Method: Token_Ring 802.5
Ethernet Encapsulation Method: Ethernet II
Checksum Method: Off
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined IPX Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00

------------------------------------------------------------------------------
Object: NetBIOS Packet Forwarding Parameters
     (slot 2, port 1, id 1300, count 1, size 11)

Forward NetBIOS frames on this port: yes
Forward NetBIOS Datagram and Datagram_Broadcast message on this port.: yes

------------------------------------------------------------------------------
Object: SNA Parameters
     (slot 2, port 1, id 2100, count 1, size 1)

Enable SNA frame forwarding on this port: yes

------------------------------------------------------------------------------
Object: List of SAP Values
     (slot 2, port 1, id 2101, count 1, size 2)

SAP value: 0x4

------------------------------------------------------------------------------
Object: XNS Parameters
     (slot 2, port 1, id 2500, count 1, size 32)

Network number (hex): 0x0
Enable XNS routing on this port: no
Encapsulation Method: Token_Ring 802.5
```

```
Encapsulation Method: Ethernet II
Checksum Method: Packet
Error Protocol Active: yes
Number of bytes returned in an error protocol packet: 42
Software loopback active: yes
Filtering Mode: deny
Status Of All Defined XNS Filters On This Port: enable
Destination Host Address: 00-00-00-00-00-00
```

Appendix C. Abbreviations

ABBREVIATION	MEANING
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation One
AUI	Attachment Unit Interface
BGP	Border Gateway Protocol
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CLNP	Connection-less Network Protocol
CRS	Configuration Report Server
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DCE	Data Communications Equipment
DDP	Datagram Delivery Protocol
DIX	Digital Equipment Corporation, Intel Corporation, Xerox Corporation
DLCI	Data Link Connection Identifier
DLS	Data Link Switching
DSU/CSU	Data Services Unit/Channel Services Unit
DTE	Data Terminal Equipment
EIA	Electronics Industry Association
EGP	Exterior Gateway Protocol
FTP	File Transfer Protocol
IAB	Internet Activities Board
ICAT	Installation and Configuration Automation Tool
ICMP	Internet Control Message Protocol
IDP	Internetwork Datagram Protocol
IEEE	Institution of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPX	Internet Packet Exchange
ISO	International Organization for Standardization
ISDN	Integrated Services Digital Network
LAA	Locally Administered Address
LBS	LAN Bridge Server
LLC	Logical Link Control
LRM	LAN Reporting Mechanism

MAC	Media Access Control
MIB	Management Information Base
MSU	Management Services Unit
NBP	Name Binding Protocol
NetBIOS	Network Basic Input Output System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
POWER	Performance Optimization With Enhanced RISC
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
PU	Physical Unit
PVC	Permanent Virtual Circuit
REM	Ring Error Monitor
RIP	Routing Information Protocol
RISC	Reduced Instruction Set Computer
RPS	Ring Parameter Server
RTMP	Routing Table Maintenance Protocol
SAP	Service Access Point
SDLC	Synchronous Data Link Control
SMIT	System Management Interface Tool
SNA	Systems Network Architecture
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SVC	Switched Virtual Circuit
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
XNS	Xerox Network Systems

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Z

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Center
Department 985, Building 657
P.O. BOX 12195
RESEARCH TRIANGLE PARK NC
USA 27709-2195

Fold and Tape **Please do not staple** Fold and Tape

ITSC Technical Bulletin Evaluation RED000

The IBM 6611 Network Processor

Publication No. GG24-3870-00

Your feedback is very important to us to maintain the quality of ITSO redbooks. **Please fill out this questionnaire and return it via one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction	____		
Organization of the book	____	Grammar/punctuation/spelling	____
Accuracy of the information	____	Ease of reading and understanding	____
Relevance of the information	____	Ease of finding information	____
Completeness of the information	____	Level of technical detail	____
Value of illustrations	____	Print Quality	____

Please answer the following questions:

a) Are you an employee of IBM or its subsidiaries? Yes____ No____

b) Are you working in the USA? Yes____ No____

c) Was the bulletin published in time for your needs? Yes____ No____

d) Did this bulletin meet your needs? Yes____ No____

If no, please explain:

_____

_____

What other Topics would you like to see in this Bulletin?

_____

_____

What other Technical Bulletins would you like to see published?

_____

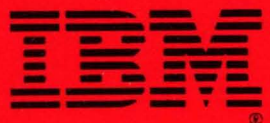
Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

_____ _____
Name Address

_____ _____
Company or Organization

_____ _____
Phone No.

GG24-3870-00



The IBM 6611 Network Processor

GG24-3870-00

PRINTED IN THE U.S.A.