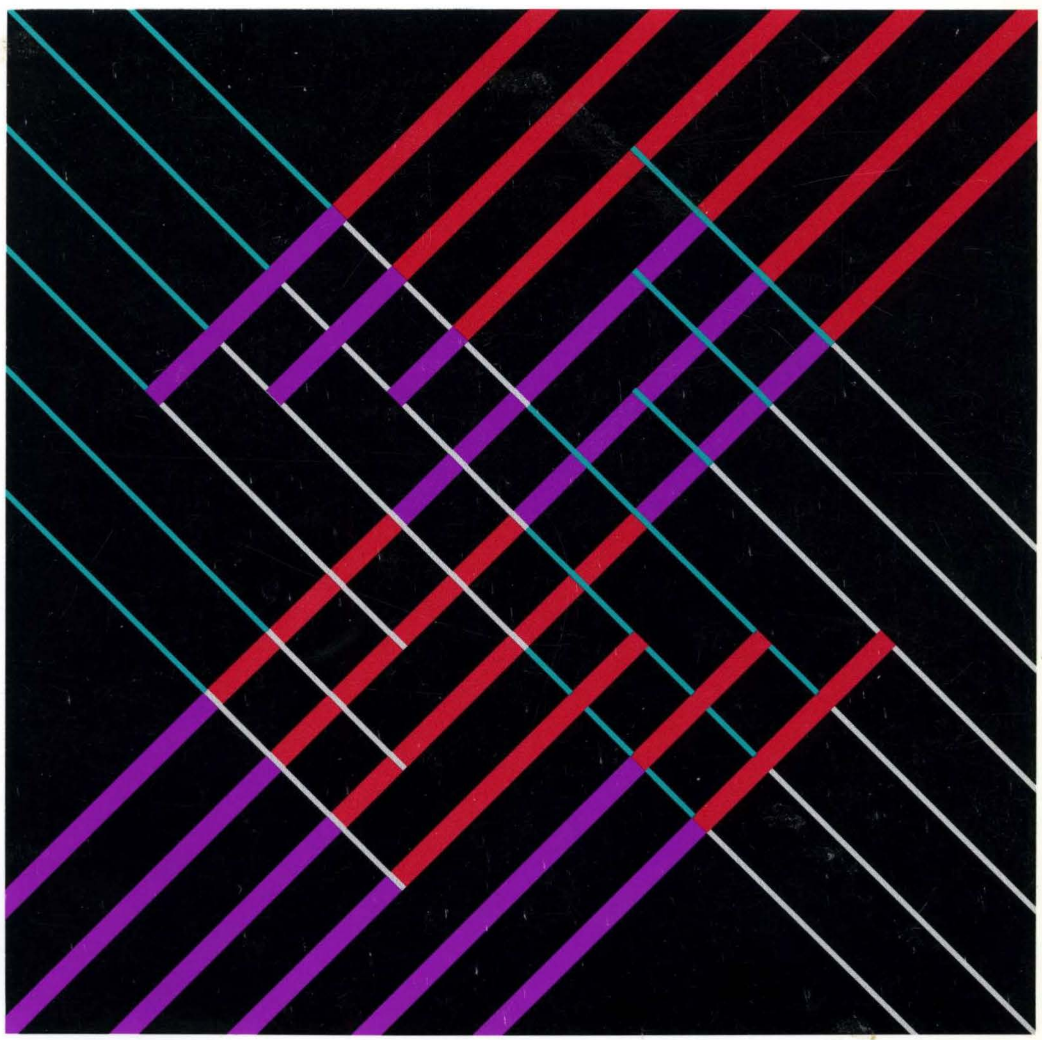
Multiprotocol Network Program

SC31-6691-01

Configuration Guide

Version 1 Release 3



IBM

Multiprotocol Network Program

SC31-6691-01

Configuration Guide

Version 1 Release 3

Note

Before using this document, read the general information under "Notices" on page xxxiii.

Second Edition, September 1994

This is a major revision of, and obsoletes, SC30-6691-00.

This edition applies to:

Version 1, Release 3 of the IBM Multiprotocol Network Program
Models 120, 125, 140, 145, 170 and 175 of the IBM 6611 Network Processor

and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters. See the Summary of Changes for the changes made to this manual. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change. Make sure you are using the correct edition for the level of the product.

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

IBM welcomes your comments. A form for readers' comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation
Department E15
P.O. Box 12195
Research Triangle Park, North Carolina 27709-9990
U.S.A.

Contents

Appendixes

Abbreviations, Glossary, Bibliography, and Index

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them 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 that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of the intellectual property rights of IBM may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter described 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:

IBM Director of Licensing
IBM Corporation
208 Harbor Drive, Building 1
Stamford, CT United States 06904

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Trademarks

The following terms, denoted by an asterisk (*) at their first occurrence in this publication, are trademarks of the IBM corporation in this country or other countries or both:

Advanced Peer-to-Peer Networking	Operating System/2
AIX	OS/2
AIXwindows	Personal System/2
APPN	PS/2
BookManager	RISC System/6000
IBM	VTAM
NetView	

The following terms, denoted by two asterisks (**) at their first occurrence in this publication, are trademarks of other companies:

Apple	Apple Computer, Inc.
AppleTalk	Apple Computer, Inc.
Banyan	Banyan Systems, Inc.
Cylink	Cylink Corporation
DECnet	Digital Equipment Corporation
Digital	Digital Equipment Corporation
Intel	Intel Corporation

Internetwork Packet Exchange (IPX)	Novell Corporation
Microsoft	Microsoft Corp.
Microsoft Windows	Microsoft Corp.
MS-DOS	Microsoft Corp.
NetWare	Novell, Inc.
Novell	Novell, Inc.
OSF/Motif	Open Software Foundation, Inc.
Tymnet	Tymshare, Inc.
UNIX	Novell, Inc.
VIrtual NEtworking Systems (VINES)	Banyan Systems, Inc.
Windows	Microsoft Corp.
Xerox	Xerox Corp.
Xerox Network Systems (XNS)	Xerox Corp.
80386	Intel Corporation

About This Book

This book describes how to configure IBM* Multiprotocol Network Program Version 1 Release 3. The Multiprotocol Network Program (*5648-016*) is the operating system that provides the bridging and routing functions for the IBM 6611 Network Processor (*6611*). The Multiprotocol Network Program (MPNP) is preloaded on the disk of the 6611. There are three components of the Multiprotocol Network Program:

- The base operating system performs routing and bridging and supports the Simple Network Management Protocol (SNMP) network manager agent.
- The IBM Multiprotocol Network Program Configuration Program (*Configuration Program*) allows you to customize the 6611 functions and communication with the network. The Configuration Program diskettes are shipped separately from the 6611 as part of the software order. You should store the diskettes in the diskette holders and store them along with this book inside the binder.
- The IBM Multiprotocol Network Program System Manager (*System Manager*) is a user interface that performs operation and node management tasks.

This book consists of the following chapters:

- **Chapter 1** provides information about getting started, planning, and troubleshooting your 6611 configuration.
- **Chapter 2** describes how to install the MPNP Configuration Program and how to migrate from Version 1 Release 1.0, Version 1 Release 1.1/Version 1 Release 1.2, or Version 1 Release 2 to Version 1 Release 3.
- **Chapter 3** explains how to operate the Configuration Program and how to transport the configuration file.
- **Chapter 4** provides details about each port type and framing method that the 6611 supports.
- **Chapter 5** provides details about each protocol that the 6611 supports for routing, bridging, and data link switching.
- **Chapter 6** provides details about node management functions you can configure on the 6611.
- **Chapter 7** discusses how to use System Manager to transport configuration files and change configuration parameters.

This book also includes a list of abbreviations, a glossary, a bibliography, and an index.

Summary of Changes

This is the second edition of the *IBM Multiprotocol Network Program Configuration Guide*. The following information is new to Version 1 Release 3 of the Multiprotocol Network Program and the Configuration Program:

- Network management support for Advanced Peer-to-Peer Networking* (APPN*)
- Translational bridging support
- Support for the LAN Network Manager (LNM) agent

- LAN Bridging Protocol enhancements
- Internetwork Protocol Exchange ** (IPX**) routing over the X.25 Adapter
- Support of IPX and Internet Protocol (IP) over non-fully meshed frame-relay networks
- Open Shortest Path First (OSPF) area filters
- ASCII conversion option on the Configuration Program
- Configuration Program support for Operating System/2* (OS/2)*
- Send multiple configuration function on the Configuration Program
- Support for Systems Network Architecture (SNA) and NetBIOS prioritization for data link switching (DLSw)
- SDLC adapter support for physical unit Type 2.1

The *IBM Multiprotocol Network Program Configuration Guide* is structured to include the following enhancements:

- Configuration verification checklists that help you verify that two or more 6611s are correctly configured to route or bridge a particular protocol between them.
- Additional multiprotocol configuration examples.

Who Should Use This Book

This book is intended for the customer who is configuring the 6611. The users include the network planner, system programmer, and network administrator.

6611 Network Processor and Multiprotocol Network Program Information

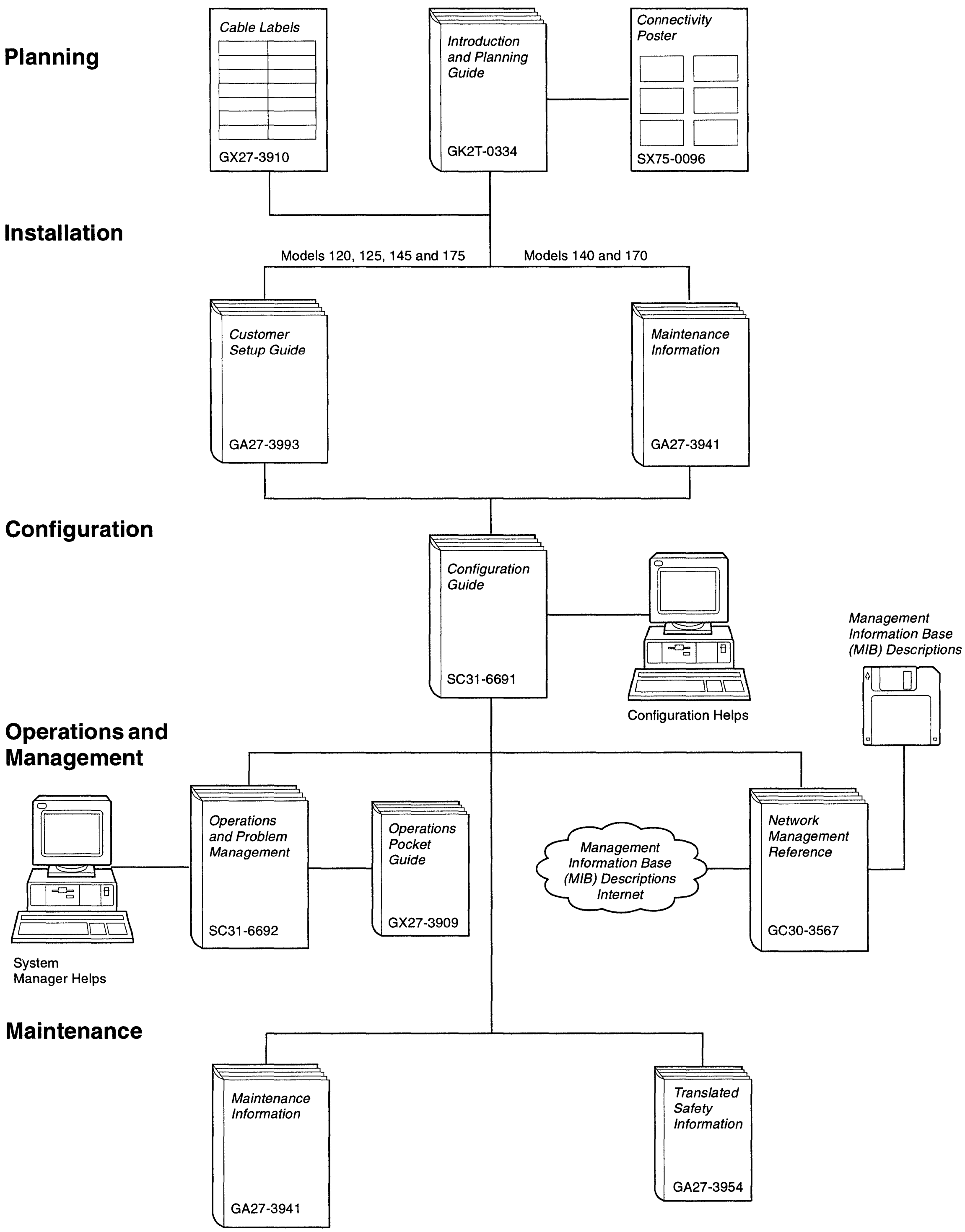


Figure 0-1. The 6611 Library

Library Overview

Table 0-1 shows the IBM 6611 Network Processor and the IBM Multiprotocol Network Program library, arranged according to tasks.

Table 0-1 (Page 1 of 2). Release 3 Library

Planning	
GK2T-0334	*IBM 6611 Network Processor Introduction and Planning Guide* Part I of this book provides information needed to understand the functions of the 6611, how to order it, and how to plan and to prepare for its installation. Part II is an overview of networking concepts and designs. Part III is a protocol reference that includes details about each of the protocols that the 6611 supports. The *IBM 6611 Network Processor Connectivity* poster is packaged with this book.
SX75-0096	*IBM 6611 Network Processor Connectivity* poster This poster illustrates some of the connectivity options for Models 120, 125, 140, 145, 170 and 175. **Note:** This poster is shipped with the *Introduction and Planning Guide* and can also be ordered separately.
GX27-3910	*IBM 6611 Network Processor Cable Labels* These labels, when completed, provide information about the: • 6611 adapters and the network devices to which the cables will be connected • Network to which the adapter will be attached • Network management support, if any, for that network **Note:** In previous releases, the cable labels had been included in the *Introduction and Planning Guide*; you can now order them separately.
Installation and Maintenance	
GA27-3993	*IBM 6611 Network Processor Customer Setup Guide* This book, shipped with Models 120, 125, 145, and 175, explains how to: • Prepare each model for installation • Install each model • Verify the successful installation of each model • Install the available features for each model • Setup an ASCII terminal and a modem so that they can communicate with the 6611 • Perform an orderly shutdown of the 6611 **Note:** GA88-6199 is the Japanese version of this book.
GA27-3941	*IBM 6611 Network Processor Maintenance Information* This book provides maintenance information for Models 120, 125, 140, 145, 170 and 175. It also provides installation instructions for Models 140 and 170. It shows how to remove and replace field replaceable units and it identifies adapters and cables that are used with the 6611.

Table 0-1 (Page 2 of 2). Release 3 Library	
GA27-3954	*IBM 6611 Network Processor Translated Safety Information* This book provides translations for caution and danger notices and other safety information found in the *IBM 6611 Network Processor Maintenance Information* and the *IBM 6611 Network Processor Customer Setup Guide*.
Configuration	
SC31-6691	*IBM Multiprotocol Network Program Configuration Guide* This book explains how to install and use the Configuration Program. It also provides instructions, examples, and scenarios that enable you to customize your 6611 configuration.
Operations and Management	
SC31-6692	*IBM Multiprotocol Network Program Operations and Problem Management* This book describes how to use the System Manager component of the IBM Multiprotocol Network Management Program to perform these tasks: • Operate the 6611 and monitor its status • Perform software problem determination • Install and maintain software • Maintain hardware • Use System Manager helps, including the fast-path • Use the fast-path commands
GX27-3909	*IBM 6611 Network Processor Operations Pocket Guide* This book shows how to operate the 6611 and explains error and status codes. It provides brief descriptions of the System Manager menus and fast-path commands.
GC30-3567	*IBM 6611 Network Processor Network Management Reference* This book provides: • Information on the network management facilities provided by the IBM 6611. • A high-level overview of the Simple Network Management Protocol (SNMP) as well as complete descriptions of the SNMP traps and SNA alerts supported. • A description of how the IBM LAN Network Manager manages token-ring networks that are remotely or locally attached to the IBM 6611. The *IBM Multiprotocol Network Program MIB Diskette* is packaged with this book.

Library Ordering Information

All IBM 6611 publications can be ordered separately.

These publications are shipped with the IBM 6611:

IBM 6611 Network Processor Customer Setup Guide (shipped with Models 120, 125, 145, and 175)

IBM 6611 Network Processor Maintenance Information

IBM 6611 Network Processor Operations Pocket Guide

IBM 6611 Network Processor Translated Safety Information

These publications are shipped with the IBM Multiprotocol Network Configuration Program:

IBM Multiprotocol Network Program Configuration Guide
IBM Multiprotocol Network Program Operations and Problem Management
IBM 6611 Network Processor Introduction and Planning Guide

The *IBM Multiprotocol Network Program MIB Diskette* is packaged with the *IBM 6611 Network Processor Network Management Reference*. The MIBs are also available over the Internet. Internet retrieval instructions are included in the *IBM 6611 Network Processor Network Management Reference*.

Obtaining Softcopy Information

Softcopy BookManager* READ library information will be available for many of the IBM 6611 publications on the *IBM Networking Systems Softcopy Collection Kit.* To place a single order for the CD-ROM, use form number SK2T-6012. To place a single order for the 3480 cartridge, use form number SK2T-6013.

Yearly subscriptions for the *IBM Networking Systems Softcopy Collection Kit*, product number 5636-PUB, are available through your branch office representative. Order feature code 2003 and media code 5003 for CD-ROM format. Order feature code 2004 and media code 5004 for 3480 cartridge format.

Note: The *Customer Setup Guide*, *Maintenance Information*, *Translated Safety Information*, *Connectivity* poster, and *Cable Labels* are not available in softcopy format.

Chapter 1. Understanding the Configuration Tasks

This chapter explains the configuration tasks and directs you to information about:

- Planning your network topology and strategy
- Installing the Configuration Program
- Updating existing configuration files and preparing for new configurations
- Using the Configuration Program
- Transporting configuration files to the 6611
- Starting the 6611

This chapter also includes a sample configuration that illustrates the configuration process, and some tips on configuration troubleshooting.

Planning Your Network Topology and Strategy

For detailed information about planning your networking topology and strategy, refer to *Introduction and Planning Guide.*

Focus on configuring your network devices to form a unified network that functions correctly; each device in your network must be configured so it is compatible with all other devices. To ensure compatibility throughout the network, it is recommended that a single individual or team define or approve the configuration for each network device, including each 6611.

It is recommended that you implement your network in three phases: first, in a simulation network; second, in a limited segment of your real production network; and third, in your full production network.

Implementing a Network for Simulation

Connect network devices, including your 6611s, to form a network that closely resembles your real production network. Set up an 6611 configuration workstation, and use it to configure each 6611 for Internet Protocol (IP) only. Test the network to make sure IP connectivity has been established.

When you have established IP connectivity, configure each 6611 for one additional protocol. Test the network to make sure this protocol is functioning correctly. Continue adding and testing one protocol at a time until you have successfully tested each of the protocols you plan to transport on your production network.

Finally, test the network to make sure all the protocols function correctly simultaneously.

Implementing a Limited Production Network

After you have verified connectivity within a simulated network, you are ready for a limited production network implementation. Attach your 6611s to an isolated segment of your production network, so that any adverse impact to your network will be limited to this segment. Try to perform this implementation at a time when it is not critical that this segment be functioning correctly.

As in the simulated network, first configure each 6611 for IP only, and test the limited network to make sure IP connectivity has been established. Then configure each 6611 for one additional protocol and test the limited network to make sure this protocol functions correctly. Continue to add and test one protocol at a time until you have successfully tested all protocols you want to transport on your full production network.

Finally, configure each 6611 for all the protocols you plan to transport on the full production network. Test the limited network to make sure all the protocols function correctly simultaneously.

Implementing Your Full Production Network

After you have verified connectivity in a limited production network, you are ready for full production network implementation. Try to perform this implementation at a time when it is not critical that your production network be functioning correctly.

Repeat the procedures outlined in "Implementing a Limited Production Network" on page 1-1, adding and testing on your full network first IP, then each of the other protocols, and finally all the protocols together.

Installing the Configuration Program

Install the Configuration Program on a RISC System/6000* workstation or on a Personal Systems/2* (PS/2)* workstation. Read Chapter 2 on page 2-1 for instructions.

Updating Existing Configuration Files

If Version 1 Release 1.0, Version 1 Release 1.1, Version 1 Release 1.2, or Version 1 Release 2 configuration files exist, migrate these files to Version 1 Release 3. See "Migrating to the Version 1 Release 3 Configuration Program" on page 2-4 for instructions.

Preparing for New Configurations

This section contains a sample scenario with step-by-step instructions for preparing the configuration worksheet before using the Configuration Program.

1. Sketch a diagram of your network so that you have a visual representation to work from. For complex networks, you may need more than one sketch to show the interconnections. For example, you might have one sketch or set of sketches that show a high-level view of the areas, groups, and concepts for your network. Other sketches might provide detail for each section of the network and specify values you will configure.

   Figure 1-1 on page 1-3 shows the sample network that is being configured. Customized values are shown.

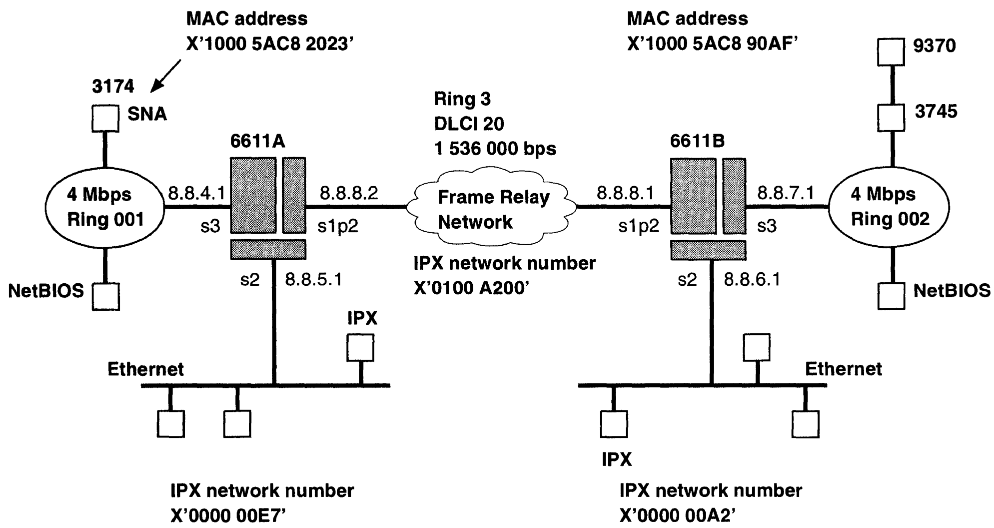


Figure 1-1. Sample Network

This network includes:

- 6611 A, which has the following ports and protocols running:
  - A serial port running Internet Protocol (IP), Internetwork Protocol Exchange (IPX), Systems Network Architecture (SNA), and Network Basic Input/Output System (NetBIOS) over frame relay
  - A token-ring port running SNA and NetBIOS
  - An Ethernet port running IPX
- 6611 B, which has the following ports and protocols running:
  - A serial port running IP, IPX, SNA, and NetBIOS over frame relay
  - A token-ring port running SNA and NetBIOS
  - An Ethernet port running IPX

6611 A and 6611 B are configured to route IPX and source route bridge SNA and NetBIOS across the frame-relay network.

Note: For complete configuration information for Figure 1-1, see "Sample Network Running IPX, IP, and DLSw" on page A-1.

2. For your convenience, you can fill out one of the Planning Charts from the *Introduction and Planning Guide* and the *About Your Machine* sheet that is provided with the 6611. A Planning Chart lists the protocols and functions you can configure in the 6611. The *About Your Machine* sheet lists which port is placed in each slot.

3. You can fill in the configuration worksheets before using the Configuration Program. Determine the configuration worksheets you need to fill out for the ports. These configuration worksheets are located with the port information in Chapter 4. Make copies of the configuration worksheets for each port in your machine.

4. After completing the port worksheets, select and copy the worksheets for the protocols that will be used on each port. These worksheets are located with the protocol information in Chapter 5.

5. After completing the protocol worksheets, select and copy the worksheets for the node management parameters you will configure. These worksheets are located with the node management information in Chapter 6.

The following configuration worksheets (Table 1-1 on page 1-4 to Table 1-3 on page 1-6) show the customized parameters needed to configure the serial port on 6611 A in Figure 1-1 for IP over frame relay.

Note: Defaults are accepted for all configuration parameters whose values are not given.

Table 1-1 (Page 1 of 2). Configuration Worksheet - Serial Port - Physical Interface - 6611 A

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable physical interface on this port Enable, Disable Enable This parameter enables or disables one of the ports on the 6611 2-Port Serial Adapter.	Enable
Parameter **Valid Values** **Default** **Description**	Interface cable (available only on A25 and A47 adapters) EIA 422 or X.21; V.35, V.36, or EIA 232 EIA 422 or X.21 This parameter specifies the type of interface cables for the serial port.	
Parameter **Valid Values** **Default** **Description**	Cylink serial number 00 000 000 to 99 999 999 None This parameter specifies the serial number of the data service unit/channel service unit (DSU/CSU) connected to this serial port.	
Parameter **Valid Values** **Default** **Description**	Transmit clock source (available only on A25 and A47 adapters) DTE, DCE DTE This parameter specifies how the transmit clock source transmits data.	
Parameter **Valid Values** **Default** **Description**	Serial line speed 9 600 to 2 048 000 bps 19 200 bps Set the serial line speed parameter to the clock rate provided by an external clocking source, such as a modem. This parameter does not change the actual clocking rate or line speed but will affect the metric value that is used to determine the cost of the route. When you use a network management station to view the the ifSpeed variable in the MIB II interface, this parameter provides the value that is displayed. **Note:** LAN Bridging Protocol uses the value of this parameter to determine the default telecommunications link error threshold.	1 536 000
Parameter **Valid Values** **Default** **Description**	Data encoding NRZI, NRZ NRZI This parameter specifies how the line transition occurs on the serial link attached to this serial port. NRZI is a common setting for modems. This setting indicates that a line transition occurs for each zero bit (the transition occurs at the start of the data bit cell). A 1 is represented by a continuous level. To keep from losing clock synchronization, you should use a stream of zeros. When you select NRZ, the data line reflects ones and zeros by level. If the data is 1 for several consecutive bits, the level of the line remains a constant 1. To keep from losing clock synchronization, you should use a stream of alternating ones and zeros.	

Table 1-1 (Page 2 of 2). Configuration Worksheet - Serial Port - Physical Interface - 6611 A

Parameter Information		Your Value
Parameter	Locally administered MAC address	
Valid Values	X'0000 0000 0000' to X'FFFF FFFF FFFE'	
Default	None	
Description	This parameter specifies the locally administered MAC address assigned to the adapter attached to this port. This MAC address is the node addressed for this port and is used: • To make routing decisions for IPX and XNS. • To enable the 6611 to generate a bridge identifier for the bridge when no local LAN ports are enabled for bridging.	
Parameter	Enable port for transmission group	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter allows you to enable or disable 2 T1 in a transmission group (2T1-TG) on this port.	
Parameter	Transmission group name	
Valid Values	1 to 8 characters, A to Z, 0 to 9	
Default	None	
Description	This parameter specifies a TG name. Each TG name on the 6611 must be unique.	

Note: A 6611 port, being both a source and sink for data, is known as data terminal equipment (DTE). A device which connects a 6611 to a network is known as data circuit-terminating equipment (DCE).

Table 1-2 (Page 1 of 2). Configuration Worksheet - Serial Port - Frame-Relay - 6611 A

Parameter Information		Your Value
Parameter	Enable frame relay on this port	
Valid Values	Enable Enable, Disable	
Default Value	Enable (when selected in the pop-up menu when the serial port is selected; if nothing is selected, then it is undefined)	
Description	This parameter enables or disables frame-relay frame forwarding on this port.	
Parameter	Polling interval	
Valid Values	5 to 30 seconds	
Default Value	10 seconds	
Description	This parameter specifies the number of seconds between successive status inquiry messages. When the LMI option parameter is set to **None**, this parameter has no effect.	
Parameter	Full inquiry interval	
Valid Values	1 to 255	
Default Value	6	
Description	This parameter specifies the number of polling intervals that pass before issuance of a full status inquiry message. When the LMI option parameter is set to **None**, this parameter has no effect.	
Parameter	LMI option	
Valid Values	ANSI T1.617 Annex D, LmiRev1, None	
Default Value	ANSI T1.617 Annex D	
Description	This parameter specifies the type of LMI that is active on the frame-relay network.	

Table 1-2 (Page 2 of 2). Configuration Worksheet - Serial Port - Frame-Relay - 6611 A

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Use InARP to resolve remote protocol addresses Enable, Disable Enable This parameter determines if the protocol addresses of the remote routers that are communicating with your IBM 6611 using frame relay are resolved by using InARP.	
Parameter **Valid Values** **Default Value** **Description**	DLCIs assigned to this port (required for each DLCI defined) A valid DLCI (integer of value in the recommended range of 15 to 1008 decimal) None This parameter contains a list of DLCIs.	20

Table 1-3 (Page 1 of 2). Configuration Worksheet - Serial Port - IP over Frame Relay - 6611 A

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable IP routing on this port Enable, Disable Disable This parameter enables or disables IP routing on a port.	Enable
Parameter **Valid Values** **Default** **Description**	IP address (required) IP addresses can be class A, class B, or class C • The class A range is 1.0.0.1 through 126.255.255.254 • The class B range is 128.0.0.1 through 191.255.255.254 • The class C range is 192.0.0.1 through 223.255.255.254 None This parameter defines the IP address of this port.	4.67.48.1
Parameter **Valid Values** **Default** **Description**	Subnet mask Value between 0.0.0.0 and 255.255.255.255. 255.255.255.255. The subnet mask must cover the network portion of the IP address.	255.255.255.255
Parameter **Valid Values** **Default** **Description**	Maximum transmission unit • 4 MB Token ring: 256 to 4472 bytes • 16 MB Token ring: 256 to 17800 bytes • Version 2.0 Ethernet: 256 to 1500 bytes • 802.3 Ethernet: 256 to 1492 bytes • Serial (V.35/36): 256 to 2048 bytes • X.25: 256 to 4096 bytes • Token ring - 1492 • Ethernet - 1492 • Serial - 1500 • X.25 - 576 The maximum transmission unit (MTU) is the number of bytes per frame of data that can be transferred across a given physical network.	
Parameter **Valid Values** **Default** **Description**	Enable Internet Control Message Protocol (ICMP) address mask requests Enable, Disable Enable This parameter allows a network administrator to enable or disable ICMP mask requests.	

Table 1-3 (Page 2 of 2). Configuration Worksheet - Serial Port - IP over Frame Relay - 6611 A

Parameter Information		Your Value
Parameter	Directed broadcast	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables directed broadcast. When this parameter is set to **Enable** and IP receives an *all host broadcast* UDP message that is destined for another interface in this router, IP forwards the message to that interface.	
Parameter	Point-to-point only	
Valid Values	Enable, disable	
Default	Disable	
Description	When this parameter is enabled, this interface will *only* support point-to-point links. Broadcast or mesh connections will not be supported on this interface.	
Parameter	Assignment for discovered DLCIs	
Valid Values	Mesh, Point-to-point	
Default	Mesh	
Description	This parameter indicates whether the DLCIs, which are discovered via the LMI options, will be assigned to the meshed network on this port or to a point-to-point link on this port.	

To prepare to configure the network in Figure 1-1 on page 1-3, you would also prepare configuration worksheets for:

- Serial Port - IPX over Frame Relay

- Ethernet Port - Physical Interface
- Ethernet Port - IPX

- Token-Ring Port - Physical Interface
- Token-Ring Port - Source Route Bridging
- Token-Ring Port - SNA
- Token-Ring Port - NetBIOS

- Node Level - IPX Routing
- Node Level - Source Route Bridging
- Node Level - DLSw
- Node Level - SNA
- Node Level - NetBIOS

6. For more information, you might also refer to the sample configurations that are included with each protocol in Chapter 5 on page 5-1. These samples include tables that summarize all the customized parameters in each sample. Defaults are accepted for all configuration options not shown.

   Note: For complete configuration information for Figure 1-1 on page 1-3, see "Sample Network Running IPX, IP, and DLSw" on page A-1.

Using the Configuration Program

For specific information about using the Configuration Program, read Chapter 3 on page 3-1.

Use the Configuration Program to create a unique configuration for each 6611 in your network. The configuration parameters for several 6611s may be similar, and you may be tempted to modify one configuration to fit the other 6611s. This is risky, and it is *not* advised. It is generally difficult to change a copy of one configuration into a configuration for another 6611 without making errors. Remember, the 6611s have different addresses, and often you must specify different parameters for each so that they are compatible.

Remember to configure node management, then ports, then protocols, then node configuration for all routing and bridging configurations except DECnet**. For DECnet configurations, configure node management first, then node configuration, and then configure ports and protocols.

Transporting the Configuration Files to the 6611

Transport each configuration file to the respective 6611. Read "Transporting the Configuration File to the 6611" on page 3-29 for instructions.

It is recommended that all configurations and updates of your 6611s be debugged and sent from a central control point. (Exceptions are the initial configurations; it is recommended that you load initial configurations by diskette onto your 6611s.) This permits a single individual or team to monitor and test the network and coordinate network changes. See Chapter 7 on page 7-1 for information about sending configurations remotely to an 6611.

Starting the 6611

Read *MPNP Operations and Problem Management* for instructions for starting the 6611.

Have patience when the 6611 is loading. It may take considerable time for some configurations to load and become functional, especially if the advanced network protocols such as OSPF are used in a large network. For large networks with thousands of devices, it is not unusual for the loading process (in which the MPNP is initialized and network connectivity to other routers is established) to take 15 minutes or more.

Configuration Troubleshooting

Errors in the Configuration Program may cause different types of problems. A problem with configuration may appear initially to be a hardware problem because the 6611 will not start or data will not flow through a port. In addition, problems with configuration may not result in an error initially; an error may occur only when specific conditions are encountered or when heavy network traffic occurs.

If you cannot resolve a problem after making a few changes to your configuration, generate a new configuration. Endless changes to a configuration often compound the problem, whereas a new configuration can usually be generated and quickly tested.

Chapter 2. Installing the Configuration Program

This chapter provides information to enable you to install and start the configuration program on a RISC System/6000 workstation or on a Personal System/2 (PS/2) workstation. This chapter also includes information about migrating from Version 1 Release 1.0 (V1R1.0), Version 1 Release 1.1 (V1R1.1), Version 1 Release 1.2 (V1R1.2), or Version 1 Release 2 (V1R2) to Version 1 Release 3 (V1R3).

Understanding Which Files Are Copied During Installation

When you install the Configuration Program on a RISC System/6000 or PS/2 workstation, several files are copied to the installation directory, which is *cfg130* by default. The files that are copied vary according to the type of workstation you are using. If you want to change the name of the installation directory, enter the name you prefer before installing the Configuration Program files. The following lists provide the file names for each type of workstation:

- AIXwindows* workstations
  - README
  - cfg.aix
  - cfg.app
  - cfg.hlp
  - cfg.msg
  - cfg
  - cfg.ini (aix.ini is located on Configuration Program Diskette 1)
  - cfg.lgo
  - cfg.ico
- Microsoft Windows** 3.0 workstations
  - README
  - cfg.exe
  - cfg.app
  - cfg.hlp
  - cfg.msg
  - cfg.ini (win30.ini is located on Configuration Program Diskette 1)
  - cfg.lgo
  - cfg.ico
  - winmem32.dll
- Microsoft Windows 3.1 workstations
  - README
  - cfg.exe
  - cfg.app
  - cfg.hlp
  - cfg.msg
  - cfg.ini (win31.ini is located on Configuration Program Diskette 1)
  - cfg.lgo
  - cfg.ico
  - winmem32.dll

- OS/2 2.1 workstations
  - README
  - cfg.exe
  - cfg.app
  - cfg.hlp
  - cfg.msg
  - cfg.ini (os2.ini is located on Configuration Program Diskette 1)
  - cfg.lgo
  - cfg.ico

Optionally, you can also install configuration samples. If you choose to install the samples, the samples.cdb and samples.doc files are also copied to the installation directory.

Note: The Configuration Program uses the user defaults file, *cfg.ini*, to set user-specified application configurables, such as font, when the program is started. Although this file can be edited manually using a text editor, such as *vi*, IBM recommends that you make changes to the user defaults file by using the User Preference window. The *ini* file will be written when you select the OK push button. If cfg.ini is not in the installation directory, the default attributes are used.

You need special fonts to run the IBM Multiprotocol Network Program Configuration Program. From an AIX* window, use the command **xset -q** to access the fonts.

RISC System/6000 Workstation Installations

This section describes how to use the Configuration Program on a RISC System/6000 workstation.

Hardware and Software Requirements

The following hardware and software are required to operate the Configuration Program on the RISC System/6000 workstation:

- AIX 3.1.5 or later with Transmission Control Protocol/Internet Protocol (TCP/IP) enabled
- AIXwindows
- 16 MB of memory
- 3.5-inch diskette drive that can read and write 1.44 MB-formatted diskettes
- 10 MB of available space on the fixed disk drive
- Graphics display that supports 640×480 resolution and 16 colors or gray scales
- Mouse

Installing the Configuration Program

To install the Configuration Program on a RISC System/6000 workstation.

Step 1 Log in to AIX as a non-root user.

Step 2 Place diskette 1 in the 3.5-inch diskette drive.

Step 3 At the AIX prompt, type the following commands:

Note: AIX is case-sensitive.

dosread -a install.aix install.aix

Where:

dosread	Reads the file from a DOS diskette and places it in the current directory.
-a	Converts the DOS file to an AIX file.
install.aix	The file name on the diskette.
install.aix	The file name to be used in the AIX system.

If the install.aix command fails, it may indicate that the current directory is not part of your search path. To continue the install, type: **./install.aix**

Then type: **chmod 550 install.aix**

Where:

chmod	Changes the file permissions given to the owner and group.
550	Defines the permission types for a user, group, and other users. In this case, the user and group are allowed read and execute permission, and others are allowed only read permission.
install.aix	The name of the file for which you are changing the permissions.

Step 4 Type **install.aix** at the AIX prompt and press **Enter**.

Step 5 Follow the prompts that appear on the screen to complete the installation.

PS/2 Workstation Installations

This section describes how to use the Configuration Program on a PS/2 workstation or on a compatible workstation.

Hardware and Software Requirements

The following hardware and software are required to use the Configuration Program on a PS/2 workstation using an Intel** 80386** or higher processor or a compatible system which has an Intel 80386 or higher processor. For workstations running Windows, the following is required:

- IBM DOS 3.3 or later, MS-DOS** 3.3 or later
- Microsoft Windows 3.0 or 3.1
- 8 MB of memory
- 3.5-inch diskette drive that can read and write 1.44 MB-formatted diskettes
- 10 MB of available space on the fixed disk drive
- Graphics display that supports 640×480 resolution and 16 colors or gray scales
- Mouse

For workstations running OS/2, the following is required:

- Operating System/2 (OS/2) 2.1
- 10 MB of memory
- 3.5-inch diskette drive that can read and write 1.44 MB-formatted diskettes
- 10 MB of available space on the fixed disk drive

- Graphics display that supports 640×480 resolution and 16 colors or gray scales
- Mouse

Installing the Configuration Program...

On a Workstation Running OS/2

To install the Configuration Program on a PS/2 workstation running OS/2, follow these steps:

Step 1 Place diskette 1 in the diskette drive.

Step 2 At the OS/2 prompt, type **a:os2inst** and press **Enter**.

Step 3 Follow the prompts that appear on the screen.

On a Workstation Running Windows

To install the Configuration Program on a PS/2 workstation running Windows, type **win a:install** beside the DOS prompt, or follow these steps:

Step 1 Type **win** beside the DOS prompt to start Windows.

Step 2 Place diskette 1 in the diskette drive.

Step 3 Select **File** from the menu bar.

Step 4 Select **Run** from the pull-down window.

Step 5 Type **a:install** on the command line and select **OK** to start the installation.

Step 6 Follow the prompts that appear on the screen.

After a successful installation on a workstation running either OS/2 or Windows, an icon labeled 6611 Configuration will be added to the program group you specify using the installation program or, by default, to the IBM 6611 program group.

Note: In a subsequent installation, a second icon labeled 6611 Configuration is added to the Main program group. To delete one of the icons, follow these steps:

Step 1 Select the icon that you want to delete.

Step 2 Select **File** from the menu bar.

Step 3 Select **Delete** from the cascade menu.

Step 4 An information message window is displayed. Select **Yes** to delete the icon.

Migrating to the Version 1 Release 3 Configuration Program

The configuration formats for V1R1.0, V1R1.1/V1R1.2, V1R2, and V1R3 are not compatible. If you want to use configuration files created using MPNP V1R1.0, V1R1.1/V1R1.2, or V1R2, you must migrate the configuration files to V1R3.

The Configuration Program converts the configuration files automatically when you read them from diskette, from your workstation, or when you retrieve them from an active 6611 using the the Communicate function of the Configuration Program. When migrating, do not use System Manager to create your first MPNP V1R3 configuration file. You must use the MPNP V1R3 Configuration Program to convert old version configuration files to produce your new MPNP V1R3 configuration files.

It is recommended that you create a back up of each configuration file *before* you convert it to the V1R3 format. After a configuration file is converted to the new format, the V1R1.0, V1R1.1/V1R1.2, and V1R2 MPNP and its IBM Multiprotocol Network Program Configuration Program will not be able to read the file. Once configuration files have been migrated to a newer release, there is no way to convert these files back to their original release.

The old version configuration files that you are converting might exist in one of three places:

- On diskette
- In the 6611
- In a configuration database (*.cdb) on the configuration workstation

If there are MPNP V1R1.0, V1R1.1, V1R1.2, and V1R2 configuration files that exist only in the 6611, save them on diskette before you upgrade the MPNP code in the 6611 to the V1R3 level. At least two copies of each needed configuration should be saved. One copy is converted to the MPNP V1R3 format and the other is saved for backup purposes.

Converting Configuration Files From Diskette

Follow these steps to convert configuration files from diskette:

1. From the menu bar of the V1R3 Configuration Program, select the **Configure** pull-down and then select **Read configuration diskette**. The Configuration Program displays a warning message to indicate that the configuration being loaded from the diskette is an old version and enables you to continue or cancel the conversion.[1]
2. Determine whether the 6611 for which the configuration file is destined will be upgraded to V1R3 or has already been upgraded to V1R3 and do one of the following:
   - When the configuration file is destined for a 6611 which will be upgraded to V1R3, configure the Schedule Configuration option. From the main menu, select **Node Management** and then select **Schedule Configuration**. On the Schedule Configuration window, set the Apply configuration parameter to **At upgrade** and set the Source release parameter to the release of MPNP before the upgrade is applied. The V1R3 configuration is activated after the 6611 had been upgraded to V1R3.
   - When the configuration file is destined for a 6611 which has already been upgraded to V1R3, do *not* configure the Schedule Configuration option. The configuration file is applied immediately.
3. Select the **Configure** pull-down and then select **Create configuration diskette**. When the diskette is complete, take it to the 6611 that is being upgraded to V1R3.

[1] You can set message prompting to disable the display of messages when upgrading previous level configuration files. Select the **Options** pull-down from the menu bar, and then select **Message prompting**. Disable the Upgrade of previous level configuration files parameter.

Converting Configuration Files Retrieved From an Active 6611

Follow these steps to convert configuration files retrieved from an active 6611:

1. From the menu bar of the V1R3 Configuration Program, select the **Communicate** pull-down, and then select **Retrieve** and select the **configuration** or **current configuration** option. The Configuration Program displays a warning message to indicate that the configuration being loaded from the diskette is an old version and enables you to continue or cancel the conversion.[1]

   Note: The 6611 may display a C73 error code as the Configuration Program attempts communication with the 6611 using V1R3 type messages before using V1R1.0, V1R1.1/V1R1.2, or V1R2 type messages. This condition is normal when using the V1R3 Configuration Program to communicate with an older version of the MPNP.

2. Determine whether the 6611 for which the configuration file is destined will be upgraded to V1R3 or has already been upgraded to V1R3 and do one of the following:

   - When the configuration file is destined for a 6611 which will be upgraded to V1R3, configure the Schedule Configuration option. From the main menu, select **Node Management** and then select **Schedule Configuration**. On the Schedule Configuration window, set the Apply configuration parameter to **At upgrade** and set the Source release parameter to the release of MPNP before the upgrade is applied. The V1R3 configuration activates after the 6611 had been upgraded to V1R3.
   - When the configuration file is destined for a 6611 which has already been upgraded to V1R3, do *not* configure the Schedule Configuration option. The configuration file is applied immediately.

3. Select the **Configure** pull-down, and then select the **Save** option and then select **Save and validate**.[2]

4. To send converted configuration files back to the 6611s, select the **Communicate** pull-down, and then select **Send** and select the **current configuration** or **multiple configurations** option. For more information about sending configurations, read "Direct IP Connection" on page 3-30.

Converting Multiple Configuration Files From a Configuration Database

Follow these steps to convert one or more configuration files from a configuration database:

1. Determine whether you want the Configuration Program to prompt you for each configuration file as it is converted.

   To disable message prompting from the menu bar of the V1R3 Configuration Program, select **Options** pull-down from the menu bar, and then select **Message prompting**. Disable the Upgrade of previous level configuration files parameter. Then select **OK**.

2. Determine whether you want the Configuration Program to automatically validate each configuration file when copying from the configuration database.[2]

---

[2] Configuration files must be validated when you use the Send multiple configurations function of the Configuration Program to send configuration files to the 6611. When you try to send files that have not been validated, a warning message appears and the file is not sent.

To enable automatic validation, select the **Options** pull-down and then select the **Validation** option. The Validation window appears. Enable the Copying database configuration(s) parameter and then select **OK**.

3. Select the **Configure** pull-down and then select **Copy database configuration(s)**. The Copy Database Configuration(s) window appears. Determine whether to copy one configuration or multiple configurations and do one of the following:
   - To copy one configuration:
     a. Select the origin database file and the configuration to be copied.
     b. Specify the destination database file that will receive the configuration, or select the database file from the list of databases displayed.
     c. Specify the destination name of the configuration file being copied or select a file name from the list of configurations displayed.
   - To copy multiple configurations:
     a. Select the origin database file and the configurations to be copied. Selected configuration file names are highlighted.
     b. Specify the destination database file that will receive the configurations, or select the database file from the list of databases displayed. The Configuration name parameter is not available.
4. Determine how to transport the configuration files to the 6611s that are being upgraded the V1R3 and then transport the files. For more information, read "Transporting the Configuration File to the 6611" on page 3-29.

Chapter 3. Using the Configuration Program

This chapter explains how to start and operate the Configuration Program. This chapter also includes instructions for creating 6611 configurations and transporting them to the 6611.

Starting the Configuration Program

The procedure you follow for starting the Configuration Program depends whether your workstation is a RISC System/6000 workstation or a PS/2 workstation.

Note: Although the V1R3 Configuration Program may take longer to load, it runs faster than previous versions.

Starting the Configuration Program on a RISC System/6000 Workstation

The following are considerations for starting the Configuration Program on a RISC System/6000 workstation.

- X-Windows must be running on the workstation before starting the Configuration Program. (Type **xinit** to start X-Windows.)
- X11fnt.coreX.fnt must be installed to have access to the M.I.T X11.4 (75 DPI and 100 DPI) fonts.
- When using an xterm screen, change the current directory to the directory containing the Configuration Program files. For example, type **cd cfg.** Then, type **cfg**. The Configuration Program appears on the screen.

  Note: To start the Configuration Program, you must have write access to the directory that contains the Configuration Program. If you attempt to start the Configuration Program from a directory to which you do not have write access, the Configuration Program displays error messages and does not appear.
- Sometimes Configuration Program windows are positioned close to the upper left corner of the window instead of the upper left corner of the window border.

  To correct this problem on RISC System/6000 workstations using the OSF/Motif** window manager, the following offsets are recommended:

  Cfg6611.normal.mappingOffset: 11,27
  Cfg6611.transient.mappingOffset: 11,27
  Cfg6611.normal.configurationOffset: 0,0
  Cfg6611.transient.configurationOffset: 0,0
- As part of the installation, the Configuration Program uses the **dosread**, **doswrite**, and **dosdir** commands. The Configuration Program also uses these commands to read and write configurations to the diskette drive. These commands must be installed on the RISC System/6000 workstation before you install and use the Configuration Program.

After you have started the Configuration Program, see "Operating the Configuration Program" on page 3-10 for instructions.

Starting the Configuration Program on a PS/2 Workstation

To start the Configuration Program on a PS/2 workstation, double click on the icon representing the Configuration Program.

Understanding the Configuration Program

The Configuration Program is designed to simplify the task of configuring a network processor by providing you with:

- An easy-to-use graphical user interface
- Built-in range and dependency checking features that help prevent configuration errors
- An extensive help facility that serves as an online guide to configuration, providing help on each configuration option and program window, including detailed background helps on each bridging, routing, and transmission protocol supported by the 6611.

This section presents an overview of these features and describes how the program is organized.

How the Configuration Program Is Organized

The Configuration Program has four major parts, as described in Table 3-1 on page 3-3. Each part of the program can be accessed from the Configuration Program main window. By default, the main window displays four slots, which represents Model 140. The main window shown in Figure 3-1 illustrates seven slots, which represents a Model 170.

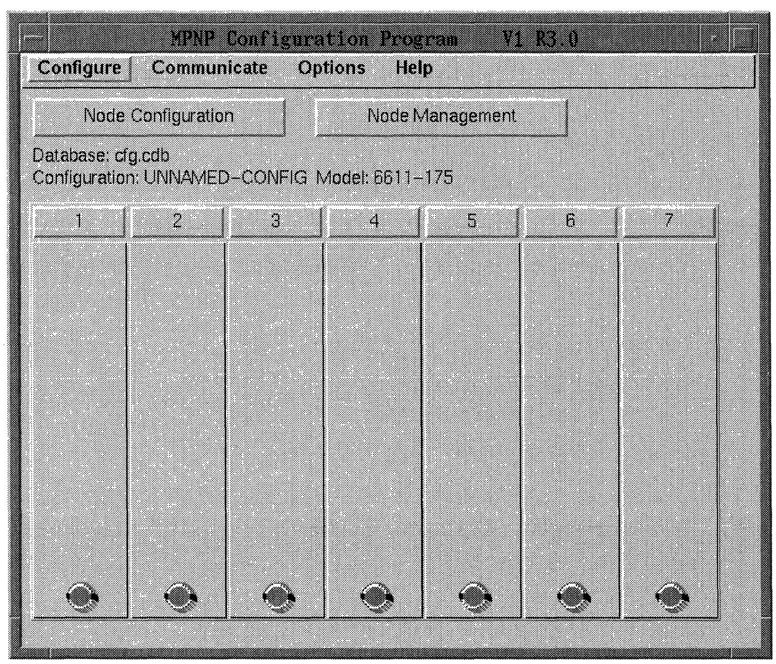


Figure 3-1. Configuration Program Main Window

Table 3-1. Configuration Program Organization

This Part...	Consists of...
Main window options	A menu bar at the top of the main window that contains the following options: • **Configure** — Select to open, save, and manage configuration files. • **Communicate** — Select to send files to and retrieve configuration data from a 6611. • **Options** — Select to tailor the Configuration Program to your own preferences or to display a configuration summary window. • **Help** — Select to display general help information for the Configuration Program and to access the Configuration Program tutorial.
Port configuration windows	A graphic on the main window of the Configuration Program that represents the physical adapter slots in a 6611. Adapters are added to the graphic by clicking on one of the numbered adapter slots and choosing an adapter from the pop-up menu that appears. When an adapter is displayed in the slot, the ports associated with that adapter are also displayed. Select the port icon to display the configuration windows for the port. These windows are used to configure the physical interface for the adapter port and each of the protocols supported on the port. Parameters configured for a specific port apply to that port only.
Node configuration window	A secondary window accessed from the Node Configuration push button on the main window. This window is used to configure protocol parameters that apply to all ports on the 6611.
Node management window	A secondary window accessed from the Node Management push button on the main window. This window lets you specify the host name for a 6611 and defines how the device will be managed through an IP network.

"Operating the Configuration Program" on page 3-10 walks you through each of these parts in detail.

Using the Configuration Program Interface

As described in Table 3-1, the Configuration Program consists of a main window with secondary windows for each adapter port, node configuration parameters, and node management parameters. Each of the secondary windows is arranged by protocol and function, and most configuration parameters are accessed by selecting an appropriate push button on these windows.

When you select the push button for a protocol or function, another window is displayed with parameters related to that protocol or function. In general, the parameters that must be answered to configure the protocol or function are contained on this first window. The window also may contain additional push buttons that enable you to define other optional parameters or features.

Control Features

The Configuration Program uses a number of control features to help you move from window to window, select configuration options, enter data, and manipulate data. These controls include:

- Push buttons
- Text entry fields
- Check boxes
- Radio buttons
- Drop-down lists
- Multiple-entry list boxes

Note: Most actions in the Configuration Program can be performed with a mouse or keyboard. Use of a mouse is highly recommended, however, to speed up the configuration task. In addition, some actions can be performed only with a mouse. The descriptions in this section assume the use of a mouse. For information on keyboard support for the Configuration Program, see Table 3-2 on page 3-8.

Push Buttons: Push buttons are used to move from one window to another within the Configuration Program or to perform a specific action. When you click on a push button, the action associated with the push button occurs immediately.

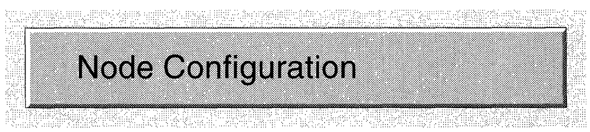


Figure 3-2. Push Button

The following *action* push buttons are commonly used within the program:

Button	**Action**
OK	Exit a window and save all changes
Reset	Reset parameter settings to their last saved state
Cancel	Exit a window without saving changes
Help	Display the help text for a window
Add	Access a detail window to add items to a list
Edit	Edit an item in a list
Delete	Delete one or more items from a list
Apply	Apply changes to a list without exiting the window
Clear	Reset the parameters for a list item to their default settings
Close	Exit a window (used in conjunction with the Apply push button)

Text Entry Fields: Text entry fields are used to enter text or numeric values. The control consists of a parameter name, followed by a range of acceptable values for the parameter (displayed in parentheses), and an entry field for the text. If the configuration parameter has a default value, the value is displayed in the entry field.

Figure 3-3 on page 3-5 illustrates a text entry field as it is displayed when the Configuration Program is running on a RISC/6000 workstation.

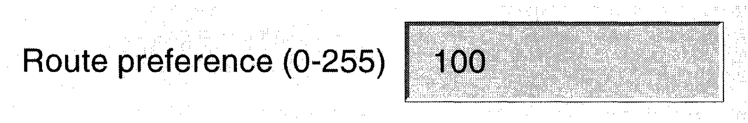


Figure 3-3. Text Entry Field Displayed on a RISC/6000 Workstation

Figure 3-4 illustrates a text entry field as it is displayed when the Configuration Program is running on a PS/2 workstation.

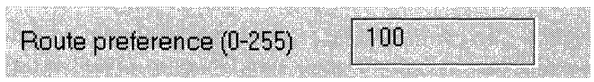


Figure 3-4. Text Entry Field Displayed on a PS/2 Workstation

Check boxes: Check boxes are used to enable or disable a parameter, protocol, or program option. Clicking on a check box changes its state. When enabled, the check box is highlighted.

Figure 3-5 illustrates check boxes as they are displayed when the Configuration Program is running on a RISC/6000 workstation.

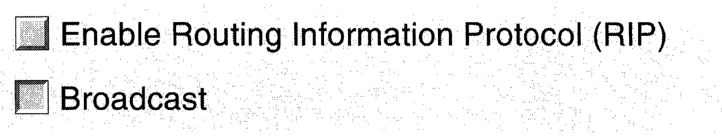


Figure 3-5. Check Boxes Displayed on a RISC/6000 Workstation

Figure 3-6 illustrates check boxes as they are displayed when the Configuration Program is running on a PS/2 workstation.

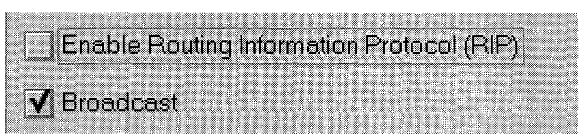


Figure 3-6. Check Boxes Displayed on a PS/2 Workstation

Note: When a check box is displayed with a push button, the check box can be used to enable or disable the function associated with the push button.

Radio Buttons: Radio buttons are used to select one option from a group of available options. An option is chosen by clicking on the radio button associated with the option. When enabled, the radio button is highlighted.

Figure 3-7 illustrates radio buttons as they are displayed when the Configuration Program is running on a RISC/6000 workstation.

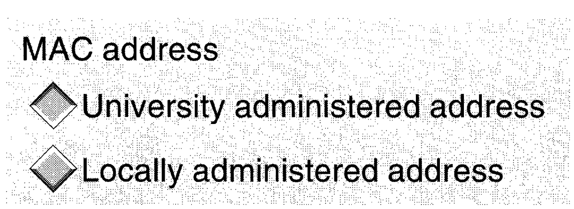


Figure 3-7. Radio Button Group Displayed on a RISC/6000 Workstation

Figure 3-8 on page 3-6 illustrates radio buttons as they are displayed when the Configuration Program is running on a PS/2 workstation.

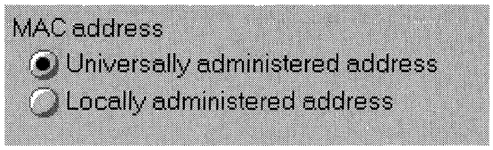


Figure 3-8. Radio Button Group Displayed on a PS/2 Workstation

Drop-Down Lists: Drop-down lists are used to select an option from a list of available options. The list is displayed by clicking on the List button to the right of the text field. When you select an option in the list, that option is displayed in the text field for the control. If the drop-down list has a default option, the default is displayed in the text field.

Figure 3-9 illustrates a drop-down list as it is displayed when the Configuration Program is running on a RISC/6000 workstation.

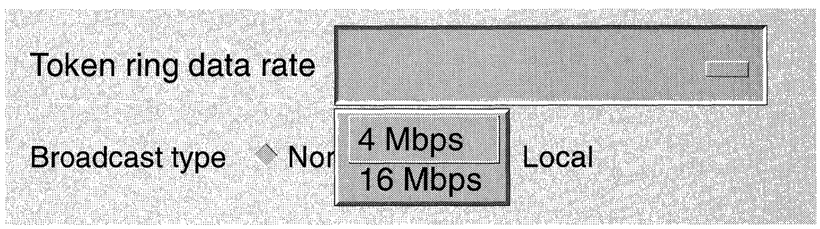


Figure 3-9. Drop-Down List Displayed on a RISC/6000 Workstation

Figure 3-10 illustrates a drop-down list as it is displayed when the Configuration Program is running on a PS/2 workstation.

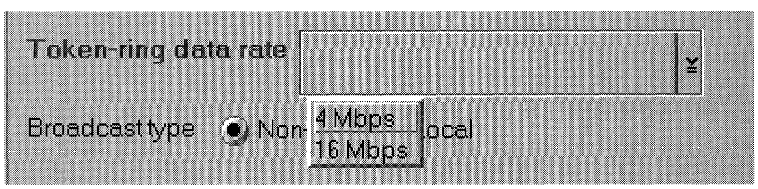


Figure 3-10. Drop-Down List Displayed on a PS/2 Workstation

Multiple-Entry List Boxes: Multiple-entry list boxes are used to create a list of items, such as filters or addresses, for use by a protocol or function. Two types of list boxes are used in the Configuration Program.

Figure 3-11 on page 3-7 shows an example of a simple list box. Values are entered in text fields to the left of the list box. When you click on the Apply push button, the values are stored as a single list entry in the list box. You can continue to add new entries to the list box until the maximum number of entries is reached. To display the values for an entry in the text fields, select the entry from the list. To delete one or more entries in the list, select the entries to be deleted and click on the Delete push button.

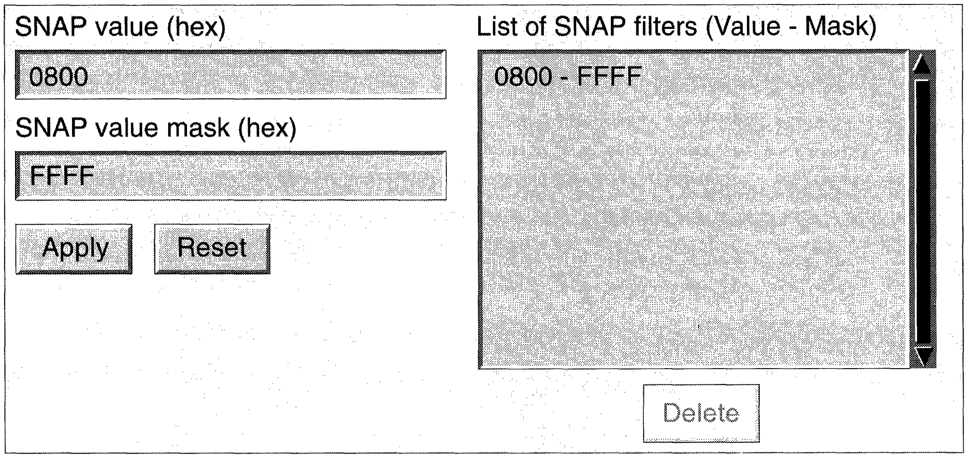


Figure 3-11. Simple Multiple-Entry List Box

Figure 3-12 shows the second type of list box. When you click on the Add push button, a detail window is displayed. Each time you answer the configuration parameters on this detail window and click on the Apply push button, an entry is added to the list box. The entry is made up of values configured on the window, so it is easy to identify. To display the window associated with an entry, select the entry from the list and click on the Edit push button. To delete one or more entries in the list, select the entries to be deleted and click on the Delete push button.

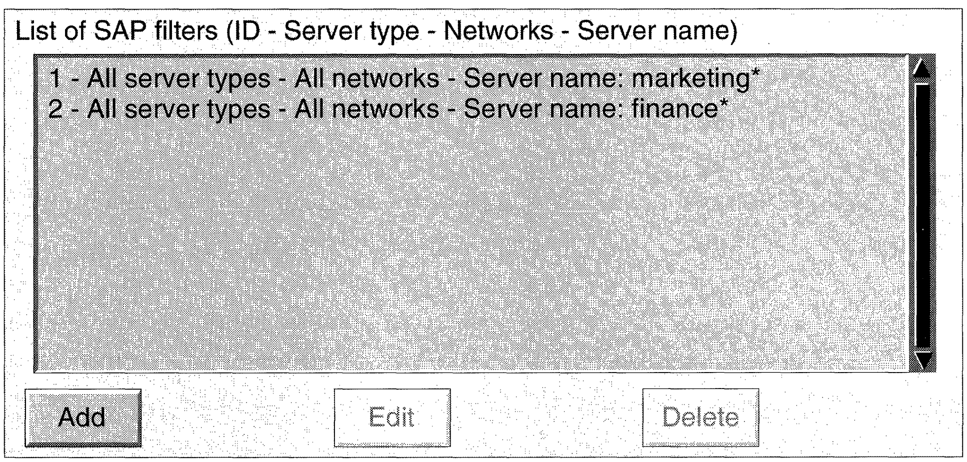


Figure 3-12. Multiple-Entry List Box with Associated Panel

Control Selection...

On a RISC/6000 Workstation: To select a text entry field in the Configuration Program when it is running on a RISC/6000 workstation, click on the field with the mouse. A horizontal box will appear around the field to show that it is the active field on the window. The background color of the field also will change.

To select another control on a window, such as a check box or radio button, click on the control itself. A horizontal box will appear around the control and any associated text to show that it is the active control on the window.

Note: When you enter a new window, the active control is always at the top of the window.

On a PS/2 Workstation: To select a text entry field in the Configuration Program when it is running on a PS/2 workstation, click on the field with the mouse. A carat appears it the first position of the field to show that it is the active field on the window.

To select another control on a window, such as a check box or radio button, click on the control itself. A horizontal box will appear around the text associated with the control to show that it is the active control on the window.

Note: When you enter a new window, the active control is always at the top of the window.

Copying, Cutting, and Pasting

Using the mouse in conjunction with the keyboard, you can copy, cut, and paste values that are displayed in text entry fields. Values can be copied from field to field on the same window, or from a field on one window to a field on another window.

To copy a value displayed in a text entry field to the another entry field, highlight the value by either double clicking on the value or by clicking on the value then holding the right mouse button while dragging the mouse. With the cursor placed over the field you are copying, click on the middle mouse button. A drop down menu that enables you to select copy, cut, or paste appears. Holding down the middle mouse button, move the mouse to select **copy**. The value is stored in the paste buffer, which can hold up to five values.

When you want to paste the *last* value copied, use the right mouse button and click on the destination text entry field. Hold the middle mouse button down and the drop down menu reappears. Select **paste**. The last value copied displays in the text entry field.

When you want to select a value to paste from the paste buffer, use the right mouse button and click on the destination text entry field. While pressing the shift key, hold the middle mouse button down and the drop down menu reappears. Select **paste**. A drop down menu displaying the last five values copied appears. Use the right mouse button to select the value to paste. The value is displayed in the text entry field.

To cut or remove a value using the mouse, highlight the value by either double clicking on the value or by clicking on the value then holding the right mouse button while dragging the mouse. Click on the middle mouse button. Hold down the middle mouse button and move the mouse to select **cut**. The value is removed from the text entry field.

Keyboard Support

Table 3-2 describes keyboard support for the Configuration Program.

Table 3-2 (Page 1 of 2). Configuration Program Keyboard Support

This Key...	Performs This Action...
Tab	Moves the cursor to the next available menu item, text entry field, push button, or other control in order from the top of a window or pop-up menu. The cursor appears as a horizontal box around the item or control.

Table 3-2 (Page 2 of 2). Configuration Program Keyboard Support

This Key...	Performs This Action...
Enter	Selects the menu item or control at the current cursor position. When the Configuration Program displays a message, the Enter key performs the same action as the OK push button.
Esc (Escape)	Exits a window without saving changes. The Esc key performs the same action as the Cancel push button.
F3	Exits a window without saving changes. The F3 key performs the same action as the Cancel push button.
F2	Resets parameter settings to their last saved state. The F2 key performs the same action as the Reset push button.
F1	Displays help for a text entry field or other window control at the current cursor position.
Delete	Deletes the next text character to the right (forward delete).
Backspace	Deletes the next text character to the left (backward delete).
Home	Moves the cursor to the beginning of the field. The cursor appears as a solid caret that indicates the cursor position in the field.
End	Moves the cursor after the last text character in the field. The cursor appears as a solid caret that indicates the cursor position in the field.
Left arrow	Moves the cursor one text character to the left.
Right arrow	Moves the cursor one text character to the right.

Additional Aids

The Configuration Program provides the following additional aids to help you configure the 6611:

Highlighting of Required Parameters: When a protocol or function is enabled in the Configuration Program, parameters that must be answered to successfully configure the protocol or function are displayed in bold and colored.

Configuration Question Marks: When a window contains required parameters that have not been configured, a question mark is displayed on the push button for the affected protocol or function. In addition, question marks are displayed:

- On the port icon on the main window when the required parameters are associated with a port.
- On the Node Configuration or Node Management push buttons when the required parameters are associated with a protocol or function on these secondary windows.

The question marks are removed when all required parameters are configured. By scanning the Configuration Program for question marks, you can quickly determine whether or not your configuration is complete.

Configuration Parameter Checks: The Configuration Program automatically checks any value entered for a parameter against the range of valid values for that parameter. When an error is detected, a message is displayed showing the range of valid parameter values. In addition, the program compares protocol addresses, as appropriate, to ensure that duplicate addresses have not been entered.

Configuration Parameter Defaults: Whenever possible, defaults are provided for configuration parameters to reduce the total number of parameters you need to define. Defaults typically reflect the recommended values for parameters, as documented in the protocol standard or applicable RFC. The optimal choice for any parameter, of course, depends on your particular network configuration.

Configuration Program Helps: The Configuration Program help windows are intended to be your primary source of information about individual configuration parameters and their dependencies. To display the help for any window in the program, select the Help push button on the window. The help for a configuration program window contains the following:

- A description of the window's purpose and any special features or restrictions.
- A *hypertext* link to each of the helps for individual configuration parameters on the program window. Hypertext links appear as highlighted text within the help window. When the highlighted text is selected, the program displays the help associated with the text.
- Hypertext links to related help topics and to the general help for the configuration protocol or function. This help includes configuration tips, background information, and any restrictions.

To display the specific help for a configuration parameter, position the cursor on the parameter field or a parameter option and press the F1 key. Individual parameter helps contain the following:

- A description of the configuration parameter
- The range of valid values or options for the parameter
- The default value for the parameter, if any
- A description of any dependencies this parameter has on other parameters
- Hypertext links to the window help, general help, and other related help topics

The hypertext links within each help enable you to move quickly from help to help without closing the initial help window. Hypertext links are also provided to link you to glossary definitions for terms used within the helps.

Operating the Configuration Program

Operating the Configuration Program is the same on a RISC System/6000 workstation and on a PS/2 workstation. When you run the Configuration Program, other files are created in the installation directory (by default) or in another directory whose path you specify. The Configuration Program can read or write the following types of files:

- Binary format configuration files

  The binary file format is known to the Configuration Program. Binary formatted files are created when you write a configuration file to the hard disk using the **Save**, **Save as**, or **Save and validate** option on the **Configure** pull-down (see Figure 3-18 on page 3-15). The files are stored in configuration databases (file names with the extension *cdb*).

Note: These configuration files must not be changed using a text editor.

- Initial machine load (IML) files

  The IML file format is known to the Multiprotocol Network Program. IML formatted files are created when you write a configuration file to a diskette using the **Create configuration diskette** option on the **Configure** pull-down (see Figure 3-15 on page 3-13), or when you write the file to the hard disk using the **Create configuration on hard disk** option on the **Configure** pull-down.

- ASCII formatted files

  The ASCII file format is useful when you want to view a configuration file online or in hardcopy printout. ASCII formatted files are created when you write a configuration file to the hard disk using one of the **ASCII File** options on the **Configure** pull-down (see Figure 3-19 on page 3-16). For more information about using ASCII files produced by the Configuration Program, read Appendix D on page D-1.

The following sections describe the Configuration Program main window and describe how to create a configuration file using the Configuration Program.

After selecting the 6611 Configuration Program icon, the window shown in Figure 3-13 is displayed.

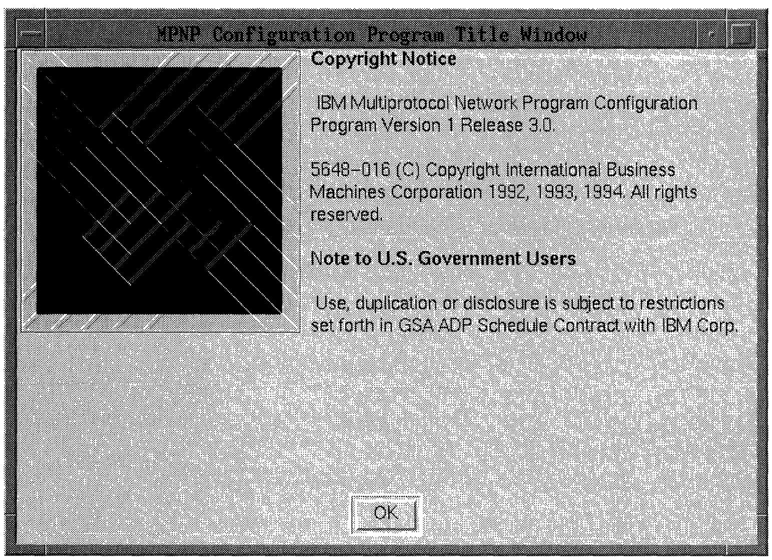


Figure 3-13. MPNP Configuration Program Title Window

Viewing the Main Window

The first window that you see after the copyright window is the main window (MPNP Configuration Program).Figure 3-14 on page 3-12 illustrates the main window.

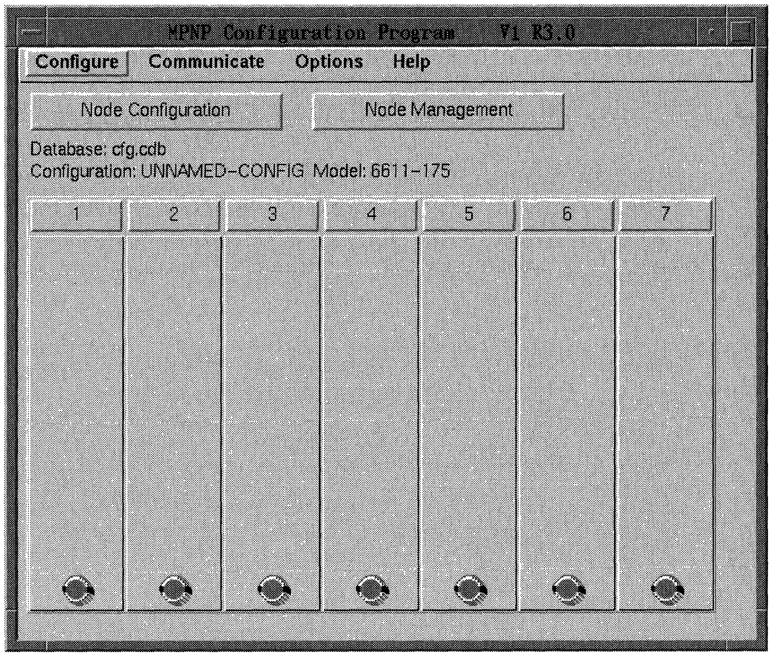


Figure 3-14. Main Window of the MPNP Configuration Program

On the main window, you see:

- The menu bar, which contains the following options:
  - Configure
  - Communicate
  - Options
  - Help
- Seven adapter slots that represent the Model 170.

  The Model 140, which has 4 slots, is the default. You can change the window to display the Model 145, which also has 4 slots, the Model 120 or Model 125, which has 2 slots, or the Model 170 or Model 175, which have 7 slots. (Refer to "Creating a 6611 Configuration File" on page 3-25 for configuration steps.)

Viewing the Menu Bar

The menu bar contains the following options:

- Configure
- Communicate
- Options
- Help

Each of these options includes a pull-down menu that contains tasks you can perform. An arrow displayed to the right of a task on the pull-down menu indicates that another level of choices is available. Use the mouse to select the arrow to display a side menu that contains further items for you to select.

An ellipse (...) displayed to the right of a task on the pull-down menu indicates that another window will appear when you select the task. This window allows you to enter the information necessary to complete the task.

Viewing the Configure Pull-down

Figure 3-15 illustrates the **Configure** pull-down.

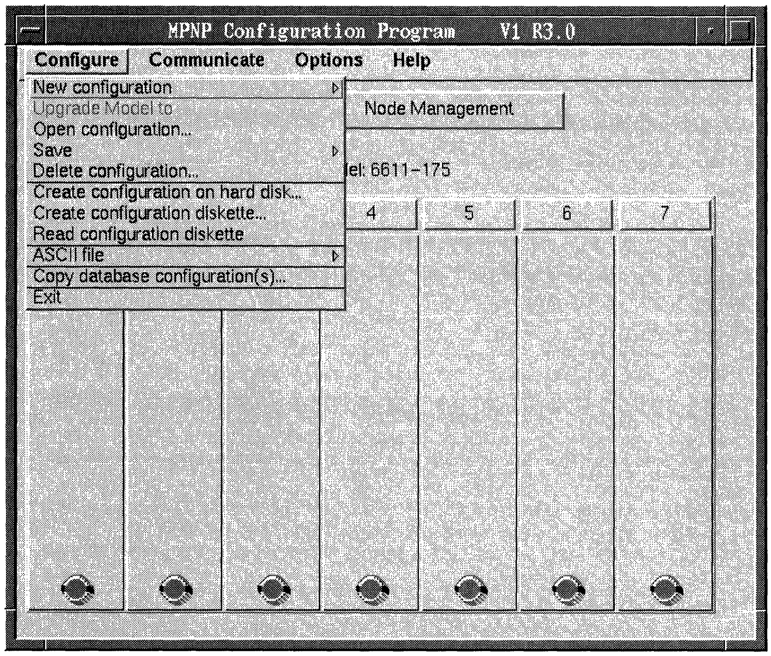


Figure 3-15. Configure Pull-Down on the Menu Bar

The **Configure** pull-down includes tasks that relate to manipulating configuration files from hard disk or diskette.

The **New configuration** option enables you to specify the model of the 6611 you are configuring. The choices are 6611-12x, 6611-140, 6611-145, 6611-170 and 6611-175. Figure 3-16 illustrates the New configuration options.

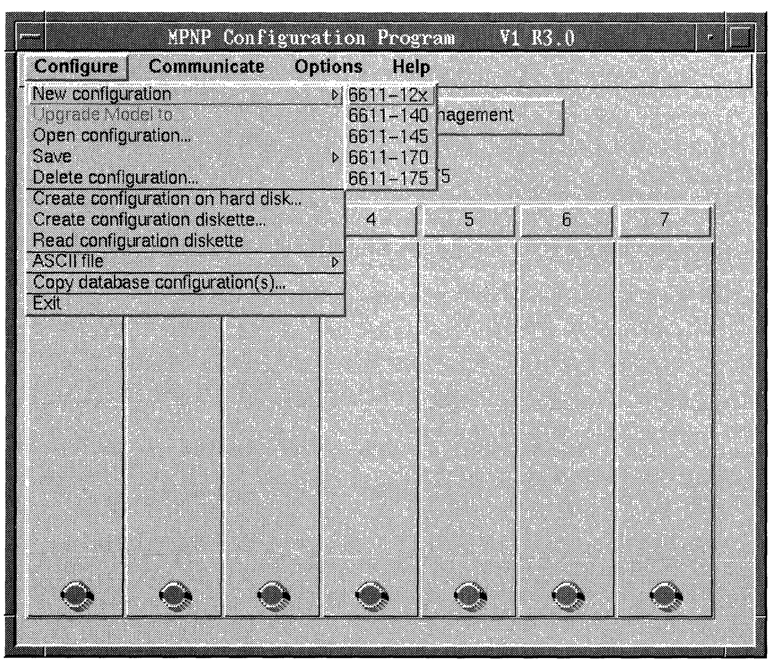


Figure 3-16. New Configuration Option on the Configure Pull-Down

Use the mouse to select the appropriate model of the 6611. The Main window of the Configuration Program is adjusted to illustrate the model you select.

The **Upgrade Model to** option enables you to specify the model of the 6611 to which to you are upgrading the configuration. This option enables you to convert existing configurations to work with the MPNP after you apply a hardware upgrade to the 6611. Table 3-3 illustrates the upgrade possibilities for each model of the 6611.

Table 3-3. 6611 Configuration Upgrade Options

	6611-140	6611-145	6611-170	6611-175
6611-12x	√	√	√	√
6611-140	NA	√[1]	√	√[1]
6611-145		NA	NA	√
6611-170			NA	√[1]
6611-175				NA

Note:

[1] When you upgrade a 6611 Model 170 or Model 120 to Model 145 or Model 175, the following adapters are not supported:

6611 Token-Ring Network 16/4 Adapter
6611 Ethernet Adapter
6611 2-Port EIA 422/449 Serial Adapter
6611 2-Port V.35/V.36 Compatible Serial Adapter

Upgrade these adapters *before* you upgrade the Multiprotocol Network Program and the configuration files for this 6611.

Figure 3-17 illustrates the Upgrade Model to options.

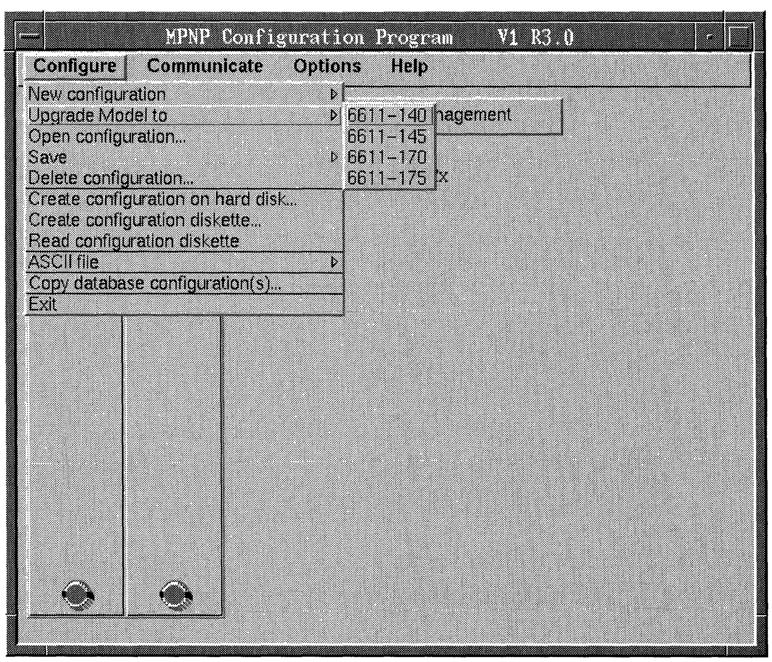


Figure 3-17. Upgrade Model to Option on the Configure Pull-Down

Use the mouse to select the appropriate model of the 6611. The choices are 6611-140, 6611-145, 6611-170, and 6611-175. The Main window of the Configuration Program is adjusted to illustrate the model you select.

The **Open configuration** option enables you to retrieve a configuration that was created and stored in a configuration database during a previous save.

Figure 3-18 illustrates the **Save** options.

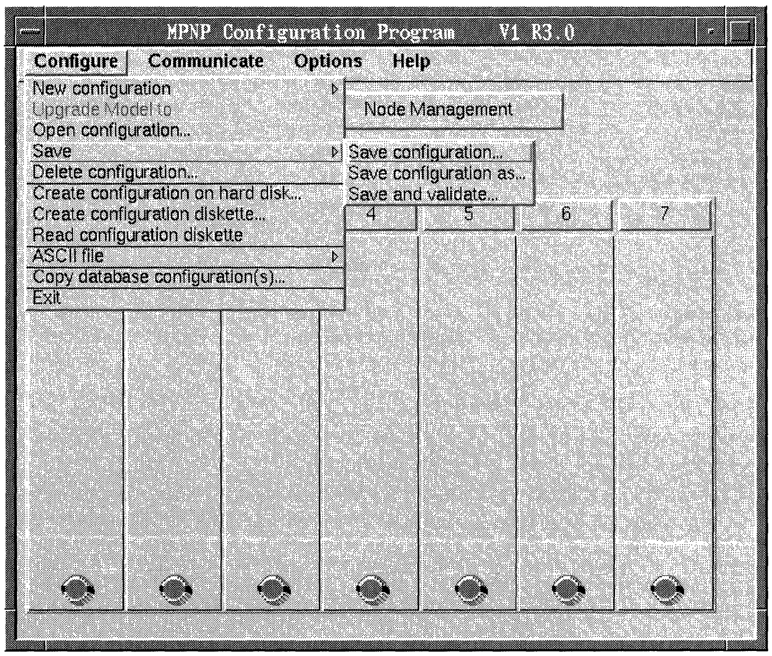


Figure 3-18. Save Option on the Configure Pull-Down

The **Save** option enables you to specify whether to overwrite, rename, or validate the configuration when you save it. These options save the configuration file in a binary format that is internal to the Configuration Program. The following options are available:

- The **Save configuration** option saves the current configuration to a specified configuration database. If the configuration was previously saved, this option overwrites the previous configuration of the same name.
- The **Save configuration as** option enables you to save the current configuration using a different name.
- The **Save and validate** option saves the current configuration and checks to ensure that all required parameters are answered and interdependencies between the ports and between the node and port levels have been satisfied. If required parameters are unanswered, an error message notifies you and the save is not successful. If interdependencies are not met, a warning message or an error message is displayed. When a warning message is displayed, you have the option to cancel or continue saving the file.

The **Delete configuration** option erases the configuration that is currently displayed. If you delete all configurations in a database, the database file is also deleted.

The **Create configuration on hard disk** option saves the current configuration, in the format that is known to the Multiprotocol Network Program, to the hard drive. You can specify the path to which the IML file is saved.

The **Create configuration diskette** option writes the current configuration to diskette as an IML file. An IML file is written in the format that is known to the Multiprotocol Network Program.

The **Read configuration diskette** option reads the configuration from a diskette.

Figure 3-19 illustrates the **ASCII File** options.

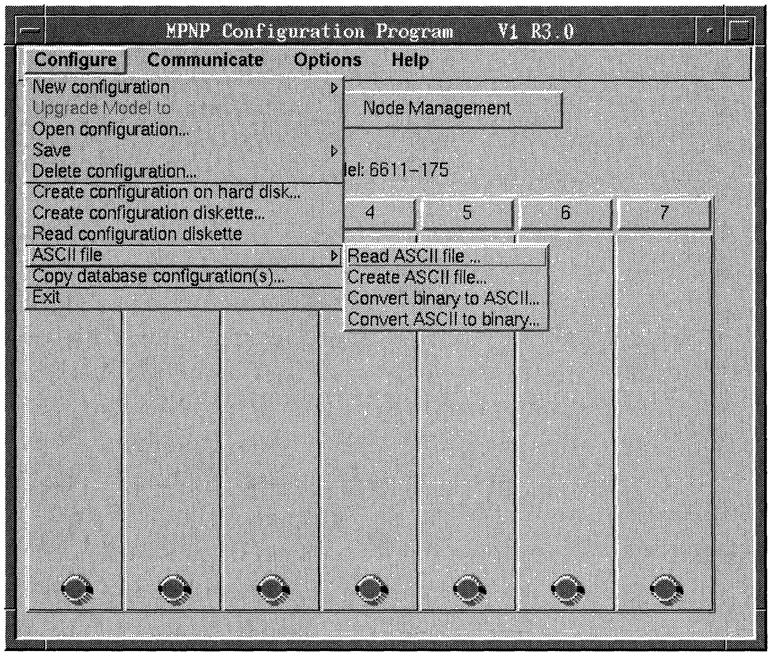


Figure 3-19. ASCII File Option on the Configure Pull-Down

The **ASCII File** option enables you to manipulate ASCII files using the Configuration Program. The following options are available:

- The **Read ASCII file** option reads an ASCII formatted configuration file from the hard drive. You specify the path from which the ASCII file is read.
- The **Create ASCII file** option writes an ASCII formatted configuration file to the hard drive. For more information about interpreting the output produced by this function, read Appendix D on page D-1.
- The **Convert binary to ASCII** option enables you to select one or more binary formatted configuration files from a configuration database, create ASCII formatted files, and save them to the hard drive.
- The **Convert ASCII to binary** option enables you to select one or more ASCII formatted configuration files from the hard drive, create binary formatted configuration files, and save them to a configuration database.

The **Copy database configuration(s)** option enables you to copy configurations from one database into another database. You can also use this option to migrate multiple configuration files. For more information, read "Converting Multiple Configuration Files From a Configuration Database" on page 2-6.

The **Exit** option takes you out of the Configuration Program and prompts you to save the configuration when the configuration has not been saved.

Viewing the Communicate Pull-down

Figure 3-20 illustrates the **Communicate** pull-down.

Note: The **Communicate** pull-down is only available when the Configuration Program is running on an AIX workstation.

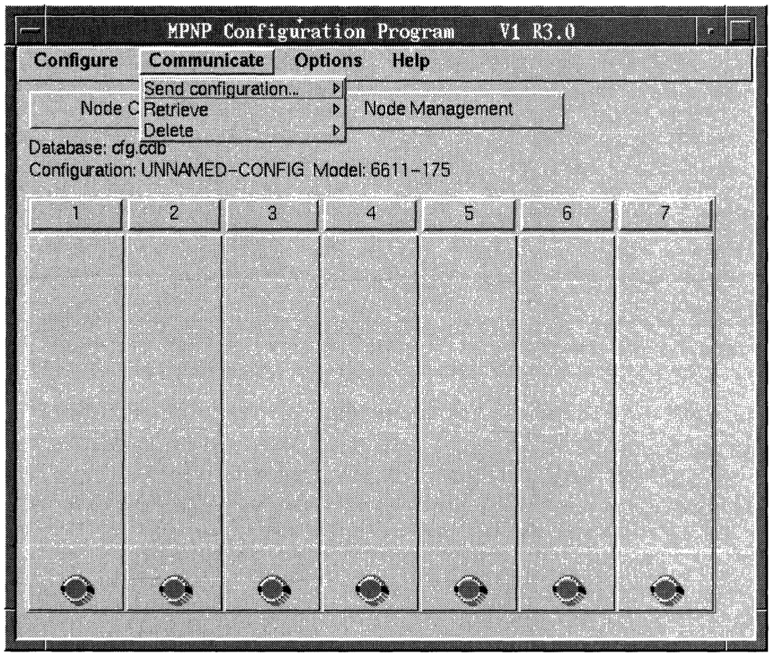


Figure 3-20. Communicate Pull-Down on the Menu Bar

The **Communicate** pull-down includes tasks that relate to sending, retrieving, and deleting configuration files from the 6611.

Figure 3-21 on page 3-18 illustrates the **Send Configuration** options.

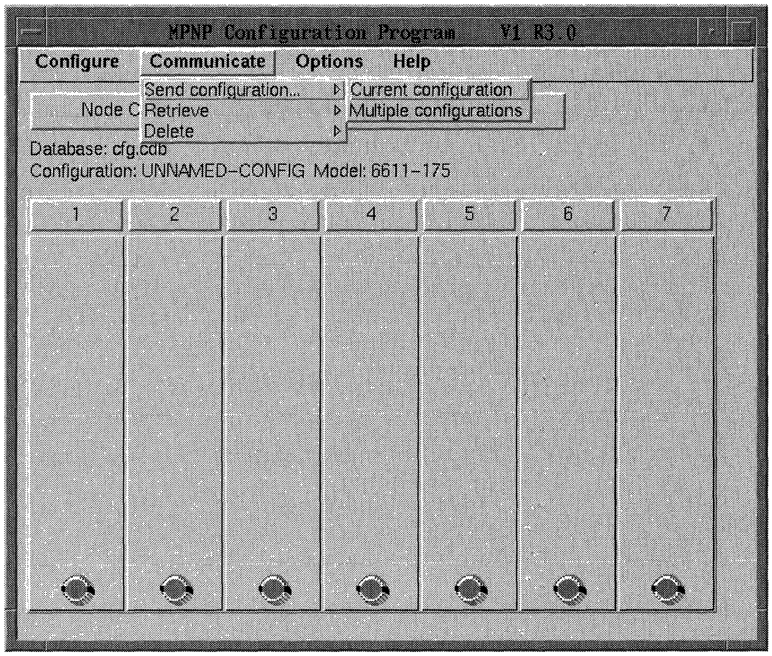


Figure 3-21. Send Configuration Option on the Communicate Pull-Down

The **Send configuration** option enables you to send the configurations from the Configuration Program to a 6611. The following options are available:

- The **Current configuration** option enables you to send the configuration that is currently displayed to a 6611.
- The **Multiple configurations** option enables you to send multiple configurations that are stored in a configuration database to a 6611. For more information, read the instructions for sending multiple configuration files on page 3-30.

For information about scheduling a time to apply configurations sent using these options, read "Specifying a Scheduled Configuration" on page 6-7.

Figure 3-22 on page 3-19 illustrates the **Retrieve** options.

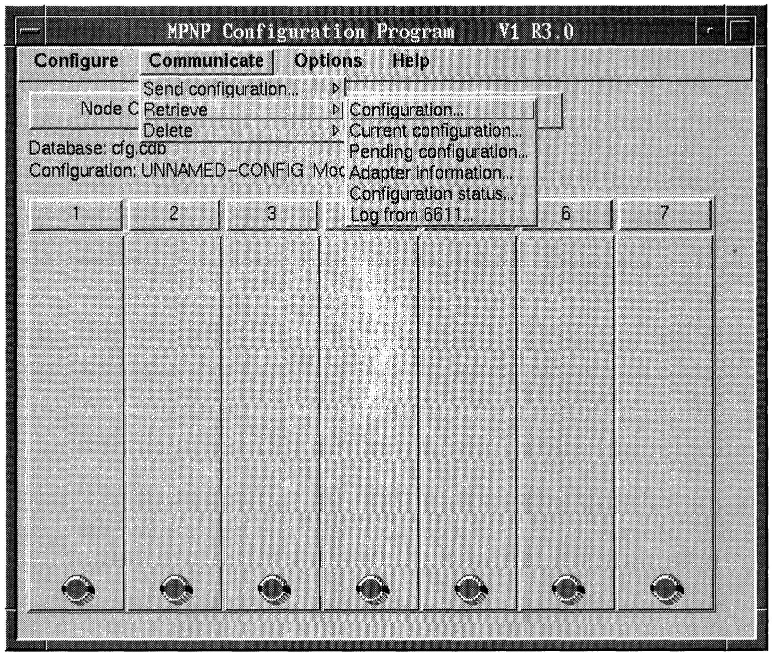


Figure 3-22. Retrieve Option on the Communicate Pull-Down

The **Retrieve** option enables you to specify which information to retrieve from the 6611. The following options are available:

- Retrieve **configuration** enables you to retrieve any configuration that is stored on the 6611. The Retrieve Configuration window contains the IP address of 6611 and Configuration name parameters.
- Retrieve **current configuration** enables you to retrieve the configuration that is currently applied to and running on the 6611. If changes made using System Manager have been applied or committed to the configuration, these changes will be included when you retrieve the current configuration from the 6611.
- Retrieve **pending configuration** enables you to retrieve any configuration that is scheduled to be applied to the 6611. The Retrieve Pending Configuration window contains the IP address of 6611 and Configuration name parameters.
- Retrieve **adapter information** retrieves information about which adapter is installed in each slot of the 6611 and displays it on the main window of the Configuration Program.
- Retrieve **configuration status** retrieves the configuration status log. This log is provided to assist IBM service personnel in diagnosing configuration errors.

  Note: An absence of entries in this log does not necessarily suggest that a protocol is not operating correctly because many protocols do not write information to this log.
- Retrieve **log from 6611** retrieves the configuration process log maintained on the 6611. The log records all actions performed by the configuration process and can be used to diagnose problems with the configuration process on the 6611 at the IP address specified.

Figure 3-23 on page 3-20 illustrates the **Delete** options.

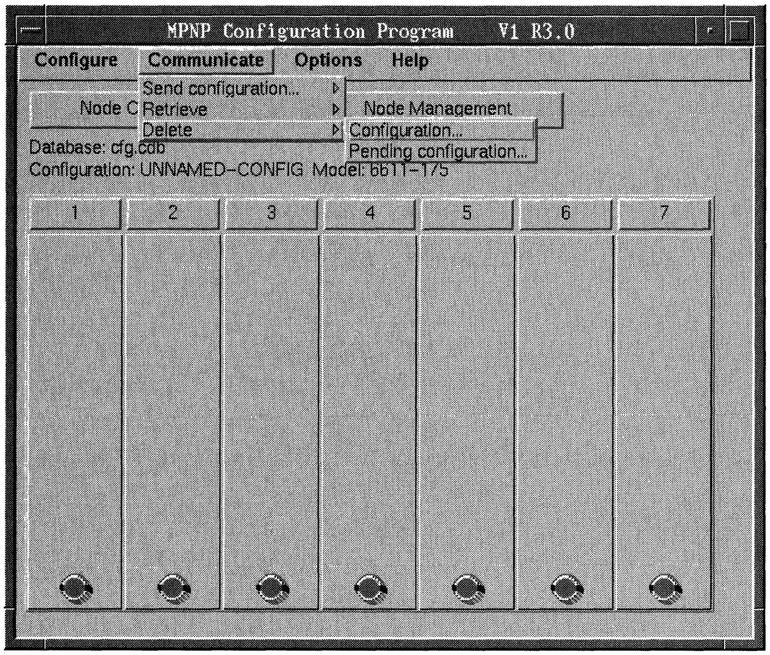


Figure 3-23. Delete Option on the Communicate Pull-Down

The **Delete** option enables you to specify which information to delete from the 6611. The following options are available:

- Delete **configuration** enables you to delete any configuration (including the current configuration) that is stored on the 6611. The Delete Configuration window contains the IP address of 6611 and Configuration name parameters.
- Delete **pending configuration** enables you to delete any configuration that is scheduled to be applied to the 6611. The Delete pending configuration window contains the IP address of 6611 and Configuration name parameters. When you select the List push button, the Configuration Program displays an alphabetical list of the configurations on the specified 6611.

Viewing the Options Pull-down

Figure 3-24 on page 3-21 illustrates the **Options** pull-down.

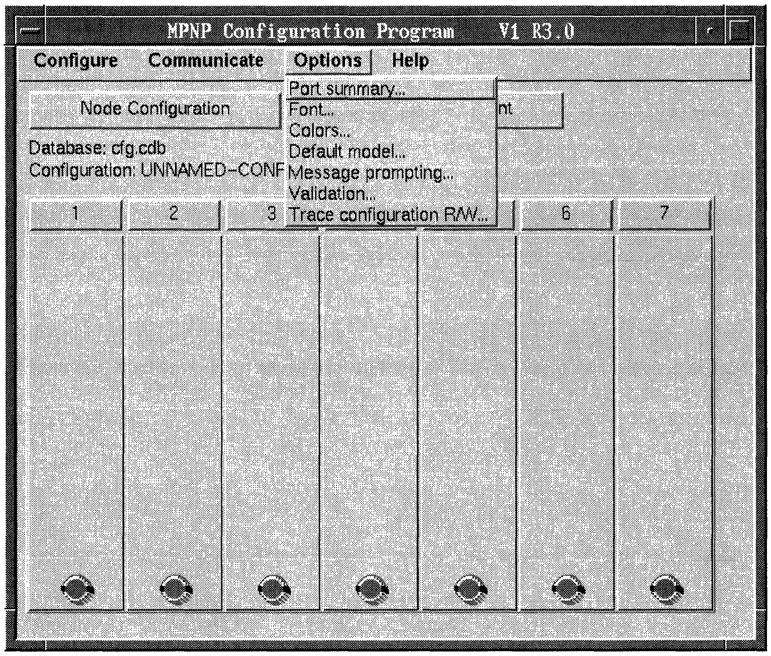


Figure 3-24. Options Pull-Down on the Menu Bar

The **Options** pull-down includes tasks that control features of the Configuration Program. Use the mouse to select the item whose defaults you want to change. The following options are available:

- The **Port summary** option displays a dynamic and visible record of your configuration.
- The **Font** option specifies the size and type of font that the Configuration Program displays.
- The **Colors** option enables you to modify the colors that the Configuration Program displays.
- The **Default model** option specifies which model of the 6611 is displayed when you open the Configuration Program. The choices are Model 12x, Model 140, Model 145, Model 170, and Model 175.
- The **Message prompting** option enables you to customize the priority of warning messages that are displayed by the Configuration Program. You can enable (default) or disable the following levels of warning messages that display if your action will cause:
  - Data loss when you use the Reset push button
  - Data loss when you use the Cancel push button
  - Missing required data
  - Upgrade previous level configuration files
- The **Validation** option enables you to control the validation of configuration files. You can enable or disable (default) whether configuration files are automatically validated before saving when:
  - Copying database configuration(s)
  - Converting ASCII to binary file(s)
- The **Trace configuration R/W** option opens a Configuration Trace window, which displays trace information each time a configuration file is saved or

retrieved. The trace option is provided to assist IBM service personnel in diagnosing configuration errors.

Viewing the Help Pull-down

Figure 3-25 illustrates the **Help** pull-down.

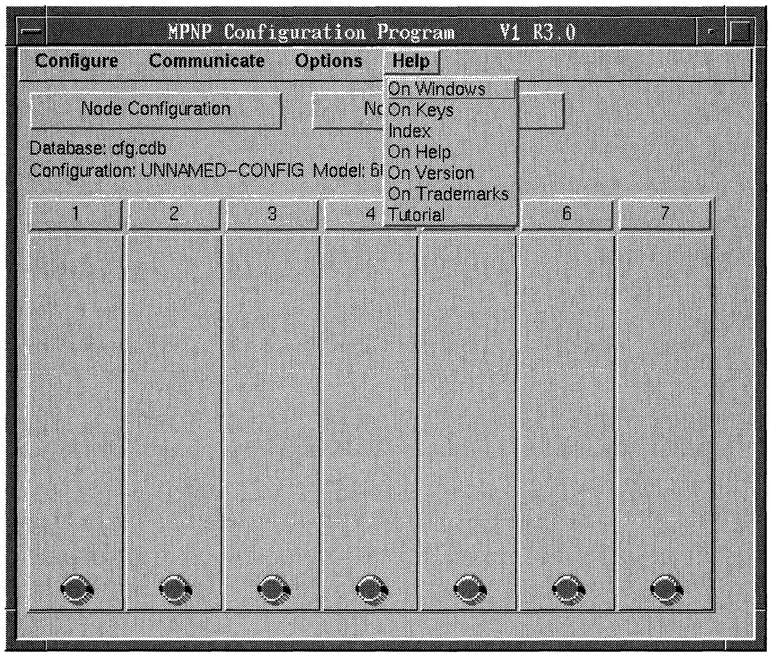


Figure 3-25. Help Pull-Down on the Menu Bar

The **Help** pull-down enables you to get help for the Configuration Program, display an index of help topics, or access the tutorial. The following options are available:

- The Help **On Windows** option displays a help that explains the options that are available on the Configuration Program main window.
- The Help **On Keys** option displays a help that explains the functions of the buttons that appear at the bottom of windows, their keyboard equivalents, and the function keys that are supported by the Configuration Program.
- The **Index** option displays a list of general help topics for adapters, protocols, and networking concepts.
- The Help **On Help** option displays a window that explains how to access general and specific help information.
- The Help **On Version** option displays a window that contains the copyright notice for the Configuration Program, the version number, and the notice to government users of licensed programs.
- The Help **On Trademarks** option displays a window that provides a list of the trademarks (held by IBM and other companies) that appear in the Configuration Program.
- The **Tutorial** option accesses the tutorial that explains how the Configuration Program works and how you can use it.

Viewing the Adapter Slots

The adapters slots contain the options shown in Figure 3-26.

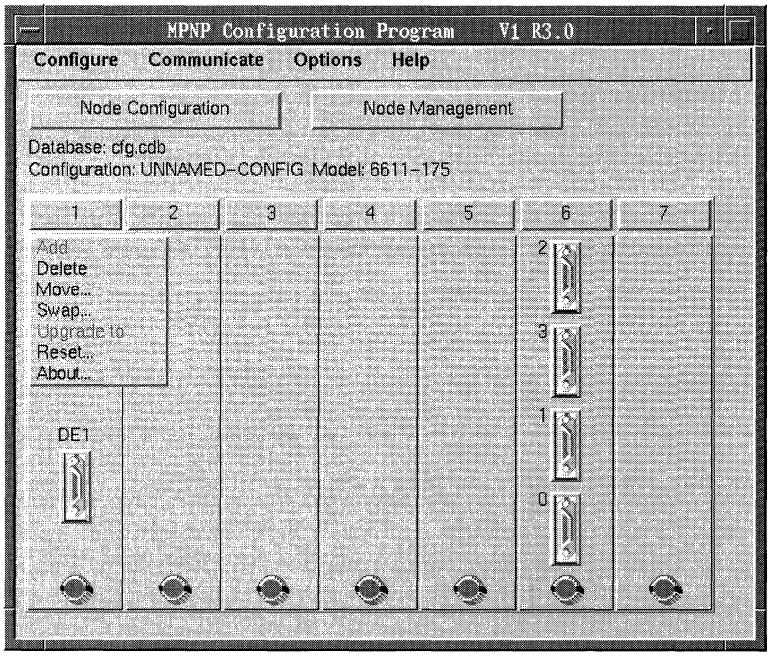


Figure 3-26. Adapter Slot Options

The **Add** option enables you to add an adapter to this slot. Figure 3-27 on page 3-24 illustrates the Add options.

The **Delete** option enables you to remove an adapter from this slot. When you remove an adapter, the configuration for this slot is lost and node level configuration questions that reference IP addresses on this slot are changed to delete references to this slot.

The **Move...** option enables you to move this adapter and its configuration to another slot. When you select this option, a window that displays the possible destination slots appears. When you select **OK**, this adapter and its configuration are moved to the destination slot.

The **Swap...** option enables you to exchange the position of two adapters. When you select this option, a window that displays the possible destination slots appears. When you select **OK**, this adapter and its configuration are moved to the destination slot, and the adapter in the destination slot (along with its configuration) are moved to this slot.

The **Upgrade to** option enables you to upgrade the configuration of an existing adapter when you replace it with a new adapter, such as a combination or multiport adapter.

The **Reset...** option enables you to reset the configuration parameters on one or more ports on this adapter to the default values. When you select this option, a window that enables you to select the ports to reset is displayed.

The **About...** option provides the full name of the adapter in this slot. This option is not available when no adapter is configured for this slot.

Figure 3-27 on page 3-24 illustrates the **Add** options.

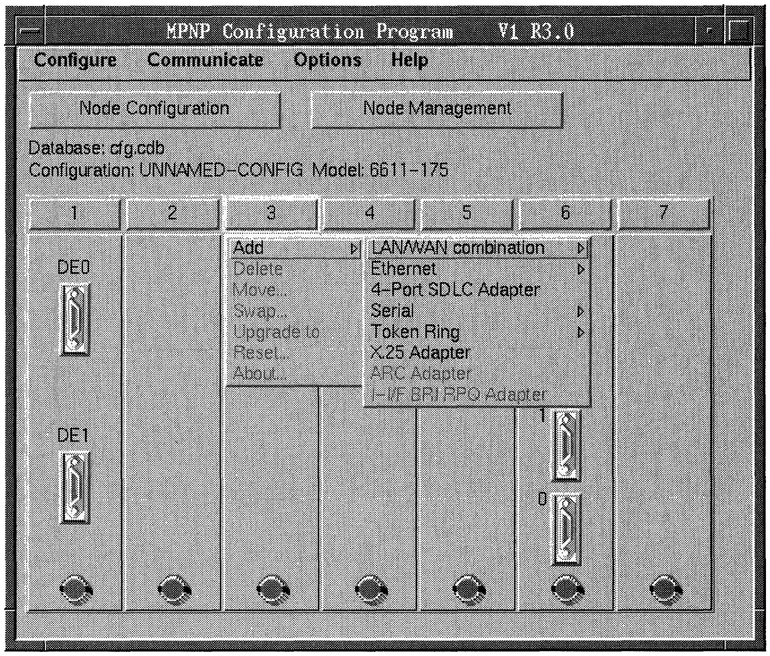


Figure 3-27. The Add Options

The **LAN/WAN combination** option enables you to add to this slot one of the following adapters:

- Multi-Interface Serial/Ethernet Combination Adapter, which contains two serial ports and one Ethernet port.
- Multi-Interface Serial/Token-Ring Combination Adapter, which contains two serial ports and one token-ring port.

The **Ethernet** option enables you to add to this slot one of the following adapters:

- Ethernet Adapter
- 1-Port Ethernet Adapter
- 2-Port Ethernet Adapter

The **4-Port SDLC Adapter** option enables you to add a 4-port SDLC adapter to this port.

The **Serial** option enables you the add to this port one of the following adapters:

- 2-Port Serial Adapter
- 2-Port Multi-Interface Serial Adapter
- 4-Port Multi-Interface Serial Adapter

The **Token Ring** option enables you to add to this port one of the following adapters:

- Token-Ring Network 16/4 Adapter
- 1-Port Token-Ring Network 16/4 Adapter
- 2-Port Token-Ring Network 16/4 Adapter

The **X.25 Adapter** option enables you to add an X.25 adapter to this slot.

The **ARC Adapter** option enables you to add an ARC adapter to this slot when you have applied PRPQ 85251 (IBM 6611ARC) and RPQ 8Q0951 (8-port asynchronous adapter EIA 232) to this 6611. The option is available for Models 140 and 170 only. You must also enable the Enable ARC parameter on the RPQ Configuration window at the node level.

The **I-I/F BRI RPQ Adapter** option enables you to add an ISDN adapter to this slot when you have applied the appropriate PRPQ and RPQ to this 6611 (see Table 3-4). You must also enable the Enable I-I/F BRI parameter on the RPQ Configuration window at the node level.

Table 3-4. I-I/F BRI Adapter RPQ and PRPQ Chart

6611 Model	RPQ	PRPQ
6611-120 1 Token-Ring and 1 I-I/F BRI RPQ adapter	8Q1300 8Q1437	P85400
6611-120 1 Ethernet and 1 I-I/F BRI RPQ adapter	8Q1301 8Q1437	P85400
6611-140	8Q1302	P85401
6611-170	8Q1302	P85402

Note: The I-I/F BRI RPQ adapter is available only for Models 120, 140, and 170.

These PRPQs make available software that enables the 6611 to provide the I-interface basic rate interface (BRI) function in Japan. These RPQs make available the two-port adapter and the associated hardware that provides direct connection from the 6611 to the Nippon Telegraph and Telephone (NTT) Corporation HSDS BRI leased line without an interface converter or a terminal adapter.

Note: On the RPQ Configuration window, you can also enable switched multi-megabit data service (SMDS) to be configured on serial ports on the 6611. PRPQ P85417 must be applied to the 6611 to enable this function. For more information, see the *Introduction and Planning Guide* or contact your IBM service representative.

Creating a 6611 Configuration File

Follow these steps to create a configuration file for a 6611:

Step 1 At the main window, verify that the correct model of the 6611 is displayed. If you want to configure a Model 120 or Model 125 (2 slots), or Model 170 or Model 175(7 slots), but a Model 140 or Model 145 (4 slots) is displayed, follow these steps:

1. Select **Configure** from the menu bar.
2. Select **New configuration** from the pull-down menu.
3. Select **6611-12x**, **6611-140**, **6611-145**, **6611-170**, or **6611-175** from the pull-down menu.

Step 2 Optionally configure the Node Management parameters, or accept the default values. To configure the parameters, select **Node Management** to specify the:

- Host name and domain name for the 6611
- Baud rate for the S1 and S2 serial ports

- Lock value of the MPNP
- SNMP network management information
- Controlling and viewing user IDs and passwords for the 6611
- Time when a configuration file is to be applied to the system
- Automatic configuration rollback information
- List of hosts that can configure the 6611 from the Configuration Program
- Mapping of host names to IP addresses
- Name and time servers on the network that you want the 6611 to use

Figure 3-28 illustrates the Node Management window.

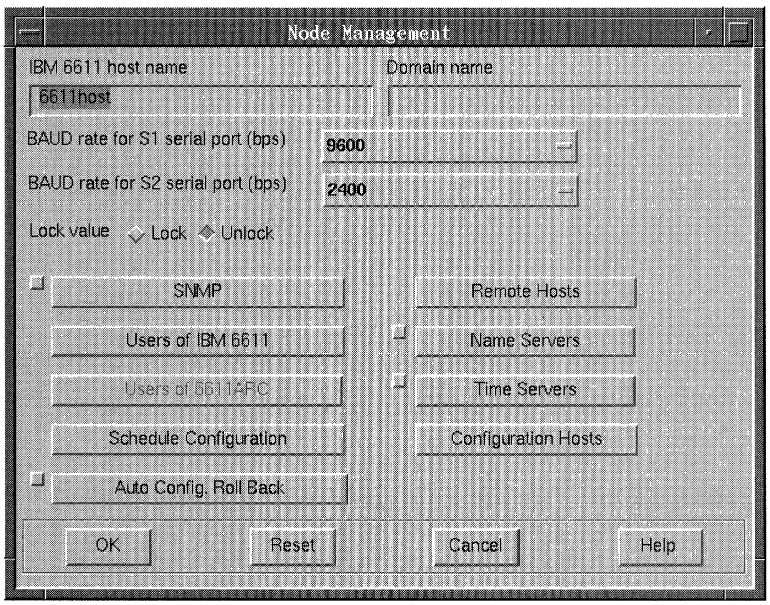


Figure 3-28. Node Management Window

Step 3 Configure the adapter slots. Select an adapter slot by clicking on the numbered push button that corresponds to the slot that you want to configure. (You cannot select the physical slot.) A pop-up menu that allows you to add an adapter appears. The other actions (delete, move, swap, upgrade to, reset and about) cannot be selected when the adapter slot is empty.

Warning: You must use the Configuration Program to add each adapter that is installed in your 6611 to the configuration. The 6611 will not load correctly if you do not add all installed adapters.

To enable an adapter, select **Add**. A pull-down menu appears. Click on the name of the adapter you want to add from the pull-down menu. You can add the following adapters:

- LAN/WAN combination
  - Multi-Interface Serial/Ethernet Combination Adapter, which contains two serial ports and one Ethernet port.

    - Multi-Interface Serial/Token-Ring Combination Adapter, which contains two serial ports and one token-ring port.
- Ethernet
    - Ethernet Adapter
    - 1-Port Ethernet Adapter
    - 2-Port Ethernet Adapter
- 4-Port SDLC Adapter
- Serial
    - 2-Port Serial Adapter
    - 2-Port Multi-Interface Serial Adapter
    - 2-Port Multi-Interface Serial Adapter
- Token Ring
    - Token-Ring Network 16/4 Adapter
    - 1-Port Token-Ring Network 16/4 Adapter
    - 2-Port Token-Ring Network 16/4 Adapter
- X.25 Adapter
- ARC Adapter
- I-I/F BRI RPQ Adapter

Step 4 Configure the adapter ports. When configuring multiport adapters, such as the LAN/WAN combination adapters, the serial adapters, and the SDLC adapter, you must configure each port that will be used.

To configure a port, select the port by clicking on the port push button. The port-level parameters window appears with a number of selections. If the window that appears has the Physical Interface push button, select the **Physical Interface** push button to configure the adapter parameters. Proceed to configure the port-level parameters for the adapter port. Repeat this step for each port that will be used. Figure 3-29 illustrates the port-level parameters window for a token-ring adapter.

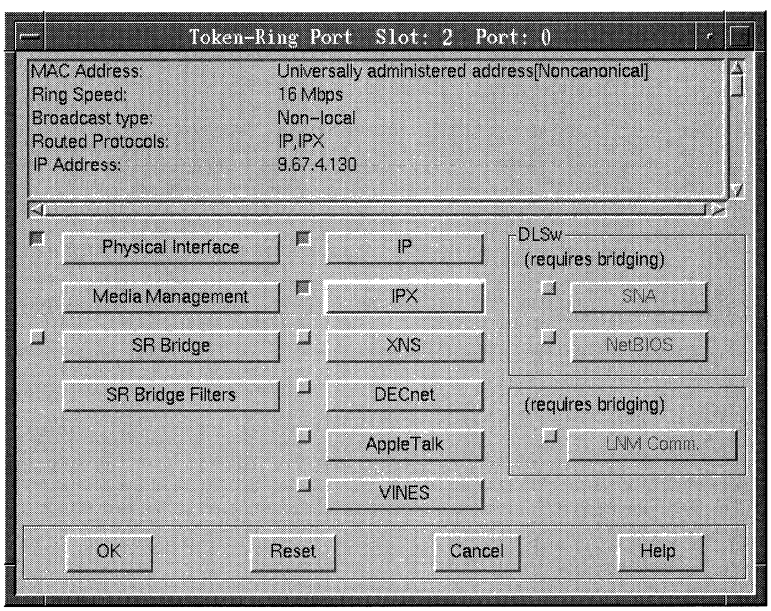


Figure 3-29. Token-Ring Adapter Port Parameters Window

Step 5 To display the Port Summary window:

Step 1 Select **Options** from the MPNP Configuration Program main window menu bar.

Step 2 Select **Port Summary** from the pull-down menu.

The Port Summary window displays current configuration information about the adapters and protocols for each adapter slot. This window continually displays the current configuration of the adapters and protocols as you continue the configuration process. Figure 3-30 illustrates the Port Summary window.

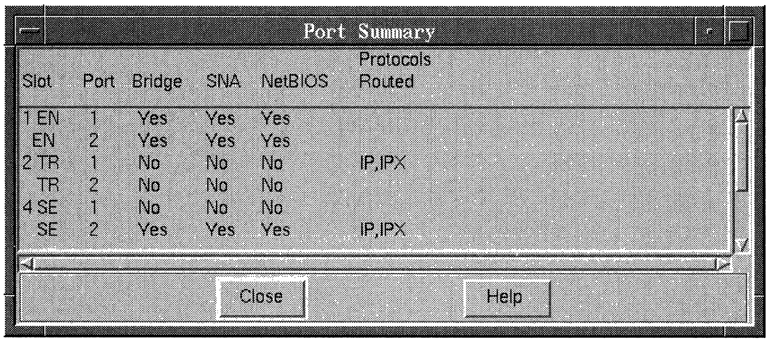


Figure 3-30. Port Summary Window

Step 6 Select **Node Configuration** to configure the routing, bridging, and data link switching functions that you want the 6611 to perform. Figure 3-31 illustrates the Node Configuration window.

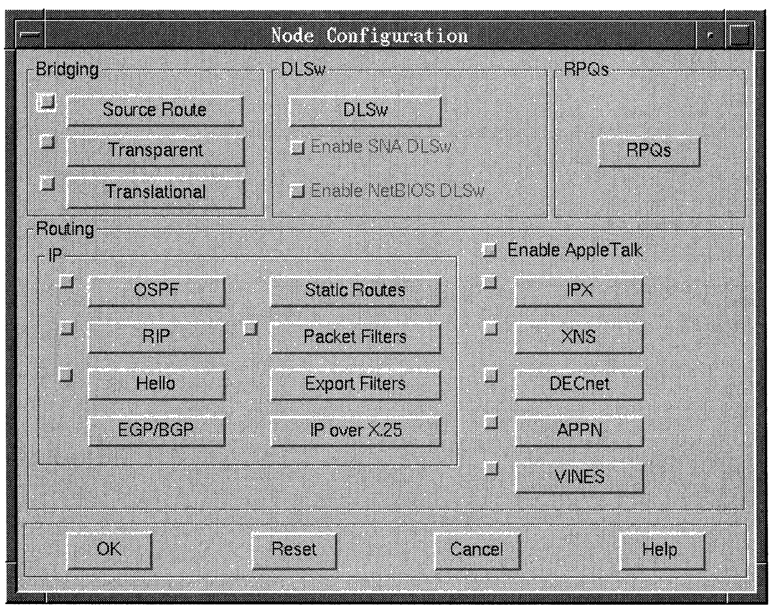


Figure 3-31. Node Configuration Window

Step 7 After you have configured all of the functions and protocols that you want enabled for the 6611, save the configuration file. At the MPNP Configuration Program main window (Figure 3-14 on page 3-12), select **Configure** and then select the **Save**. You can select the **Save configuration ...**, **Save configuration as ...**, or **Save and validate ...** option to save the file.

Continue with "Transporting the Configuration File to the 6611" for instructions on how to transport the file.

Transporting the Configuration File to the 6611

After you have created a configuration file using the Configuration Program, you must transport the file to the 6611. You may transport the file using a diskette or using a network connection to the 6611.

Note: The preferred method to transport the initial configuration is to carry the diskette to the 6611 and place it the diskette drive. Then, turn the power switch to **On** (I). See "Transporting the File Using a Diskette" for more instructions.

Transporting the File Using a Diskette

After you have created a configuration file using the Configuration Program, you can transport the file to the 6611 using a diskette. Follow these steps to create a configuration diskette and load the diskette on the 6611:

1. Select **Configure** from the menu bar of the Configuration Program main window.
2. Select **Create configuration diskette** from the pull-down menu. Enter the information that the program needs to copy the file to the desired drive.
3. Carry the configuration diskette to the 6611 and place it in the diskette drive.
4. To read the configuration file, set the 6611 key mode switch to **Normal** and then set the power switch to **On** (I).

   The configuration process installs the configuration parameters and uses those parameters as the current configuration.
5. Observe the 3-digit display while the configuration process reads the file. See *IBM 6611 Network Processor Maintenance Information* for an explanation about the codes that are displayed. When the configuration process has read the file and initialized the 6611 and its adapters, the code `c66` is displayed on the 3-digit display.
6. After the configuration process has completed, remove the diskette from the drive.

   Note: The diskette drive will be read when a power-on reset (POR) occurs.

   Warning: You must remove the diskette to prevent the diskette from being read accidentally during a subsequent configuration of the 6611. Removing the diskette also prevents accidentally overwriting the configuration file on the diskette.

Transporting the File without Using a Diskette

After you have created a configuration file using the Configuration Program, you may use one of these three methods to transport the file over a network connection to the 6611:

- Direct IP connection
- Modem transfer method
- File Transfer Protocol (FTP) transfer method

Direct IP Connection

You can send a file directly from the Configuration Program workstation to a 6611 provided that:

- The workstation is a RISC System/6000 workstation which has a network connection to the 6611 and the 6611 is active on the network.
- A minimal initial configuration has been installed on the IBM 6611. See "Initial Configuration without Using a Diskette" on page 7-2 for instructions about how to perform a minimal configuration.

Notes:

1. To use the Send configuration function, configure all the adapters that are in the 6611. If there are adapters in your 6611 that you do not want to use, you must still define them in the configuration. After defining these adapters in the configuration, access the adapter port configuration for the adapters that you do not want to use (see Figure 3-29 on page 3-27 for an illustration of the Token-Ring Adapter Port Parameters window). Disable the Enable physical interface parameter, which defaults to enable for all port types except SDLC.
2. Use the **Save and validate** option on the Configure pull-down (see Figure 3-18 on page 3-15) to validate the file before you use the Send configuration function. If you attempt to send a configuration file that has not been validated, an error message is displayed and the file is not sent.

Use the following procedures to send one or more configuration files from the RISC System/6000 workstation to one or more 6611s.

To send a single configuration file to a single 6611:

1. Select **Communicate** from the menu bar of the MPNP Configuration Program main window.
2. Select **Send configuration...** from the pull-down menu and then select the **current configuration** option. The Send Configuration window appears. Enter the IP address of the destination 6611 and the name of the configuration that is currently displayed and then select **OK** to send the file to the 6611.

   The 6611 will automatically process the configuration file upon receipt *unless* you modify the configuration file to change the time at which the configuration is applied. For more information, read "Specifying a Scheduled Configuration" on page 6-7.

To send multiple configuration files to multiple 6611s:

1. Select **Communicate** from the menu bar of the MPNP Configuration Program main window.
2. Select **Send configuration...** from the pull-down menu and then select **multiple configurations** option. The Send Multiple Configurations window appears.
   a. Use the Send list path parameter to specify the path to the directory where the configuration databases (**.cdb*) that contain the configuration files are stored. The Send lists you create have the extension *.mdb* and must be stored in the same directory as the configuration databases specified in the Send lists.

b. Use the Send list name parameter to create a list of configuration files to send to multiple 6611s. Each send list contains multiple entries that enable you to send multiple configurations to multiple 6611s, but only one configuration to each 6611. Each entry in the send list contains the name of the configuration to be sent, the name of the configuration database that contains that configuration, and the IP address of the destination 6611.

   To create a Send list, enter an 8 character alphanumeric Send list name and select the **Add/Insert** push button. The Add to Send List window appears. You can use the Copy List push button to copy a send list that you want to modify, or use the Delete List push button to remove a send list from the list of Send lists.

   To add an entry to the Send list, access the Add to Send List window and select the database name from the Databases list. The configuration files contained in that configuration database are displayed in the Configurations list. Select each configuration to add to the Send list. Then use the Router IP destination parameter to specify the IP address of the destination 6611 and select the **Apply** push button. The Send list name is added to the list of Send lists. Use the Reset push button to retain the same configuration database but clear the configuration to enable you to add another configuration to the Send list. Use the Clear push button to clear all information that you have added or selected, and use the Close push button to return to the preceding window.

   Repeat the preceding step to add entries to the Send list. Select a Send list and use the Edit push button to change an entry in the Send list, or use the Delete push button to remove an entry from the Send list.

c. Use the Override reboot parameters to specify whether the destination 6611 applies the configuration files upon receipt and possibly reboots, or whether it applies the configuration files at a specified time.

   When the Enable override reboot parameter is disabled, each destination 6611 automatically processes the configuration file according to the value of the Apply configuration parameter for each configuration file (the default is to apply the configuration immediately). For more information, read "Specifying a Scheduled Configuration" on page 6-7. To override the value of the Apply configuration parameter and specify the time at which each 6611 applies the specified configuration file, select the **Override Reboot Parameters** push button. Specify the reboot type (synchronized or serialized[1]) and use the Apply configuration parameter to specify the time at which the configuration files are applied. Then select **OK**.

d. Determine whether to enable or disable the Stop on send error parameter (the default is Disable). For more information about this parameter, access the online help.

e. Select **OK** to send the specified configuration files to the destination 6611s.

---

[1] Select **Synchronized reboot** when you want all 6611s to which you are sending configurations to perform initial program load (IPL) at the same time. Use the Apply configuration parameter to specify when the configurations are applied and the 6611s perform IPL.

Select **Serialized reboot** when you want the IPL of the 6611s to occur at scheduled intervals. Use the Year, Month, Day, Hour, and Minute parameters set the time at which the first configuration in the Send list is applied to the 6611, which performs IPL. Use the Time delay minutes parameter to specify the length of time between the application configuration files to each 6611 on the Send list.

Modem Transfer Method

You can send a configuration file from a remote workstation to a 6611 using a modem connection if the workstation:

- Is connected using a modem to the 6611 through one of its EIA 232 serial ports.

  The workstation can be connected using a modem to another node on the same network as the 6611 provided that the other node supports remote login (**rlogin**) and has a network connection to the 6611. The 6611 must be active on the network.

- Supports outgoing calls and the Xmodem Protocol.

See "Modem Attachment" on page 7-2 for instructions about how to send a configuration file using this method.

FTP Transfer Method

You can send a configuration file from a remote workstation to a 6611 using FTP over an IP network. The following conditions must be met:

- For initial configuration, a minimal configuration must be installed on the 6611 and the 6611 is active on the IP network. See "Initial Configuration without Using a Diskette" on page 7-2 for instructions about how to perform a minimal configuration.
- The workstation is active on the IP network and supports FTP.

See "FTP Transfer Method" on page 7-4 for instructions about how to send a configuration file using this method.

Chapter 4. Configuring Ports and Framing Methods

This section provides information about the ports available on adapters supported by the 6611. Remember to configure node management, then ports, then protocols, then node configuration for all routing and bridging configurations except DECnet. For DECnet configurations, configure node management first, then node configuration, and then configure ports and protocols.

Warning: You must use the Configuration Program to add each adapter that is installed in your 6611 to the configuration. The 6611 will not load correctly if you do not add all installed adapters.

Each port or framing method description contains the following information:

Restrictions This section lists restrictions for configuring the port or framing method.

Configuration Changes Some of the IBM 6611 configuration parameters can be changed dynamically and do not require a machine restart. This section lists the changes that:

- Require the specific function to restart
- Require the 6611 to restart

Compatible Protocols This section lists the protocols that this port or framing method supports for routing, local bridging (in which the 6611 acts as a single bridge to connect multiple LAN segments without using a telecommunications link), and remote bridging (in which two 6611s act as bridges to connect multiple LANs across a telecommunications link).

Worksheet This section contains worksheets to be used when configuring the port or framing method. *The values on each worksheet correspond to the values displayed on the window of the Configuration Program that is identified by the title of the worksheet.*

Where applicable, each port or framing method description also contains the following information:

Configuration Options This table lists the steps for creating a basic configuration for this port or framing method, and lists additional configuration options.

Configuration Verification Checklist This checklist helps you verify that two 6611s are correctly configured to perform bridging or routing over the port or framing method.

Sample Network Graphic This section includes an illustration of a sample network.

Summary of All Customized Parameters in Sample This section includes tables that show the values that you configure to enable the protocols to run on the sample network. A value of NA indicates that a parameter is not applicable to the configuration.

Serial Port and V.35/V.36 Serial Port

The Serial Port and V.35/V.36 Serial Port (referred to collectively in this section as *serial ports*) provide an interface between the 6611 and a data service unit/channel service unit (DSU/CSU) or high-speed serial converter.

The serial port is available on the following multiport adapters:

- 6611 2-Port EIA 422/449 Serial Adapter
- 6611 Model 120 2-Port EIA 422/449 Serial Adapter
- 6611 2-Port V.35/V.36 Compatible Serial Adapter
- 6611-A25 2-Port Multi-Interface Serial Adapter
- 6611-A47 2-Port Multi-Interface Serial Adapter
- 6611-A25 4-Port Multi-Interface Serial Adapter
- 6611-A47 4-Port Multi-Interface Serial Adapter
- 6611-A25 Multi-Interface Serial/Token-Ring Combination Adapter
- 6611-A47 Multi-Interface Serial/Token-Ring Combination Adapter
- 6611-A25 Multi-Interface Serial/Ethernet Combination Adapter
- 6611-A47 Multi-Interface Serial/Ethernet Combination Adapter

Each port is capable of operating at speeds of 9 600 bps to 2 048 000 bps.

Support for IP transmission groups and queue priority is available only on the serial port. *Queue priority* enables you to specify the number of packets that will be allowed to flow from the high, medium, and low priority bandwidth allocation queues. Using queue priority options, you can control the serial port buffer space that can be allocated for each queue in case of buffer pool saturation. For more information about the queue priority parameters, see Table 4-2 on page 4-5 or access the online help provided in the Configuration Program. For more information about transmission groups, read "Transmission Groups" on page 5-106.

You must configure the Data encoding parameter (NRZ, NRZI) when you want to use these ports for PPP and frame relay. Data encoding must match the encoding used by other routers on the network. When you use these ports for LAN Bridging Protocol, the Data encoding parameters is not selectable; it is always set to **NRZI**.

To configure a serial port, you must first select the Data link protocol (PPP, Frame Relay, LAN Bridging Protocol). Then configure the serial port parameters and the protocols that you want the adapter to transmit and receive.

Restrictions

When you define transmission groups on the serial port, the transmission group name must be unique on the 6611.

Configuration Changes ...

That Require the Function to Restart

None

That Require the 6611 to Restart

- Cylink serial number
- Data encoding
- Data link protocol
- Enable physical interface on this port
- Interface cable
- Locally administered MAC address
- Serial line speed
- Transmit clock source

Compatible Protocols

The 6611 supports local and remote bridging of all network protocols. See "Frame Relay" on page 4-6, "LAN Bridging Protocol" on page 4-17, and "Point-to-Point Protocol (PPP)" on page 4-27 for information about which protocols each framing method supports.

Worksheets

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-30 on page D-22 for a mapping of parameter names and their associated labels.

Use the following tables as worksheets for your serial adapter configurations.

- Serial Port - Physical Interface on page 4-3
- Change Queue Priority on page 4-5
- LNM Communication on page 4-5

Table 4-1 (Page 1 of 2). Configuration Worksheet - Serial Port - Physical Interface

Parameter Information		Your Value
Parameter	Enable physical interface on this port	
Valid Values	Enable, Disable	
Default	Enable	
Description	This parameter enables or disables one of the ports on a multiport serial adapter.	
Parameter	Interface cable (available only on A25 and A47 adapters)	
Valid Values	EIA 422 or X.21; V.35, V.36, or EIA 232	
Default	EIA 422 or X.21	
Description	This parameter specifies the type of interface cables for the serial port.	
Parameter	Cylink serial number	
Valid Values	00 000 000 to 99 999 999	
Default	None	
Description	This parameter specifies the serial number of the data service unit/channel service unit (DSU/CSU) connected to this serial port.	
Parameter	Transmit clock source (available only on A25 and A47 adapters)	
Valid Values	DTE, DCE[1]	
Default	DTE	
Description	This parameter specifies how the transmit clock source transmits data.	

Table 4-1 (Page 2 of 2). Configuration Worksheet - Serial Port - Physical Interface

Parameter Information	Your Value
Parameter Serial line speed **Valid Values** 9600 to 2048000 bps **Default** 19200 bps **Description** Set the serial line speed parameter to the clock rate provided by an external clocking source, such as a modem. This parameter does not change the actual clocking rate or line speed but will affect the metric value that is used to determine the cost of the route. When you use a network management station to view the the ifSpeed variable in the MIB II interface, this parameter provides the value that is displayed. **Note:** LAN Bridging Protocol uses the value of this parameter to determine the default telecommunications link error threshold.	
Parameter Data encoding **Valid Values** NRZI, NRZ **Default** NRZI **Description** This parameter specifies how the line transition occurs on the serial link attached to this serial port. NRZI is a common setting for modems. This setting indicates that a line transition occurs for each zero bit (the transition occurs at the start of the data bit cell). A 1 is represented by a continuous level. To keep from losing clock synchronization, you should use a stream of zeros. When you select NRZ, the data line reflects ones and zeros by level. If the data is 1 for several consecutive bits, the level of the line remains a constant 1. To keep from losing clock synchronization, you should use a stream of alternating ones and zeros.	
Parameter Locally administered MAC address **Valid Values** X'0000 0000 0000' to X'FFFF FFFF FFFE' **Default** None **Description** This parameter specifies the locally administered MAC address assigned to the adapter attached to this port. This MAC address is the node addressed for this port and is used: • To make routing decisions for IPX and XNS. • When the 6611 is configured as a bridge but no LAN ports are enabled for bridging. The 6611 requires at least one port MAC address to generate a bridge identifier for the bridge. • When the 6611 is configured as a translational bridge and source route bridging is enabled on a serial port. The MAC address is required in this case to provide a source address for BPDUs transmitted on the port.	
Parameter Enable port for transmission group **Valid Values** Enable, Disable **Default** Disable **Description** This parameter allows you to enable or disable 2 T1 in a transmission group (2T1-TG) on this port.	
Parameter Transmission group name **Valid Values** 1 to 8 characters, A to Z, 0 to 9 **Default** None **Description** This parameter specifies a TG name. Each TG name on the 6611 must be unique.	

Table 4-2. Configuration Worksheet - Change Queue Priority

Parameter Information		**Your Value**
Parameter	Link bandwidth allocation for high priority queue	
Valid Values	1 to 10	
Default Value	4	
Description	This parameter specifies the maximum number of elements which will be processed from the high priority queue in ratio to the medium and low priority queues.	
Parameter	Link bandwidth allocation for medium priority queue	
Valid Values	1 to 10	
Default Value	2	
Description	This parameter specifies the maximum number of elements which are processed from the medium priority queue in ratio to the high and low priority queues.	
Parameter	Link bandwidth allocation for low priority queue	
Valid Values	1 to 10	
Default Value	4	
Description	This parameter specifies the maximum number of elements which will be processed from the low priority queue in ratio to the high and medium priority queues.	
Parameter	Queue bandwidth reservation for high priority queue	
Valid Values	10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%	
Default Value	30%	
Description	This parameter specifies the portion of the available buffer space on the serial adapter to be used for queuing elements on the high priority queue, if the buffer space on the adapter is saturated.	
Parameter	Queue bandwidth reservation for medium priority queue	
Valid Values	10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%	
Default Value	30%	
Description	This parameter specifies the portion of the available buffer space on the serial adapter to be used for queuing elements on the medium priority queue, if the buffer space on the adapter is saturated.	
Parameter	Queue bandwidth reservation for low priority queue	
Valid Values	10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%	
Default Value	40%	
Description	This parameter specifies the portion of the available buffer space on the serial adapter to be used for queuing elements on the low priority queue, if the buffer space on the adapter is saturated.	

Table 4-3. Configuration Worksheet - LNM Communication

Parameter Information		**Your Value**
Parameter	Enable LNM communication through this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the IBM LAN Network Manager (LNM) to communicate with the 6611 through this port.	

1 A 6611 port, being both a source and sink for data, is known as data terminal equipment (DTE). A device which connects a 6611 to a network is known as data circuit-terminating equipment (DCE).

Frame Relay

Frame relay is an interface standard that describes the boundary between a user's equipment and a fast-packet network. In frame-relay systems, error frames are discarded; recovery is handled end-to-end at the protocol layer rather than hop-to-hop (as X.25 handles error recovery, for instance).

The 6611 implements RFC 1294 and includes support for permanent virtual circuits (PVCs). The 6611 acts as the data terminal equipment (DTE) and attaches to the frame handler, also known as the data circuit-terminating equipment (DCE). The 6611 supports fragmentation of frames before transmission and reassembly of frames after reception if the packets are larger than the frame relay MTU.

Frame relay is configured only on serial ports (see 4-2 for a list of adapters that contain serial ports). The frame-relay configuration of each serial port on the multiport and combination adapters is independent of the other port or ports attached to that adapter. This means that another protocol, such as PPP, can be configured on one port and frame relay on another. The frame-relay parameters can be different and independent on each port.

Frame relay can be configured:

- On dedicated, point-to-point links. This configuration is also known as a *back-to-back* configuration. See "Sample Network Graphic One - Frame Relay on a Dedicated Line" on page 4-10 for an example of a back-to-back frame relay configuration.
- On a public or private frame-relay network. See "Sample Network Graphic Two - Frame Relay on a Public or Private Frame Relay Network" on page 4-13 for an example.

The 6611 supports the following frame relay topologies:

Fully Meshed Frame-Relay Networks: The 6611 implementation of frame relay supports a fully meshed frame-relay topology. In fully meshed networks, each 6611 has a unique PVC to every other 6611 interconnected by the frame-relay network.

In a fully meshed environment, the LMI protocol and InARP can be used to dynamically learn DLCIs and destination protocol addresses. If provided by the frame-relay service, the LMI protocol can automatically provide the local DLCI number corresponding to each PVC accessible from the 6611. If InARP is supported by the protocol, the 6611 can use InARP to provide a logical mapping between a specific local DLCI and the corresponding destination address for each protocol access at the destination 6611. When InARP is not available, the mapping between the DLCI and the destination protocol address is statically configured through the Configuration Program.

Partially Meshed Frame-Relay Networks: In partially meshed frame-relay networks, the 6611 does not have a unique PVC to every other 6611 in the frame relay network. The 6611 may be required to act as an intermediate hop between the source and destination nodes. Several common partially meshed configurations include the single star configuration, in which one central router acts as a hub and performs intermediate routing to enable the peripheral routers to communicate, and the double star configuration, in which several central routers perform intermediate routing. For more information about these configurations, refer to the *Introduction and Planning Guide*.

The 6611 supports partially meshed frame-relay configurations on a per protocol basis. See Table 4-4 for information about the mesh requirements for each protocol that is forwarded by the 6611.

Table 4-4. Frame-Relay Mesh Requirements Per Protocol

Protocol	**Requirements**
Source route, transparent, and translational bridging	The 6611, when performing bridging function, bridges traffic from one DLCI to another DLCI. The 6611 does not require a fully meshed frame-relay network to perform bridging.
OSPF	Single star configurations are supported for OSPF on the 6611. However, double star configurations that are not fully meshed are not supported because OSPF requires that the router in the hub of the star must be configured as the designated router and each designated router must have direct access to every router in the network.
RIP	When RIP is enabled on the 6611, the physical link is assigned a single IP address, regardless of the number of DLCIs available on that connection. The 6611 uses the split horizon technique for RIP. Therefore, the IP implementation of RIP on the 6611 views the physical connection to the frame-relay network as a single interface and sends a RIP broadcast. Frame relay sends that RIP message on all DLCIs configured for that port. All devices connected to these DLCIs receive the same RIP frames from the 6611. In MPNP prior to Version 1 Release 3, RIP requires a fully meshed frame-relay network to ensure any-to-any connectivity; star configurations are not supported. In Version 1 Release 3, point-to-point links are used to define partially meshed star configurations to the frame-relay network.
AppleTalk	In MPNP prior to Version 1 Release 3, AppleTalk requires a fully meshed frame-relay network. In Version 1 Release 3, the 6611 can be configured to send the entire routing table when it sends routing updates. When the Enable split horizons for routing updates parameter is disabled, the 6611 supports AppleTalk routing in partially meshed frame-relay environments.
DECnet	In MPNP prior to Version 1 Release 1.2, partially meshed configurations are not supported for DECnet. In Version 1 Release 1.2 and later, DECnet is supported in a partially meshed frame-relay network as long as no DECnet end nodes are directly attached to the frame-relay network and split horizon is disabled.
IPX	In MPNP prior to Version 1 Release 3, partially meshed IPX configurations are supported only when the Split horizon for SAP and RIP updates parameter is set to **Off** and when PTF 289 for V1R1.1.2 or PTF 331 for V1R2 is installed. In Version 1 Release 3, the 6611 can be dynamically assigned with multiple IPX network numbers for each frame relay link. When multiple network numbers are provided and split horizon is disabled, the 6611 supports IPX over partially meshed frame relay.
VINES	The 6611 supports VINES routing in partially meshed frame-relay environments.
XNS**	XNS requires a fully meshed frame-relay network.

Refer to the *IBM 6611 Network Processor Introduction and Planning Guide* for more information about frame relay.

Restrictions

Depending on the configuration of frame relay, you may need to provide additional information when configuring the protocols and bridging that will be transported by frame relay.

- To enable frame relay between two ports when the LMI option parameter is set to **None**, you must specify the same data link connection identifiers (DLCIs) on each port.
- If the router at the other end of the DLCI does not support the Inverse Address Resolution Protocol (InARP), then you must enter the protocol address of the remote router for each DLCI.
- If AppleTalk** is routed across frame relay, InARP must be enabled.
- When a frame-relay port is configured to run AppleTalk or a bridging protocol, you must explicitly define the DLCIs that will be used by these and *all other* protocols running on the port.
- When an Ethernet LAN is attached to an 6611 that is receiving frames from a frame-relay network, the maximum transmission unit (MTU) for frame relay must be greater than or equal to the MTU for the Ethernet LAN.
- When configuring frame relay on the serial adapter, the Data encoding parameter (NRZ, NRZI) should be consistent across the network. For more information, see the description of the Data encoding parameter on page 4-4.

Configuration Changes ...

That Cause the Function to Restart

None

That Cause the 6611 to Restart

- Enable frame relay on this port
- Polling interval
- Full inquiry interval
- LMI option
- Use InARP to resolve remote protocol addresses
- DLCIs assigned to this port
- Any change to the static configuration of protocol addresses to DLCIs (for more information, see Source Route Bridging “Configuration Changes...” on page 5-5, Transparent Bridging “Configuration Changes...” on page 5-43, Dual Mode Bridging “Configuration Changes...” on page 5-77, IP “Configuration Changes ...” on page 5-103, Appletalk “Configuration Changes...” on page 5-222, DECnet “Configuration Changes ...” on page 5-257, IPX “Configuration Changes...” on page 5-276, VINES “Configuration Changes ...” on page 5-304, and XNS “Configuration Changes...” on page 5-324)

Compatible Protocols

The 6611 supports local and remote bridging of all network protocols. The following protocols can be routed:

- AppleTalk
- Advanced Peer-to-Peer Networking (APPN)
- Banyan** VINES**
- DECnet

- IP
- IPX
- NetBIOS (transported by data link switching)
- SNA (transported by data link switching or APPN)
- XNS

Configuration Options

Table 4-5 summarizes the configuration options for frame relay. After configuring frame relay on the port, enable bridged and routed protocols at the port and node level.

Table 4-5. Frame-Relay Configuration Options

<table>
<tr><th>WHEN configuring frame relay...</th><th>THEN optionally...</th></tr>
<tr><td>...on a back-to-back link:
Enable frame relay on this port.
Set the LMI option parameter to None.
Enable InARP or explicitly define the remote protocol addresses for each protocol that runs on this frame-relay port.
Define any DLCIs that are assigned to this port. The DLCIs on the frame-relay port of either end of the link must be the same.
Note: When a frame-relay port is configured to run AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by these and all other protocols running on the port.
First, configure the frame-relay protocol by defining a list of DLCIs assigned to the serial port. Then as you define individual protocols on the port, specify which DLCIs are available for use by each protocol.</td><td>Set the polling interval and the full enquiry interval.</td></tr>
<tr><td>...on a public or private network:
Enable frame relay on this port.
Set the LMI option to ANSI T1.617 Annex D or LmiRev1.
Enable InARP or explicitly define the remote protocol addresses for each protocol that runs on this frame-relay port.
Define any DLCIs that are assigned to this port.
Note: When a frame-relay port is configured to run AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by these and all other protocols running on the port.
First, configure the frame-relay protocol by defining a list of DLCIs assigned to the serial port. Then as you define individual protocols on the port, specify which DLCIs are available for use by each protocol.</td><td>Set the polling interval and the full enquiry interval.</td></tr>
</table>

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform routing or bridging over a serial adapter running frame relay. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 4-6. Frame Relay Configuration Verification Checklist

Frame Relay Rule	Configuration Parameter	√
Port-Level Parameters:		
For a given connection, ensure that the Enable physical interface on this port parameter is enabled.	Enable physical interface on this port	
Ensure that frame relay is the framing method and is enabled on both ends of a given connection.	Enable Frame Relay on this port	
	Framing method	
The value of the Use InARP to resolve remote protocol addresses parameter must be the same across connections.	Use InARP to resolve remote protocol addresses	
Ensure that the value of the LMI option parameter is the same across the connection. When the LMI option parameter is set to **None**, the DLCI numbers must be the same.	LMI option	
	DLCIs assigned to this port	
If the Use InARP to resolve remote protocol addresses parameter is disabled, all DLCIs must be configured and DLCI destinations must be defined to provide a logical mapping between the DLCI and the destination protocol address.	Use InARP to resolve remote protocol addresses	
	DLCIs assigned to this port	
If source route bridging, transparent bridging, dual mode bridging, or AppleTalk is enabled, all DLCIs that will be used must be configured.	Enable Source Route Bridging on this port	
	Enable Transparent Bridging on this port	
	Enable AppleTalk on this port	
	Enable Dual Mode Bridging on this port	
	DLCIs assigned to this port	

Sample Network Graphic One - Frame Relay on a Dedicated Line

Figure 4-1 on page 4-11 illustrates a frame relay network in which two routers (6611 A and 6611 B) are connected over a dedicated line. This configuration is also known as a *back-to-back* configuration.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP over frame relay
  - A token-ring port running IP

- 6611 B, which has the following port types and protocols running:
  - A serial port running IP over frame relay
  - A token-ring port running IP

The following information is shown in Figure 4-1:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

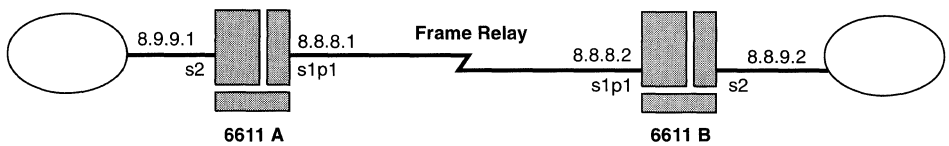


Figure 4-1. Sample Network for Routing TCP/IP Using Frame Relay over a Dedicated Line

This sample network shows the configuration of:

- Frame relay over a dedicated line
- Static routes defined
- Serial and token-ring ports

Summary of All Customized Parameters in Sample One

Use this section as a reference for Figure 4-1. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 4-7. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Data link protocol	Frame Relay	Frame Relay

Table 4-8. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table 4-9. Serial Port - Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Enable Frame Relay on this port	Enable	Enable
Polling interval	10 seconds	10 seconds
Full inquiry interval	6	6
LMI option	None	None
Use InARP to resolve remote protocol addresses	Enable	Enable
DLCIs assigned to this port	50	50

Table 4-10. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Disable	Disable
Point-to-point only	Disable	Disable
Assignment for discovered DLCIs	Mesh	Mesh
IP Priority	NA	NA
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and Protocols Running on Them

Table 4-11. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 4-12. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.9.9.1	8.8.9.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 4-13. Node Level - Static Route Detail Parameters Configured

Parameter	6611 A Value	6611 B Value
Destination IP address	Specific	Specific
Destination address	8.8.9.0	8.9.9.0
Destination mask	255.255.255.0	255.255.255.0
Next hop router number 1	8.8.8.2	8.8.8.1
Next hop router number 2	None	None
Next hop router number 3	None	None
Preference	50	50
Retain route in master table	Disable	Disable

Sample Network Graphic Two - Frame Relay on a Public or Private Frame Relay Network

Figure 4-2 on page 4-14 illustrates a frame relay network in which two routers (6611 A and 6611 B) are connected by a public or private network. InARP is enabled to resolve remote protocol addresses.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP over frame relay
  - A token-ring port running IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP over frame relay
  - A token-ring port running IP

The following information is shown in Figure 4-2 on page 4-14:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

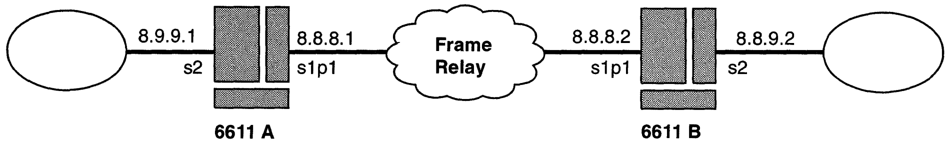


Figure 4-2. Sample Network for Routing TCP/IP Using Frame Relay over a Public or Private Network

This sample network shows the configuration of:

- Frame relay over a public or private network
- Serial and token-ring ports

Summary of All Customized Parameters in Sample Two

Use this section as a reference for Figure 4-2. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and the Protocols Running on Them

Table 4-14. Serial Port Parameters Configured

Parameter	**6611 A Slot 1 Port 1 Value**	**6611 B Slot 1 Port 1 Value**
Data link protocol	Frame Relay	Frame Relay

Table 4-15. Serial Port - Physical Interface Parameters Configured

Parameter	**6611 A Slot 1 Port 1 Value**	**6611 B Slot 1 Port 1 Value**
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table 4-16. Serial Port - Frame-Relay Parameters Configured

Parameter	**6611 A Slot 1 Port 1 Value**	**6611 B Slot 1 Port 1 Value**
Enable Frame Relay on this port	Enable	Enable
Polling interval	10 seconds	10 seconds
Full inquiry interval	6	6
LMI option	ANSI T1.617 Annex D	ANSI T1.617 Annex D
Use InARP to resolve remote protocol addresses	Enable	Enable
DLCIs assigned to this port	None	None

Table 4-17. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Disable	Disable
Point-to-point only	Disable	Disable
Assignment for discovered DLCIs	Mesh	Mesh
IP Priority	NA	NA
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and Protocols Running on Them

Table 4-18. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 4-19. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.9.9.1	8.8.9.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 4-20. Node Level - RIP Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Routing Information Protocol (RIP)	Enable	Enable
Broadcast	Enable	Enable
Zero reserved fields	Enable	Enable
Route preference	100	100

Port Level Worksheet

Use the following table as a worksheet for your port level configurations.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-27 on page D-21 for a mapping of parameter names and their associated labels.

Table 4-21. Configuration Worksheet - Frame-Relay Ports

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable frame relay on this port Enable, Disable Enable This parameter enables or disables frame-relay frame forwarding on this port.	
Parameter **Valid Values** **Default Value** **Description**	Polling interval 5 to 30 seconds 10 seconds This parameter specifies the number of seconds between successive status inquiry messages. When the LMI option parameter is set to **None**, this parameter has no effect.	
Parameter **Valid Values** **Default Value** **Description**	Full inquiry interval 1 to 255 6 This parameter specifies the number of polling intervals that pass before issuance of a full status inquiry message. When the LMI option parameter is set to **None**, this parameter has no effect.	
Parameter **Valid Values** **Default Value** **Description**	LMI option ANSI T1.617 Annex D, LmiRev1, None ANSI T1.617 Annex D This parameter specifies the type of LMI that is active on the frame-relay network.	
Parameter **Valid Values** **Default Value** **Description**	Use InARP to resolve remote protocol addresses Enable, Disable Enable This parameter determines if the protocol addresses of the remote routers that are communicating with your IBM 6611 using frame relay are resolved by using InARP.	
Parameter **Valid Values** **Default Value** **Description**	DLCIs assigned to this port (required for each DLCI defined) A valid DLCI (integer of value in the recommended range of 15 to 1008 decimal) None This parameter contains a list of DLCIs.	

LAN Bridging Protocol

The LAN Bridging Protocol enables an 6611 to communicate over a serial link with one of the following token-ring bridge programs operating on a PS/2 workstation:

- IBM Token-Ring Network Bridge Program, Version 2.2.4 or later
- IBM Remote Token-Ring Bridge/DOS Version 1.01 or later

This configuration is sometimes referred to as *compatibility mode bridging*.

Restrictions

- This protocol runs only on a serial line attached to a serial adapter port on the 6611. Frame relay and PPP cannot be configured on the same serial adapter port when this protocol is selected.
- When connecting the RS449 interface on the 6611 and the V.35 or X.21 interface on the PS/2 bridge, ensure that the 6611 RS449 cable does *not* invert the data. For more information about the 6611 R449 cables, read the *Introduction and Planning Guide*.

Configuration Changes ...

That Require the LAN Bridging Function to Restart

- LAN Bridging Protocol parameters
  - Enable LAN Bridging Protocol on this port
  - Auto reboot on error
  - Performance counter threshold
  - Telecommunications link error threshold
  - Memory dump on error
  - Event log drive
- LNM management parameters
  - Enable ring parameter server
  - Enable ring error monitor
  - Enable configuration report server
  - Virtual MAC address
  - Locally administered MAC address
  - MAC address format
  - Link password 0
  - Link password 1
  - Link password 2
  - Link password 3
- Port-level Source Route Bridging parameters
- Port-level Source Route Bridge filter parameters
- Node-level Source Route Bridging or Translational Bridging parameters
- Node-level Source Route Bridging or Translational Bridging spanning tree parameters
- Node-level DLSw parameters

That Require the 6611 to Restart

None

Compatible Protocols

The 6611 supports compatibility mode bridging of all network protocols. No protocols can be routed.

Configuration Options

Table 4-22 summarizes the configuration options for LAN Bridging Protocol. After configuring LAN Bridging Protocol on the serial port, enable bridged protocols at the port and node level.

Table 4-22. LAN Bridging Protocol Configuration Options

WHEN configuring LAN Bridging Protocol...	THEN optionally...
...on a serial port: • Enable the physical interface on this port. • Enable LAN Bridging Protocol on this port. • If the MAC address of the PS/2 token-ring bridge located on the segment to which this port attaches is locally administered, select the LNM Management push-button. On the LNM Management window, set the Virtual MAC address parameter to **Locally administered address** and enter a locally administered address. • Enable Source Route Bridging on this port and enter the ring number. • Enable LNM communication on at least one bridging port on this 6611 to allow LNM to communicate with the 6611.	• Specify the other physical interface parameters. • Specify the other LAN Bridge Port parameters. • Specify the other Source Route Bridging parameters. • Configure Source Route Bridging filters.
...at the node level: • Enable Source Route or Translational Bridging. • Specify the bridge number and the designated ring number, and enable LAN bridging protocol. • On the DLSw window, specify the virtual ring segment number.	• Specify the other Source Route or Translational Bridging parameters. • Specify the port filter order for Source Route Bridging. • Specify address mapping, Ethernet V2.0 support, transparent bridging parameters, spanning tree parameters, and port filter order or Translational Bridging.

Configuration Verification Checklist

Use the following checklist to help you verify that one or more 6611s are correctly configured to perform bridging over a serial port running LAN Bridging Protocol. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 4-23. LAN Bridging Protocol Configuration Verification Checklist		
LAN Bridging Protocol Rule	**Configuration Parameter**	√
Node-Level Parameters:		
Ensure that the Enable Source Route Bridging on this port parameter is enabled.	Enable Source Route Bridging on this port	
Ensure that the value of the Designated ring number parameter on the Source Route Bridging window is the same as the value of the Ring number parameter configured for a token-ring, frame-relay, or PPP port on this 6611. The value of the Designated ring number parameter can *not* be the same as the ring number for a LAN Bridging Protocol port.	Designated ring number	
	Ring number (port-level parameter)	
Port-Level Parameters:		
Ensure that the Enable physical interface parameter is enabled on this port.	Enable physical interface on this port	
Ensure that the Enable LAN Bridging Protocol on this port parameter is enabled.	Enable LAN Bridging Protocol on this port	
Ensure that the Enable Source Route Bridging on this port parameter is enabled.	Enable Source Route Bridging on this port	
Ensure that the Enable LNM communication parameter is enabled on at least one port of this 6611 if you want to manage attached bridges using LAN Network Manager.	Enable LNM Communication	

Sample Network Graphic

Figure 4-3 shows an 6611 that is configured as a compatibility mode bridge and is connected to a PS/2 bridge. Information that passes between ring 4 and ring 8 is bridged.

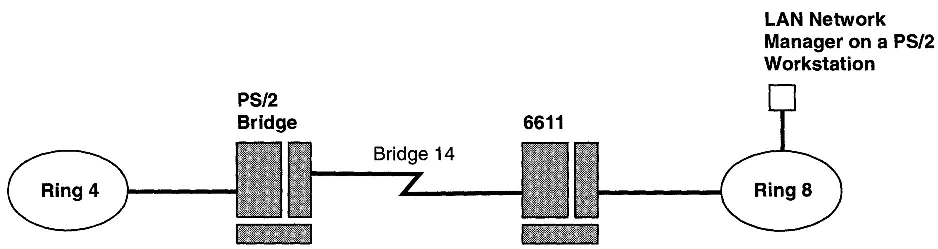


Figure 4-3. Sample Network for Compatibility Mode Bridging

This sample network shows the configuration of:

- Compatibility mode bridging
- IBM Token-Ring Network Bridge Program on a PS/2
- Serial and token-ring ports on the 6611

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 4-3. The following tables list the customized parameters for the configuration of the 6611s in the sample network.

Serial Port and Protocols Running on It

Table 4-24. Serial Port Parameters Configured

Parameter	6611 Value
Data link protocol	LAN Bridging Protocol

Table 4-25. Serial Port - Physical Interface Parameters Configured

Parameter	6611 Value
Enable physical interface on this port	Enable
Interface cable	V.35, V.36, or EIA 232
Cylink serial number	None
Transmit clock source	DCE
Serial line speed	64000
Data encoding	NA
Locally administered MAC address	None
Enable port for transmission group	NA
Transmission group name	NA

Table 4-26. Serial Port - LAN Bridging Protocol Parameters Configured

Parameter	6611 Value
Enable LAN bridging protocol on this port	Enable
Auto reboot on error	Enable
Performance counter threshold	10
Telecommunications link error threshold	0
Memory dump on error	Default drive
Event log drive	Default drive

Table 4-27. Serial Port - LNM Management Parameters Configured

Parameter	6611 Value
Enable ring parameter server	Enable
Enable ring error monitor	Enable
Enable configuration report server	Enable
Virtual MAC address	Locally administered address
Locally administered address	400066110154
MAC address format	Noncanonical
Passwords to link to network managers	
Link password 0	NA
Link password 1	NA
Link password 2	NA
Link password 3	NA

Table 4-28. Serial Port - Source Route Bridging Parameters Configured

Parameter	6611 Value
Enable Source Route Bridging on this port	Enable
Spanning tree mode	Automatic
Path cost	0
Port priority for Translational Bridging	80
Port state	NA
Ring number	4
Max. transmission unit (octets)	2052

Token-Ring Port and Protocols Running on It

Table 4-29. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	NA
MAC address format	NA
Token ring data rate	4 Mbps
Broadcast type	Non-local

Table 4-30. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 Value
Enable Source Route Bridging on this port	Enable
Spanning tree mode	Automatic
Path cost	0
Port priority for Translational Bridging	80
Port state	NA
Ring number	8
Max. transmission unit (octets)	2052

Table 4-31. Token-Ring Port - LNM Communication Parameters Configured

Parameter	6611 Value
Enable LNM communication through this port	Enable

Node-Level Parameters Configured

Table 4-32. Node Level - Source Route Bridging Parameters Configured

Parameter	6611 Value
Enable Source Route Bridging	Enable
Bridge number	14
Enable LAN Bridging Protocol	Enable
Designated ring number	8
Spanning tree parameters	
Bridge priority	8000
Hello time	2
Forward delay time	15
Max age	20

Table 4-33. Node Level - DLSw Parameters Configured

Parameter	6611 Value
Protocols forwarded by DLSw	
SNA	Disable
NetBIOS	Disable
SNA transmission bias	NA
Maximum NetBIOS frame size	2052
DLSw parameters	
Virtual ring segment number	FFF
Destination cache timeout	8
Default DLSw IP address for this 6611	NA

Configuring the IBM Token-Ring Network Bridge Program

When you configure the IBM Token-Ring Network Bridge Program and the 6611 to run as halves of a split bridge, the 6611 must be configured as the *primary* side of the bridge. In this configuration, the 6611 sends configuration information to the IBM Token-Ring Network Bridge Program, which is running as the *secondary* half of the bridge.

To configure the IBM Token-Ring Network Bridge Program:

1. Specify the installation of the secondary half of the bridge on the PS/2 workstation.
2. Specify whether to copy IBM-supplied bridge filters.
3. Accept the default values for the Locally administered address, Shared RAM address, and Early token release parameters in the CONFIG.SYS, or customize them for your configuration.
4. Customize the communications port. Refer to Table 4-33 for the values.

Table 4-34. Communications Port Configuration Program, Page 1 of 1

Parameter	Bridge 14 Value
Line data rate in bits per seconds	64000
Electrical interface (1=V.24, 2=V.35, 3=X.21)	2
Communcations port transmit buffer size in bytes (type 0 to use default)	7489 (default)
Bridge mode (1=leased, 2=switched)	1
Enable modem state verification (Y=Yes, N=No)	Y

Viewing the IBM Token-Ring Network Bridge Program Configuration

The following tables list the values that display when the IBM Token-Ring Network Bridge Program is running and you view the configuration.

Table 4-35. Bridge Configuration, Page 1 of 5

Parameter	Bridge 14 Value
Bridge program level	2.24
Bridge number	E
LAN segment number connected to this bridge half	004
LAN segment number connected to the other bridge half	FFF
Frame forwarding active	Yes
Largest frame size in bytes	2052
Bridge performance threshold (frames lost per 10,000)	10
Telecommunications link error threshold (frames lost per 10,000)	980
Restart on error	Yes

Table 4-36. Bridge Configuration, Page 2 of 5

Parameter	Local LAN segment 004	Remote LAN segment FFF
LAN segment data rate in Mbps	4	16
Hop count limit	7	7
Port's address	400044440004	400066110154
Port microcode level	000010A79073	000000CCCCCCC
Drive for memory dump on error	0	0
Drive for error log	0	0

Table 4-37. Bridge Configuration, Page 3 of 5

Parameter	Local LAN segment 004	Remote LAN segment FFF
Enable Functional Addresses		
Parameter server	Yes	No
Error monitor	Yes	No
Configuration report server	Yes	No
Bridge	Yes	No

Table 4-38. Bridge Configuration, Page 4 of 5

Parameter	Bridge E	
	Local LAN segment 004	**Local LAN segment FFF**
Single-route broadcast	Yes	Yes
Single-route broadcast selection mode	Automatic	
Automatic Single-Route Broadcast Parameters		
Bridge label	8000	
Path cost increment	00000370	

Table 4-39. Bridge Configuration, Page 5 of 5 - Communications Port Parameters

Parameter	Bridge E
Line data rate in bits per second	64000
Electrical interference	2
Transmit buffer size in bytes	7489
Bridge mode	1
Enable modem state verification	Yes

Port Level Worksheet

Use the following tables as worksheets for your port level configurations.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-25 on page D-21 for a mapping of parameter names and their associated labels.

Table 4-40 (Page 1 of 2). Configuration Worksheet - LAN Bridge Port

Parameter Information	Your Value
Parameter Enable LAN Bridging Protocol on this port **Valid Values** Enable, Disable **Default Value** Enable **Description** This parameter enables or disables the connection, through this serial port, to a PS/2 workstation that is running the IBM Token-Ring Network Bridge Program.	
Parameter Auto reboot on error **Valid Values** Enable, Disable **Default Value** Enable **Description** This parameter indicates whether the IBM token-ring bridge program (running on a PS/2 workstation connected to the 6611 port over a serial link) automatically reboots to recover from an error that terminates the program.	
Parameter Bridge performance counter threshold **Valid Values** 0 to 9999 (remove trailing and leading blanks) **Default Value** 10 **Description** This parameter represents the maximum allowable number of frames that are *not* forwarded through the bridge (on the PS/2 workstation at the other end of the serial link attached to this port) during each one-minute interval.	

Table 4-40 (Page 2 of 2). Configuration Worksheet - LAN Bridge Port

Parameter Information		Your Value
Parameter	Telecommunications link error threshold	
Valid Values	0 to 9999 (0 being the default value provided by the IBM token-ring bridge program)	
Default Value	0	
Description	This parameter represents the maximum allowable number of frames that are *not* forwarded through the bridge (on a PS/2 workstation attached to this serial port via a serial line) due to errors on the telecommunications link. This ratio represents the number of frames per 10000 that are lost on the link. Each unit is 0.01% frames not forwarded.	
Parameter	Memory dump on error	
Valid Values	Default drive, A drive, B drive, C drive, D drive	
Default Value	Default drive	
Description	This parameter identifies the disk drive (on the PS/2 workstation at the other end of the serial line attached to this serial port) that is used to write a memory dump when the program is terminated by an internal programming error.	
Parameter	Event log drive	
Valid Values	Default drive, A drive, B drive, C drive, D drive	
Default Value	Default drive	
Description	This parameter identifies the disk drive (on the PS/2 workstation at the other end of the serial line attached to this serial port) that is used to write a memory dump when the IBM Token-Ring Network Bridge Program on that workstation is terminated by an internal programming error.	

Table 4-41 (Page 1 of 2). Configuration Worksheet - LNM Management

Parameter Information		Your Value
Parameter	Enable ring parameter server	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables the ring parameter server functional address for this token-ring port.	
Parameter	Enable ring error monitor	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables the ring error monitor functional address for this token-ring port.	
Parameter	Enable configuration report server	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables the configuration report server functional address for this token-ring port.	
Parameter	Virtual MAC address	
Valid Values	LAN bridge derived address, Locally administered address	
Default Value	LAN bridge derived	
Description	This parameter specifies the MAC address on the data link switching (DLSw) virtual ring to which the LAN Network Manager (LNM) program can link to manage the token-ring segment attached to this port.	

Table 4-41 (Page 2 of 2). Configuration Worksheet - LNM Management

Parameter Information		Your Value
Parameter	Locally administered MAC address	
Valid Values	A valid MAC address	
Default Value	None	
Description	This parameter specifies a locally administered virtual MAC address on the DLSw virtual ring to which the LAN Network Manager (LNM) program can link to manage the locally-attached token-ring segment.	
Parameter	MAC address format	
Valid Values	Noncanonical, Canonical	
Default Value	Noncanonical	
Description	This parameter specifies the address format used for the Locally administered MAC address parameter. The noncanonical format is typically used in token-ring networks.	
Passwords to link to network managers (up to 4 links)		
Parameter	Link password 0	
Valid Values	6 to 8 alphanumeric characters when answered, or blank when no password is used (input is converted to uppercase)	
Default Value	00000000	
Description	Use link passwords to secure the reporting links that the network managers establish with the bridge. These reporting links obtain network management information.	
Parameter	Link password 1	
Valid Values	6 to 8 alphanumeric characters when answered, or blank when no password is used (input is converted to uppercase)	
Default Value	00000000	
Description	Use link passwords to secure the reporting links that the network managers establish with the bridge. These reporting links obtain network management information.	
Parameter	Link password 2	
Valid Values	6 to 8 alphanumeric characters when answered, or blank when no password is used (input is converted to uppercase)	
Default Value	00000000	
Description	Use link passwords to secure the reporting links that the network managers establish with the bridge. These reporting links obtain network management information.	
Parameter	Link password 3	
Valid Values	6 to 8 alphanumeric characters when answered, or blank when no password is used (input is converted to uppercase)	
Default Value	00000000	
Description	Use link passwords to secure the reporting links that the network managers establish with the bridge. These reporting links obtain network management information.	

Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) defines transmission data over a serial link through a serial port.

When PPP is configured on more than one port of a multiport serial adapter, the PPP parameters can be different and independent on each port unless a transmission group is defined. See "Restrictions" for more information about transmission group restrictions.

You may configure PPP on one port and other protocols on the other ports of multiport serial adapter.

To configure PPP, you must do the following:

- Enable or disable PPP on each serial adapter port. The default value is set to **Enable**.
- Tailor the parameters by modifying the default values for the other parameters to match your specific network configuration.

Restrictions

- PPP can be configured only for a serial port.
- The method of PPP link quality determination, Link Quality Monitoring RFC or Link Control Protocol (LCP) pings, must be the same for all PPP peers.
- You should not configure more protocols over a PPP link than will be used. Unused or unneeded protocols consume router processor and memory resources, as well as link bandwidth.
- Routers at both ends of a PPP link should be configured to have the same protocols sent over that link. This is especially important with older PPP implementations because they vary in their interpretation of the PPP RFCs. If both ends of the PPP link do not have the same protocols configured, then interoperability and link establishment problems are possible.
- Transmission groups can only be configured over two serial ports on a single serial adapter. After you configure one serial port for transmission group, the Configuration Program automatically enables transmission group and sets the transmission group name on the other serial port. Refer to Table 4-42 for the serial port combinations that can support a transmission group.

Table 4-42. Transmission Group Serial Port Assignments

Type of Serial Adapter	Serial Ports That Can Form a Transmission Group
2-port serial adapter	T0 and T1
4-port serial adapter	D0 and D1, or D2 and D3
Serial/Ethernet combination adapter	CE1 and CE2
Serial/token-ring combination adapter	CT1 and CT2

- Each transmission group must have a unique transmission group name.

Configuration Changes...

That Require the Function to Restart

- PPP parameters
  - Maximum receive unit
  - Use magic number for loopback detection
- Link quality monitoring protocol parameters
  - Select link quality monitoring method
  - Link quality monitoring interval
  - Allowable number of lost link quality reports
  - Allowable percentage of lost packets
  - Allowable percentage of lost octets
  - Allowable number of lost LCP pings
  - LCP ping timeout
  - Number of successful LCP pings for recovery

That Require the 6611 to Restart

- Enable Point-to-Point Protocol (PPP) on this port

Compatible Protocols

The 6611 supports local and remote bridging of all network layer protocols. The following protocols can be encapsulated within PPP frames:

- AppleTalk
- APPN
- Banyan VINES
- DECnet
- IP
- IPX
- NetBIOS (transported by data link switching)
- SNA (transported by data link switching or APPN)
- XNS

Source route bridging, translational bridging, and transparent bridging are supported over serial links using PPP. For more information about bridging LANs over serial links, see the *Introduction and Planning Guide*.

Configuration Options

Table 4-43 on page 4-29 summarizes the configuration options for PPP.

Table 4-43. PPP Configuration Options

WHEN configuring PPP on a serial adapter port...

- Select the serial adapter port that will be configured for PPP
  - Enable PPP on the port
    - Determine the maximum receive unit size
    - Determine your need to enable loopback protection
    - Determine your need to enable one of the link quality monitoring methods
      - If you choose to enable the link quality monitoring protocol, then:
        - Determine the link quality monitoring interval
        - Select the monitoring criteria
        - Even though you selected the link quality monitoring protocol method, LCP ping parameters should still be set in case a PPP peer does not support the same RFCs as configured above.
          - Determine the allowable number of lost LCP pings
          - Determine the LCP ping timeout value
          - Determine the number of LCP pings needed for recovery

        In such a case, this router will automatically begin using the LCP ping method:
      - If you choose to enable LCP pings only, then:
        - Determine the allowable number of lost LCP pings
        - Determine the LCP ping timeout value
        - Determine the number of LCP pings needed for recovery
- Determine which bridging method (if any) will be used over the PPP link:
  - Source route bridging (see Table 5-5 on page 5-10)
  - Transparent bridging (see Table 5-39 on page 5-49)
  - Dual mode bridging (see Table 5-69 on page 5-80)
- Select the protocols that will be routed over the PPP link:
  - IP (see Table 5-105 on page 5-107)
  - IPX (see Table 5-368 on page 5-277)
  - XNS (see Table 5-429 on page 5-324)
  - DECnet (see Table 5-346 on page 5-259)
  - AppleTalk (see Table 5-300 on page 5-226)
  - VINES (see Table 5-402 on page 5-305)
- Determine if DLSw will take place over the PPP link:
  - SNA (see Table 5-478 on page 5-360)
  - NetBIOS (see Table 5-472 on page 5-356)
- Determine the physical interface parameter values that are appropriate to the port.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform routing or bridging over a serial adapter running PPP. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 4-44. PPP Configuration Verification Checklist		
PPP Rule	**Configuration Parameter**	√
Port-Level Parameters:		
The Enable Point-to-Point Protocol on this port parameter must be enabled on all ports configured for the PPP protocol.	Enable Point-to-Point Protocol on this port	
Ports connected with a PPP link should have the same values for the following parameters: • Maximum receive unit size • Use magic number for loopback protection • Select link quality monitoring method • Link quality monitoring interval	Maximum receive unit size	
	Use magic number for loopback protection	
	Select link quality monitoring method	
	Link quality monitoring interval	

Sample Network Graphic

Figure 4-4 illustrates a network where IP routing is enabled between a workstation and a file server over serial ports across a network. The IP traffic is encapsulated in PPP frames over the serial link.

This sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP over PPP
  - A token-ring port running IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP over PPP
  - A token-ring port running IP

The following information is shown in Figure 4-4:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

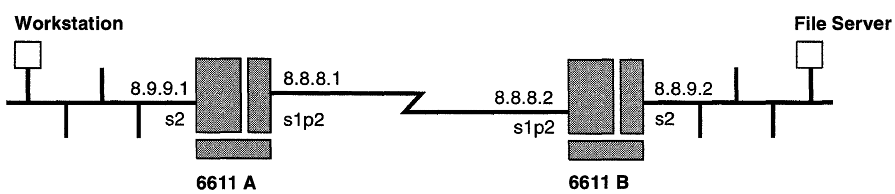


Figure 4-4. Sample PPP Network

This network sample shows the configuration for:

- PPP over serial ports
- Token-ring ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 4-4 on page 4-30. The following tables list the customized parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 4-45. Serial Port Parameters Configured

Parameter	**6611 A Slot 1 Port 1 Value**	**6611 B Slot 1 Port 1 Value**
Data link protocol	PPP	PPP

Table 4-46. Serial Port - Physical Interface Parameters Configured

Parameter	**6611 A Slot 1 Port 1 Value**	**6611 B Slot 1 Port 1 Value**
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table 4-47. Serial Port - PPP Parameters Configured

Parameter	**6611 A Slot 1 Port 1 Value**	**6611 B Slot 1 Port 1 Value**
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 4-48. Serial Port - IP over PPP Parameters Configured

Parameter	**6611 A Slot 1 Port 1 Value**	**6611 B Slot 1 Port 1 Value**
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and Protocols Running on Them

Table 4-49. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 4-50. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.9.2	8.9.9.1
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 4-51. Node Level - RIP Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Routing Information Protocol (RIP)	Enable	Enable
Broadcast	Disable	Disable
Zero reserved fields	Enable	Enable
Route preference	100	100

Port Level Worksheets

To enable serial adapters to transmit and receive PPP frames, you need to enable PPP on the adapter port.

Use the following tables as worksheets for your port level configurations.

- Point-to-Point Protocol on page 4-33
- Define Link Quality Monitoring Protocol Options on page 4-33
- Define LCP Ping Options on page 4-34

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-29 on page D-22 for a mapping of parameter names and their associated labels.

Table 4-52. Configuration Worksheet - Point-to-Point Protocol

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable Point to Point Protocol (PPP) on this port Enable, Disable Enable This parameter enables or disables PPP on this port.	
Parameter **Valid Values** **Default** **Description**	Maximum receive unit size 1500 to 2052 (octets) 1500 This parameter defines the maximum number of octets per packet that are expected to be received on the attached serial line.	
Parameter **Valid Values** **Default** **Description**	Use magic number for loopback detection Enable, Disable Disable This parameter defines the magic number, which provides a way to detect looped-back links.	
Parameter **Valid Values** **Default** **Description**	Select link quality monitoring method Link Quality Monitoring protocol, Link Control Protocol (LCP) pings, None Link Quality Monitoring protocol This parameter selects the method that will be used to monitor the quality of the link attached to this port.	

| Table 4-53 (Page 1 of 2). Configuration Worksheet - Link Quality Monitoring Protocol Options

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Link quality monitoring interval (seconds) 2 to 25 200 000 seconds 20 Counts of packets and octets are received from the remote router according to the time interval specified by this parameter. If the remote router does not specify its own time interval, then this router will send packet and octet counts to the remote router according to this time interval.	
Monitoring criteria: select at least one		
Parameter **Valid Values** **Default** **Description**	Allowable number of lost link quality reports 1 to 65 535 10 This parameter specifies the maximum number of inbound and outbound link quality reports that can be lost before the link is terminated. Even though the inbound and outbound counters are separate, this parameter applies to both.	
Parameter **Valid Values** **Default** **Description**	Allowable percentage of lost packets 1 to 100 percent 15 This parameter specifies the percentage of inbound and outbound packets that can be lost before the link is terminated. Even though the inbound and outbound percentages are separately calculated, this parameter applies to both.	
Parameter **Valid Values** **Default** **Description**	Allowable percentage of lost octets 1 to 100 percent 15 This parameter specifies the percentage of octets that can be lost, in inbound and outbound frames, before the link is terminated. Even though the inbound and outbound percentages are separately calculated, this parameter applies to both.	

Table 4-53 (Page 2 of 2). Configuration Worksheet - Link Quality Monitoring Protocol Options

Parameter Information		Your Value
LCP ping: keepalive monitoring and link recovery method		
Parameter **Valid Values** **Default** **Description**	Allowable number of lost LCP pings 1 to 65 535 4 This parameter specifies the maximum consecutive number of LCP pings that can be lost before the link is terminated.	
Parameter **Valid Values** **Default** **Description**	LCP ping timeout 1 to 65 535 10 This parameter controls the use of LCP pings when monitoring or recovering a link.	
Parameter **Valid Values** **Default** **Description**	Number of successful LCP pings for recovery 1 to 65 535 5 If the link is terminated, this parameter specifies the number of consecutive successful LCP pings that must be issued before the link is reestablished.	

Table 4-54. Configuration Worksheet - Define LCP Ping Options

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Allowable number of lost LCP pings 1 to 65 535 4 This parameter specifies the maximum consecutive number of LCP pings that may be lost before a link is terminated.	
Parameter **Valid Values** **Default** **Description**	LCP ping timeout 1 to 65 535 10 This parameter controls the use of LCP pings when monitoring or recovering a link.	
Parameter **Valid Values** **Default** **Description**	Number of successful LCP pings for recovery 1 to 65 535 5 If the link is terminated, this parameter specifies the number of consecutive successful LCP pings that must be issued before the link is reestablished.	

Ethernet Port

The Ethernet port enables a 6611 to attach to an IEEE 802.3 network or to an Ethernet Version 2 network. You can configure the Ethernet port to support IEEE 802.3, Ethernet Version 2, and IEEE Ethernet subnetwork access point (SNAP).

After you configure the Ethernet port parameters, configure the protocols that you want the adapter to transmit and receive.

The Ethernet port is available on the following adapters:

- 6611 Ethernet Adapter
- 6611 Model 120 Ethernet Adapter
- 6611-A25 1-Port Ethernet Adapter
- 6611-A47 1-Port Ethernet Adapter
- 6611-A47 2-Port Ethernet Adapter
- 6611-A25 Multi-Interface Serial/Ethernet Combination Adapter
- 6611-A47 Multi-Interface Serial/Ethernet Combination Adapter

Restrictions

When an Ethernet LAN is attached to an 6611 that is receiving frames from a frame relay network, the maximum transmission unit (MTU) for frame relay must be greater than or equal to the MTU for the Ethernet LAN.

Configuration Changes ...

That Require the Function to Restart

None

That Require the 6611 to Restart

- Enable physical interface on this port
- MAC address
- Locally administered address
- Enable additional multicast addresses

Compatible Protocols

The 6611 supports local and remote bridging of all network protocols. The following protocols can be routed:

- AppleTalk
- APPN (transported by DLSw)
- Banyan VINES
- DECnet
- IP
- IPX
- NetBIOS (transported by DLSw)
- SNA (transported by DLSw)
- XNS

Worksheet

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-26 on page D-21 for a mapping of parameter names and their associated labels.

Table 4-55 (Page 1 of 2). Configuration Worksheet - Ethernet Port - Physical Interface

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable physical interface on this port Enable, Disable Enable This parameter enables or disables the 6611 Ethernet port.	
Parameter **Valid Values** **Default** **Description**	MAC address Universally administered address, Locally administered address Universally administered address This parameter indicates whether you want to use the universally administered address as the port's medium access control (MAC) sublayer address.	
Parameter **Valid Values** **Default** **Description**	Locally administered address The range of valid addresses is, X'x2 xx xx xx xx xx' X'x6 xx xx xx xx xx' X'xA xx xx xx xx xx' X'xE xx xx xx xx xx' where *x* is any hexadecimal digit. None If you are using a locally administered MAC address for the port, this parameter specifies the address to be used. This address must be entered in canonical format.	
Parameter **Valid Values** **Default** **Description**	Enable additional multicast addresses Enable, Disable Disable This parameter enables or disables the use of additional multicast addresses to allow the Ethernet port to receive frames that are addressed to a group of adapters.	

Table 4-55 (Page 2 of 2). Configuration Worksheet - Ethernet Port - Physical Interface

Parameter Information		Your Value
Multicast Address List Parameter: Configured for each multicast address defined		
Parameter	Multicast MAC address (required for each additional multicast address defined)	
Valid Values	A hexadecimal string with one of the following formats: X'x1 xx xx xx xx xx' X'x3 xx xx xx xx xx' X'x5 xx xx xx xx xx' X'x7 xx xx xx xx xx' X'x9 xx xx xx xx xx' X'xB xx xx xx xx xx' X'xD xx xx xx xx xx' X'xF xx xx xx xx xx' where *x* is any hexadecimal digit. The multicast bit in the first octet must be set to 1 (X'xxxx xxx1').	
Default	None	
Description	This parameter specifies an additional multicast address that includes this Ethernet port. The address must be entered in canonical format.	

Note:

- A maximum of 265 multicast addresses can be specified for an Ethernet port.
- Ethernet addresses are typically represented in canonical form. Canonical form is the address format defined as the standard MAC address representation by the IEEE. In this format, the bit within each octet that is to be transmitted first on a LAN is represented as the least significant bit. For addresses in noncanonical form, the bit within each octet that is transmitted first is represented as the most significant bit.

  To illustrate, the following bit string is shown in both noncanonical and canonical forms:

  B'00010011 00000000 01011010 00000000 00000000 00000001'

  - In noncanonical form: X'13 00 5A 00 00 01'
  - In canonical form: X'C8 00 5A 00 00 80'

Table 4-56. Configuration Worksheet - LNM Communication

Parameter Information		Your Value
Parameter	Enable LNM communication through this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the IBM LAN Network Manager (LNM) to communicate with the 6611 through this port.	

SDLC Adapter

The SDLC adapter enables an 6611 to attach to serial communications links that use a CCITT V.35, an EIA 232-D, a CCITT V.24/V.28, or a CCITT X.21 physical interface. Each port can be connected to only one physical interface. The following list and Figure 4-5 specify the interfaces associated with each port:

- Port 0: EIA 232-D, CCITT V.24/V.28, CCITT V.35, or CCITT X.21
- Port 1: EIA 232-D, CCITT V.24/V.28, or CCITT V.35
- Port 2: EIA 232-D or CCITT V.24/V.28
- Port 3: EIA 232-D or CCITT V.24/V.28

The four ports of the SDLC adapter are provided by the 6611 SDLC Adapter Interface Cable (*SDLC Adapter Interface Cable*). The single cable connector on the SDLC adapter is connected to the SDLC Adapter Interface Cable, which has multiple cables and connectors for the supported physical interfaces. Each of the cable connectors on the SDLC Adapter Interface Cable is associated with only one of the four ports. The SDLC Adapter Interface Cable is connected to one or more SDLC adapter cables, each of which is connected to a serial communications link.

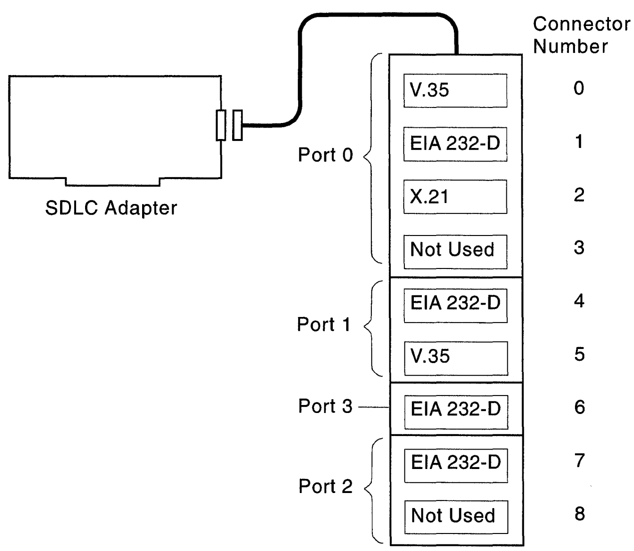


Figure 4-5. SDLC adapter Ports

The following list specifies the maximum number of connections to the adapter as determined by the type of interface used:

- Four EIA 232-D connections (using ports 0, 1, 2, and 3)
- Four CCITT V.24/V.28 connections (using ports 0, 1, 2, and 3)
- Two CCITT V.35 connections (using ports 0 and 1)
- One CCITT X.21 connection (using port 0)
- Up to four connections of mixed type (using ports 0, 1, 2, and 3)

Note: The 6611 requires different V.35 cables to be used for SDLC and serial ports. Check the part number to ensure that you are using the correct V.35 cable for the SDLC adapter. For more information, read the *Introduction and Planning Guide*.

You must configure at least the following SDLC adapter configuration parameters for each port you want to use:

- Physical link type
- Serial encoding

Refer to the *Introduction and Planning Guide* for additional information on the SDLC adapter.

Configuring SNA Link Stations for the SDLC Adapter

After you configure the SDLC adapter parameters, you must configure each SNA link station attached to the SDLC adapter. Up to 254 SNA link stations can be defined on each SDLC adapter port. SNA link stations are PU Type 2.0 by default; to support PU Type 2.1 link stations, enable the Station type 2.1 parameter and enter the Secondary SDLC address for this 6611.

Data link switching provides communication between SNA link stations attached to the SDLC adapter and either a SNA link station attached to a LAN on the same 6611 or a SNA link station attached to a LAN on a remote 6611. To configure a SNA link station to communicate through DLSw, you must specify the following SNA link station parameters on the SDLC adapter:

- Station address
- Station source MAC address (noncanonical)
- Station Source SAP

The Station address parameter specifies the SDLC address of this station. This value must match the value assigned on the link station. The Station source MAC address parameter maps the link station's SDLC address to a MAC address on the virtual ring maintained by DLSw. This MAC address allows the SNA station to appear to other network devices as if it were attached to a LAN. The Station source MAC address is a locally administered address that does not correspond to any physical address. The Station Source SAP parameter specifies the source service access point (SSAP) to be used for communication with this link station.

Optionally, you can also configure the following parameters:

- Station destination MAC address (noncanonical)
- Station Destination SAP
- Station type 2.1
- Secondary SDLC address for this 6611
- Station XID value
- SNA link station options

When you configure the Station destination MAC address parameter, the 6611 activates the SNA link station and attempts to establish a connection between the link station and the device at the specified destination MAC address. When both stations are configured as PU type 2.1 nodes, the destination MAC address can be the virtual MAC address of the destination SDLC station. Otherwise, the destination MAC address is the physical MAC address of a SNA device on a LAN. When the Station destination MAC address is not specified, the SNA link station is activated only when the 6611 receives information addressed to the station.

Restrictions

- A maximum of three SDLC adapters can be operated in the 6611 Model 140. A maximum of six SDLC adapters can be operated in the 6611 Model 170. Only SNA is supported on the SDLC adapter.
- A maximum of 254 SNA stations can be configured for a port on the SDLC adapter. The values you configure for one station are independent of the values you configure for the other stations and independent of each SDLC port.
- A hardware failure might occur if the IBM 6611 is directly attached to a PS/2, and you try to reconfigure the line speed without shutting down the Communications Manager session on the PS/2. To ensure that the hardware failure does not occur, shut down the Communications Manager session, reconfigure the line speed, and then restart the session.
- When you directly attach an external device, such as an IBM 3174 Communications Controller, to the IBM 6611 through an SDLC port, the following restrictions apply:
  - The external device must use the EIA 232 interface and accept line speeds of 4800, 9600, 19200, or 38400 bps.
  - The external device must be configured for external clocking, while the SDLC port in the IBM 6611 must be configured for internal clocking.

  For more information about directly attaching external devices to the SDLC adapter, read the *Introduction and Planning Guide*.

Configuration Changes ...

That Require the SDLC Function to Restart

- Physical interface parameters
  - Enable physical interface on this port
  - Serial encoding
  - Request to send
  - Data rate select
  - Data terminal ready

That Require the 6611 to Restart

- SNA link station parameters
  - Station address
  - Station source MAC address
  - Station Source SAP
  - Station destination MAC address
  - Station Destination SAP
  - Station type 2.1
  - Secondary SDLC address for 6611
  - Station XID value
- SNA link station option parameters
  - Primary slow list timeout
  - Retransmit count
  - Retransmit threshold
  - Primary repoll threshold
  - Primary repoll count
  - Transmit window count
  - Maximum I-field size
  - Force disconnect timeout
  - Primary repoll timeout

Compatible Protocols

The SDLC adapter supports routing of SNA and SDLC to logical link control (LLC) conversion (both transported by DLSw).

Worksheets

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-28 on page D-21 for a mapping of parameter names and their associated labels.

Use the following tables as worksheets for your SDLC adapter configurations:

- 4 Port SDLC - Physical Interface on page 4-41
- SNA Link Station - Detail on page 4-42
- SNA Link Station Options on page 4-43

Table 4-57 (Page 1 of 2). Configuration Worksheet - 4 Port SDLC - Physical Interface

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable interface Enable, Disable Disable This parameter enables or disables this SDLC adapter port.	
Parameter **Valid Values** **Default** **Description**	Serial encoding NRZ, NRZI NRZ This parameter specifies how the line transition occurs on the serial link attached to this SDLC adapter port.	
Parameter **Valid Values** **Default** **Description**	Request to send Continuous, Controlled Continuous This parameter determines the manner in which the communications link connected to this port uses the request to send (RTS) signal while modems are attached.	
Parameter **Valid Values** **Default** **Description**	Data rate select Full, Alternate Full This parameter indicates the data transfer rate you want to use on the communications link connected to this SDLC adapter port.	
Parameter **Valid Values** **Default** **Description**	Data terminal ready Connect data set to line (CDSTL), Data terminal ready (DTR) Connect data set to line (CDSTL) This parameter determines the desired signal used on this SDLC adapter port, if the 6611 is ready to communicate with the modem attached to the communications link.	
Parameter **Valid Values** **Default** **Description**	Bit clocking External, Internal External This parameter indicates which data communication equipment, either the 6611 or the modem, provides the clock signal for synchronizing data transmission. Select **External** if you want the modem to provide the bit clocking. Select **Internal** if you want the 6611 to provide bit clocking.	

Table 4-57 (Page 2 of 2). Configuration Worksheet - 4 Port SDLC - Physical Interface

Parameter Information		Your Value
Parameter	Transmit rate	
Valid Values	4800, 9600, 19200, 38400 bps	
Default	19200 bps	
Description	This parameter specifies the data transfer rate you want to use on the communications link connected to this SDLC adapter port. This parameter can be defined only when the Bit clocking parameter is set to **Internal**.	

| *Table 4-58 (Page 1 of 2). Configuration Worksheet - SNA Link Station - Detail*

Parameter Information		Your Value
Parameter	Station address (required)	
Valid Values		X'00' to X'FE'. X'00' is only valid when this station is a PU type 2.1 stations and is the only PU type 2.1 station attached to this port.	
Default	None	
Description	This parameter specifies the SDLC address of this station.	
Parameter	Station source MAC address (required)	
Valid Values	An address in noncanonical format with a valid range of: X'4000 0000 0000' to X'7FFF FFFF FFFF'	
Default	None	
Description	This parameter specifies an address in the form of a MAC address that is associated with the station's SDLC address. This MAC address represents the station on the virtual ring maintained by DLSw. The address is locally administered and cannot correspond to any physical MAC address within the network.	
Parameter	Station Source SAP (required)	
Valid Values	X'02' to X'EC', in increments of 2	
Default	None	
Description	This parameter specifies the service access point (SAP) on the SNA station that will send and receive data.	
Parameter	Station destination MAC address	
Valid Values	An address in noncanonical format with a valid range of: X'4000 0000 0000' to X'7FFF FFFF FFFF'	
Default	None	
Description	This parameter defines the physical MAC address of a destination SNA station on a token-ring or Ethernet LAN. When this parameter is specified, the 6611 activates the SNA station and attempts to establish a connection between the station and the device at the specified destination MAC address. When this parameter is not specified, the SNA station is activated only when the 6611 receives information addressed to the station.	
Parameter	Station Destination SAP	
Valid Values	X'02' to X'EC', in increments of 2	
Default	None	
Description	This parameter specifies the service access point (SAP) on the destination SNA station to which data will be sent.	

Table 4-58 (Page 2 of 2). Configuration Worksheet - SNA Link Station - Detail

Parameter Information		Your Value
Parameter	Station type 2.1	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter specifies whether this SNA station is a type 2.1 (T2.1) node. When this parameter is set to **Disable**, the node type is assumed to be type 2.0. When this parameter is enabled and there is only one SNA station defined on the port, the link station role for this SNA station (primary or secondary) is negotiated with the locally attached 6611. In this case, the Secondary SLDC address for 6611 parameter must be specified because the 6611 may assume the role of a secondary station after role negotiation. When this parameter is set to **Enable** there are other SNA stations defined on the port (either T2.1 or non-T2.1 stations), the link station role for the 6611 defaults to primary.	
Parameter	Secondary SDLC address for 6611	
Valid Values	X'01' to X'FF'	
Default	None	
Description	This parameter specifies the secondary SDLC address for the locally-attached 6611 and is required if this SNA station is defined as a type 2.1 node. This address will be used if the 6611 assumes the role of a secondary station during link station role negotiation.	
Parameter	Station XID value	
Valid Values	X'0000 0000' to X'FFFF FFFF'	
Default	None	
Description	This parameter specifies an XID value that uniquely identifies this station. XID values are exchanged between SNA stations when a connection is being established.	

Table 4-59 (Page 1 of 2). Configuration Worksheet - SNA Link Station Options

Parameter Information		Your Value
Parameter	Primary slow list timeout	
Valid Values	0 to 60 seconds. 0 disables slow list polling.	
Default	None	
Description	This parameter specifies the amount of time (in seconds) that the primary station should wait between polls to stations on the *slow list*. Secondary stations that are not transmitting data are placed on the slow list after a period of time. Stations on the slow list are polled less frequently by the primary station. Stations are taken off the slow list as soon as they begin to transmit data.	
Parameter	Retransmit count	
Valid Values	1 to 50 frames	
Default	10 frames	
Description	This parameter specifies the number of contiguous information frame bursts that will be transmitted to this station before declaring a permanent transmission error.	
Parameter	Retransmit threshold	
Valid Values	1 to 100 frames	
Default	10 frames	
Description	This parameter defines the number of information frame retransmissions allowed as a percentage of total information frame transmissions.	

Table 4-59 (Page 2 of 2). Configuration Worksheet - SNA Link Station Options

Parameter Information		Your Value
Parameter	Primary repoll threshold	
Valid Values	1 to 100 percent	
Default	10 percent	
Description	This parameter defines the number of repolls as a percentage of the totals polls sent to the secondary station. The specified percentage equals the maximum rate of repolls allowed.	
Parameter	Primary repoll count	
Valid Values	3 to 50 times	
Default Value	15 times	
Description	This parameter defines the number of times that the primary station should poll the secondary station unsuccessfully before marking the station as not working.	
Parameter	Transmit window count	
Valid Values	1 to 7 frames	
Default Value	7 frames	
Description	This parameter defines the number of SDLC information frames to send to this station before turning the line around to get a response.	
Parameter	Maximum I-field size	
Valid Values	265 to 2100 octets	
Default Value	265 octets	
Description	This parameter specifies the maximum size information frame (I-frame) that the 6611 can transmit or receive. Larger I-frames will be segmented into smaller frames equal to the size specified by this parameter. To prevent errors, ensure that the bridges in your network do not specify a maximum transmission unit size smaller than this maximum I-frame size.	
Parameter	Force disconnect timeout	
Valid Values	1 to 600 seconds	
Default Value	120 seconds	
Description	This parameter defines the number of seconds the 6611 should wait after requesting a disconnect (DISC) from the link before forcing a disconnect.	
Parameter	Primary repoll timeout	
Valid Values	1 to 250 tenths of a second	
Default Value	30 tenths of a second	
Description	The primary station polls the secondary station and waits for a response from the secondary station. This parameter defines the length of time (in tenths of a second) that the primary station should wait for a response from the secondary station.	

Token-Ring Port

The Token-Ring Port enables a 6611 to attach to an IEEE 802.5 network, such as the IBM Token-Ring Network. The Token-ring data rate parameter must be configured to match the data rate of the token ring to which it is attached. The choices are 4 Mbps or 16 Mbps.

After you configure the token-ring port parameters, configure the protocols for which you want the port to transmit and receive frames.

The token-ring port is available on the following adapters:

- 6611 Token-Ring Network 16/4 Adapter
- 6611 Model 120 Token-Ring Network 16/4 Adapter
- 6611-A25 1-Port Token-Ring Network 16/4 Adapter
- 6611-A25 2-Port Token-Ring Network 16/4 Adapter
- 6611-A47 1-Port Token-Ring Network 16/4 Adapter
- 6611-A47 2-Port Token-Ring Network 16/4 Adapter
- 6611-A25 Multi-Interface Serial/Token-Ring Combination Adapter
- 6611-A47 Multi-Interface Serial/Token-Ring Combination Adapter

Restrictions

None

Configuration Changes ...

That Require the Function to Restart

None

That Require the 6611 to Restart

- Enable physical interface on this port
- MAC address
- Locally administered address
- Token-ring data rate
- Broadcast type
- MAC address format

Compatible Protocols

The 6611 supports local and remote bridging of all network protocols. The following protocols can be routed:

- AppleTalk
- APPN (transported by DLSw)
- Banyan VINES
- DECnet
- IP
- IPX
- NetBIOS (transported by DLSw)
- SNA (transported by DLSw)
- XNS

Worksheets

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-32 on page D-23 for a mapping of parameter names and their associated labels.

Use the following tables as worksheets for your token-ring port configurations:

- Token Ring Port - Physical Interface on page 4-46
- Media Management on page 4-47
- LNM Management on page 4-48
- LNM Communication on page 4-49

Table 4-60 (Page 1 of 2). Configuration Worksheet - Token Ring Port - Physical Interface

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable physical interface on this port Enable, Disable Enable This parameter enables or disables the 6611 Token-Ring Network 16/4 port.	
Parameter **Valid Values** **Default** **Description**	MAC address Universally administered address, Locally administered address Universally administered address This parameter indicates whether you want to use the universally administered address as the port's medium access control (MAC) sublayer address.	
Parameter **Valid Values** **Default** **Description**	Locally administered address For an address in noncanonical format, the valid range is, X'4000 0000 0000' to X'7FFF FFFF FFFF' For an address in canonical format, the valid ranges are, X'x2 xx xx xx xx xx' X'x6 xx xx xx xx xx' X'xA xx xx xx xx xx' X'xE xx xx xx xx xx' where *x* is any hexadecimal digit. None If you are using a locally administered MAC address for the port, this parameter specifies the address to be used.	
Parameter **Valid Values** **Default** **Description**	MAC address format Noncanonical, canonical Noncanonical This parameter specifies the format used for the locally administered address. This address is typically entered in noncanonical format.	
Parameter **Valid Values** **Default** **Description**	Token ring data rate (required) 4 Mbps, 16 Mbps None This parameter specifies the data rate of the ring to which the port is connected.	

Table 4-60 (Page 2 of 2). Configuration Worksheet - Token Ring Port - Physical Interface

Parameter Information		Your Value
Parameter	Broadcast type	
Valid Values	Non-local, Local	
Default	Non-local	
Description	This parameter specifies whether broadcasts are sent with the routing information (RI) bit turned on and pass through source route bridges to other rings, or are sent with the RI bit turned off and pass only through transparent bridges to other rings.	

Note: Canonical form is the address format defined as the standard MAC address representation by the IEEE. In this format, the bit within each octet that is to be transmitted first on a LAN is represented as the least significant bit. For addresses in noncanonical form, the bit within each octet that is transmitted first is represented as the most significant bit.

To illustrate, the following bit string is shown in both noncanonical and canonical forms:

B'00010011 00000000 01011010 00000000 00000000 00000001'

- In noncanonical form: X'13 00 5A 00 00 01'
- In canonical form: X'C8 00 5A 00 00 80'

Table 4-61. Configuration Worksheet - Media Management

Parameter Information		Your Value
Parameter	Enable ring error monitor	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the ring error monitor functional address for this token-ring port.	
Parameter	Enable configuration report server	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the configuration report server functional address for this token-ring port.	
Parameter	Enable ring parameter server	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the ring parameter server functional address for this token-ring port.	
Parameter	Token ring segment number	
Valid Values	X'001' to X'FFF'	
Default Value	None	
Description	This parameter uniquely identifies the token-ring segment attached to this port within the bridged token-ring network.	

Table 4-62 (Page 1 of 2). Configuration Worksheet - LNM Management

Parameter Information		Your Value
Parameter	Enable LNM to manage this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter specifies whether the LAN Network Manager (LNM) program can remotely manage the ring error monitor (REM) server, the configuration report server (CRS), and the ring parameter server (RPS) for this token-ring port. Each of these servers can be individually activated or deactivated per port.	
Parameter	Bridge performance counter threshold	
Valid Values	0 to 9999	
Default Value	None	
Description	This parameter counts the number of frames per 10 000 that the token-ring port received, but was unable to relay within the designated 1-minute time frame. This inability to relay is due to a target ring inoperative state, adapter congestion, or a frame that is not valid. Each unit is 0.001% frames not forwarded.	
Parameter	Virtual MAC address	
Valid Values	Port derived address, Locally administered address	
Default Value	Port derived	
Description	This parameter specifies the MAC address on the DLSw virtual ring to which the LAN Network Manager (LNM) program can link to manage the token-ring segment attached to this port.	
Parameter	Locally administered address	
Valid Values	A valid MAC address	
Default Value	None	
Description	This parameter specifies a locally administered virtual MAC address on the data link switching (DLSw) virtual ring to which the LAN Network Manager (LNM) program can link to manage the locally-attached token-ring segment. The address is typically entered in noncanonical format in the MAC address format parameter.	
Parameter	MAC address format	
Valid Values	Noncanonical, Canonical	
Default Value	Noncanonical	
Description	This parameter specifies the address format used for the Locally administered address parameter. The noncanonical format is typically used in token-ring networks.	
Passwords to link to LNM		
Parameter	Link password 0	
Valid Values	6 to 8 alphanumeric characters when answered, or blank when no password is used (input is converted to uppercase)	
Default Value	00000000	
Description	Use link passwords to secure the reporting links that the network managers establish with the bridge. These reporting links obtain network management information.	
Parameter	Link password 1	
Valid Values	6 to 8 alphanumeric characters when answered, or blank when no password is used (input is converted to uppercase)	
Default Value	00000000	
Description	Use link passwords to secure the reporting links that the network managers establish with the bridge. These reporting links obtain network management information.	

Table 4-62 (Page 2 of 2). Configuration Worksheet - LNM Management

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Link password 2 6 to 8 alphanumeric characters when answered, or blank when no password is used (input is converted to uppercase) 00000000 Use link passwords to secure the reporting links that the network managers establish with the bridge. These reporting links obtain network management information.	
Parameter **Valid Values** **Default Value** **Description**	Link password 3 6 to 8 alphanumeric characters when answered, or blank when no password is used (input is converted to uppercase) 00000000 Use link passwords to secure the reporting links that the network managers establish with the bridge. These reporting links obtain network management information.	

Table 4-63. Configuration Worksheet - LNM Communication

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable LNM communication through this port Enable, Disable Disable This parameter enables or disables the IBM LAN Network Manager (LNM) to communicate with the 6611 through this port.	

X.25 Adapter

The X.25 adapter allows the 6611 to act as a data terminal equipment (DTE) device. Permanent virtual circuits (PVCs) providing continuous connections and switched virtual circuits (SVCs) providing periodic connections are established over the X.25 network.

For more information about X.25, see the *Introduction and Planning Guide.*

Restrictions

- The X.25 adapter cannot be configured for bridging.
- You can configure a maximum of four X.25 adapters for each 6611 (Model 140, Model 170, Model 145 and Model 175).
- Packet filters that are configured on the node level are not applied to inbound X.25 packets.

Configuration Changes ...

That Require the X.25 Function to Restart

- Subscription mapping parameters
  - Local DTE address (NUA)
  - Network identifier
  - Lowest logical channel number (SVC outgoing)
  - Number of logical channels (SVC outgoing)
  - Lowest logical channels (SVC 2-way)
  - Number of logical channels (SVC 2-way)
  - Lowest logical channel number (SVC incoming)
  - Number of logical channels (SVC incoming)
  - Lowest logical channel number (PVC)
  - Number of logical channels for PVCs
- Subscription mapping option parameters
  - CCITT support
  - Frame window size
  - Frame modulo
  - Connection mode
  - Auto-call unit
  - Auto-call unit disconnection timeout
- PVC settings parameters
  - Logical channel number
  - Receive packet size
  - Transmit packet size
  - Receive packet window
  - Transmit packet window
  - Autoreset value
- SVC options parameters
  - Default receive packet size
  - Default transmit packet size
  - Default receive packet window
  - Default transmit packet window

- Include calling address in call request packets
- Calling address in incoming call packets
- Allow incoming calls
- Allow outgoing calls

- Facilities control parameters
  - Packet size negotiation facility
  - Packet window size negotiation facility
  - Packet size and packet window size negotiation
  - Reverse charging facility
  - Allow reverse charging
  - Basic format
  - Extended format
  - CUG with OA selection facility - basic format
  - CUG with OA selection facility - extended format
  - Closed user group

- Network tuning parameters
  - N2 counter
  - T1 timer
  - T4 timer
  - Maximum number of clear packets
  - Maximum number of reset packets
  - T24 timer
  - T25 timer
  - Poll timer

That Require the 6611 to Restart

- Physical interface parameters
  - Enable X.25 interface on this port
  - Type of line
  - Locally administered MAC address

Compatible Protocols

The 6611 supports local and remote bridging of all network protocols. The following protocols can be routed:

- IP
- IPX
- SNA (transported by DLSw)
- NetBIOS (transported by DLSw)
- APPN (transported by DLSw)

Configuration Options

Table 4-64 summarizes the options for configuring the X.25 adapter.

Table 4-64 (Page 1 of 2). X.25 Configuration Options

<table>
<tr><th>WHEN configuring the X.25 adapter for...</th><th>THEN optionally...</th></tr>
<tr><td>...a basic configuration:
• Enable the X.25 interface.
• Specify whether the X.25 adapter is DTE or DTE back-to-back (Type of line parameter).
• Specify the local DTE address on the Subscription Mapping window.</td><td>• Specify the protocols that will be routed over this X.25 port. For more information, see Table 5-105 on page 5-107 and Table 5-368 on page 5-277.
• Specify other subscription mapping options, PVC settings, and SVC options.
• Specify network tuning options.</td></tr>
<tr><td colspan="2">...no SVC packet size negotiation:
Configure the basic X.25 configuration, then:
• On the SVC Options window:
– Set the Default SVC receive packet size parameter to your default receive packet size for SVCs.
– Set the Default SVC transmit packet size parameter to your default transmit packet size for SVCs.
• On the Facilities Control window: disable the Packet Size Negotiation Facility parameter.
• On the SVC Options window for each protocol running over X.25:
– Set the Receive packet size parameter to None.
– Set the Transmit packet size parameter to None.
• Ensure that PVC and SVC options match your X.25 network subscription.
Note: The Packet size and Packet Window size negotiation parameter is not applicable.</td></tr>
<tr><td colspan="2">...SVC packet size negotiation:
Configure the basic X.25 configuration, then:
• On the SVC Options window:
– Set the Default SVC receive packet size parameter to your default receive packet size for SVCs.
– Set the Default SVC transmit packet size parameter to your default transmit packet size for SVCs.
• On the Facilities Control window:
– Enable the Packet Size Negotiation Facility parameter.
– Set the Packet size and Packet Window size parameter to Negotiate or Validate.
Validate means that an incoming value for packet size is accepted when it is less than or equal to the value for the Receive packet size parameter or the Transmit packet size parameter as applicable. The call is cleared otherwise.
Negotiate means that an incoming value for packet size is negotiated down in the call accepted packet when it is greater than the value for the Receive packet size parameter or the Transmit packet size parameter as applicable.
• On the SVC Options window for each protocol running over X.25:
– For outgoing calls, set the Receive packet window size parameter to your target receive packet size.
– For outgoing calls, set the Transmit packet window size parameter to your target transmit packet size.
• Ensure that PVC and SVC options match your X.25 network subscription.</td></tr>
</table>

Table 4-64 (Page 2 of 2). X.25 Configuration Options

WHEN configuring the X.25 adapter for...

...no SVC packet window size negotiation:

Configure the basic X.25 configuration, then:

- On the SVC Options window:
  - Set the Default SVC receive packet window parameter to your default receive packet size for SVCs.
  - Set the Default SVC transmit packet window parameter to your default transmit packet size for SVCs.
- On the Facilities Control window: disable the Packet window size negotiation facility parameter.
- On the SVC Options window for each protocol running over X.25:
  - Do not give the Receive packet window size parameter a value.
  - Do not give the Transmit packet window size parameter a value.
- Ensure that PVC and SVC options match your X.25 network subscription.

Note: The Packet size and Packet Window size negotiation parameter is not applicable.

...SVC packet window size negotiation:

Configure the basic X.25 configuration, then:

- On the SVC Options window:
  - Set the Default SVC receive packet window parameter to your default receive packet window size for SVCs.
  - Set the Default SVC transmit packet window parameter to your default transmit packet window size for SVCs.
- On the Facilities Control window:
  - Enable the Packet window size negotiation facility parameter.
  - For incoming calls, set the Packet size and packet window size negotiation parameter to **Negotiate** or **Validate**.

  Validate means that an incoming value for packet window size is accepted when it is less than or equal to the value for the Receive packet window size parameter or the Transmit packet window size parameter as applicable. The call is cleared otherwise.

  Negotiate means that an incoming value for packet window size is negotiated down in the call accepted packet when it is greater than the value for the Receive packet window size parameter or the Transmit packet window size parameter as applicable.
- On the SVC Options window for each protocol running over X.25:
  - For outgoing calls, set the Receive packet window size parameter to your target receive packet size.
  - For outgoing calls, set the Transmit packet window size parameter to your target transmit packet window size.
- Ensure that PVC and SVC options match your X.25 network subscription.

Testing Your X.25 Configuration

To verify your X.25 configuration, test:

- Your frame and packet level configurations to ensure that the 6611 can communicate with the DCE to connects to the X.25 network
- Any IP or IPX applications that will run across that network

This section describes how to test the 6611's X.25 configuration to verify that the 6611 can communicate with the DCE. This can be done without traversing an X.25 network. See Figure 4-6 on page 4-54 for the sample test scenario.

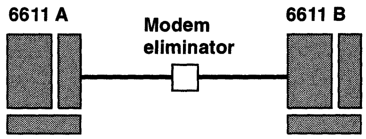


Figure 4-6. Sample Test Network for X.25 Connections

Configure two 6611s (6611 A and 6611 B) to match your network subscription. Also configure IP and modify the value of the Type of line parameter so that the 6611 A value is set to **Back-to-back DTE** and the 6611 B value is set to **DTE**.

Connect 6611 A's X.25 port to a modem eliminator, then connect 6611 B's X.25 port to the modem eliminator. Transport and load the configurations on to the 6611s. When the configurations are loaded, access the System Manager on 6611 A and issue an IP ping to the IP address of 6611 B's X.25 port. If this ping is not successful, verify that your configurations are correct and try again. If the ping is successful, access 6611 B's System Manager and issue an IP ping to 6611 A's X.25 port. If your configurations are valid, the IP ping flows across this connection as if a real X.25 network existed between the 6611s.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform bridging or routing over the X.25 adapter. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 4-65 (Page 1 of 2). X.25 Configuration Verification Checklist

X.25 Rule	**Configuration Parameter**	√
Port-Level Parameters:		
The Enable physical interface on this port parameter must be enabled on all ports that communicate using X.25.	Enable physical interface on this port	
When two 6611s are running back-to-back (no cloud in between), the value of the Type of line parameter for one port should be set to **Back-to-back DTE** while the value for the remote port should be set to **DTE**.	Type of line	
When the T1 timer parameter is set below the default of 60, the value may cause a loss of carrier.	T1 timer	
Both communicating ports must have identical values for the following parameters: • Network identifier • CCITT support • Packet modulo • Enable ICMP address mask requests • Maximum transmission unit	Network identifier	
	CCITT support	
	Packet modulo	
	Maximum transmission unit	

Table 4-65 (Page 2 of 2). X.25 Configuration Verification Checklist		
X.25 Rule	**Configuration Parameter**	√
For the PVC - Detail window, PVC Defaults window, and SVC Options window, the value of the local port's Receive packet size parameter must equal the value of the remote port's Transmit packet size parameter, and vice versa.	Receive packet size (PVC - Detail)	
	Transmit packet size (PVC - Detail)	
	Receive packet size (PVC Defaults)	
	Transmit packet size (PVC Defaults)	
	Receive packet size (SVC - Options)	
	Transmit packet size (SVC - Options)	
The value of the local port's Destination IP address for X.25 parameter must be equal to the value of the remote port's IP address parameter, and vice versa.	Destination IP address for X.25	
	IP address	
The value of the local port's Remote DTE address parameter must be equal to the value of the remote port's Local DTE address parameter, and vice versa.	Remote DTE address	
	Local DTE address	
If running RIP, the value of the local port's Destination IP address for X.25 parameter must be included in the RIP IP address of Trusted Router list for that port.	Destination IP address for X.25	
	IP address of trusted router	

Sample Network Graphic

Figure 4-7 on page 4-56 shows a sample network in which four 6611s (6611 A, 6611 B, 6611 C, and 6611 D) are configured to route IP and IPX over an X.25 network.

The following information is shown in Figure 4-7 on page 4-56:

- IP addresses
- IPX network numbers
- Slot and port numbers, abbreviated s*x* p*y*
- Ring numbers and ring speeds

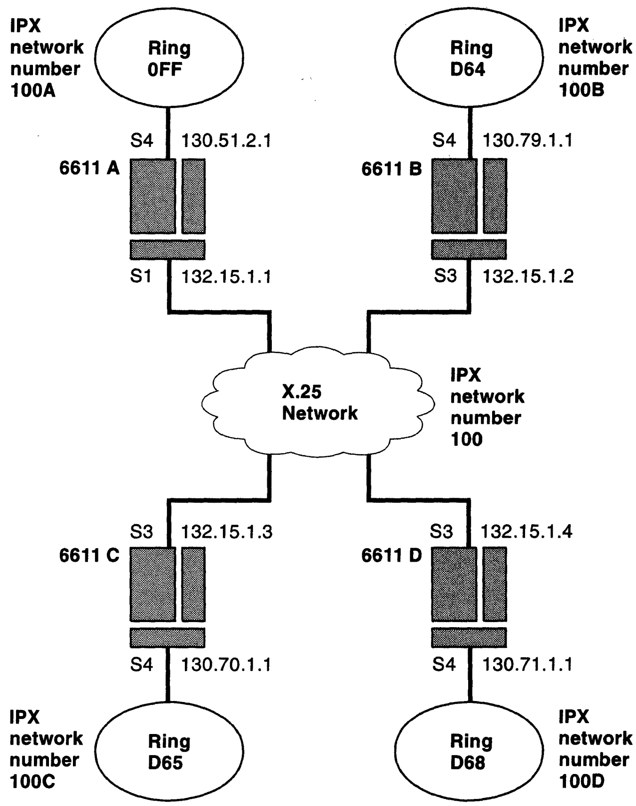


Figure 4-7. Sample X.25 Network

The sample network shows the configuration of:

- X.25 connection of routers 6611 A, 6611 B, 6611 C, and 6611 D
- IP addressing and static routes
- IPX routing
- Source route bridging on the token rings

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 4-7. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

X.25 Ports and the Protocols Running on Them

Table 4-66. X.25 Port - X.25 Port Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 1 Value	6611 C Slot 3 Value	6611 D Slot 3 Value
Enable X.25 interface on this port	Enable	Enable	Enable	Enable
Type of line	SVC	SVC	SVC	SVC
Locally administered MAC address	6611A	6611B	6611C	6611D

Table 4-67. X.25 Port - Subscription Mapping Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 1 Value	6611 C Slot 3 Value	6611 D Slot 3 Value
Local DTE address (NUA)	26240101131900	26240101130900	26240114123600	26240141010300
Country code ID	none	none	none	none
Network identifier	Telenet	Telenet	Telenet	Telenet
Lowest logical channel number for outgoing SVCs	251	251	251	251
Number of logical channels for outgoing SVCs	0	0	0	0
Lowest logical channel number for two-way SVCs	1	1	1	1
Number of logical channels for two-way SVCs	20	20	20	20
Lowest logical channel number for incoming SVCs	5	5	5	5
Number of logical channels for incoming SVCs	0	0	0	0
Lowest logical channel number for PVCs	1	1	1	1
Number of logical channels for PVCs	0	0	0	0

Table 4-68. X.25 Port - SVC Options Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 1 Value	6611 C Slot 3 Value	6611 D Slot 3 Value
SVC defaults				
Receive packet size	512	512	512	512
Transmit packet size	512	512	512	512
Receive packet window	7	7	7	7
Transmit packet window	7	7	7	7
SVC parameters				
Include calling address in call request packets	Include	Include	Include	Include
Calling address in incoming call packets	*	*	*	*
Allow incoming calls	Enable	Enable	Enable	Enable
Allow outgoing calls	Enable	Enable	Enable	Enable

Table 4-69. X.25 Port - IP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 1 Value	6611 C Slot 3 Value	6611 D Slot 3 Value
Enable IP routing on this port	Enable	Enable	Enable	Enable
IP addresss	132.15.1.1	132.15.1.2	132.15.1.3	132.15.1.4
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit	1492	1492	1492	1492
Enable ICMP address mask request	Enable	Enable	Enable	Enable

Table 4-70. X.25 Port - 6611 A X.25 Remote IP Host Parameters Configured

Parameter	6611 A Slot 3 Value 1	6611 A Slot 3 Value 2	6611 A Slot 3 Value 3
List of X.25 remote hosts			
Destination IP address for X.25	132.15.1.2	132.15.1.3	132.15.1.4
Virtual circuit type	SVC	SVC	SVC
Remote SVC address	26240101130900	26240114123600	26240141010300
Logical channel number	NA	NA	NA

Table 4-71. X.25 Port - 6611 B X.25 Remote IP Host Parameters Configured

Parameter	6611 B Slot 1 Value 1	6611 B Slot 1 Value 2	6611 B Slot 1 Value 3
List of X.25 remote hosts			
Destination IP address for X.25	132.15.1.1	132.15.1.3	132.15.1.4
Virtual circuit type	SVC	SVC	SVC
Remote SVC address	26240101131900	26240114123600	26240141010300
Logical channel number	NA	NA	NA

Table 4-72. X.25 Port - 6611 C X.25 Remote IP Host Parameters Configured

Parameter	6611 C Slot 3 Value 1	6611 C Slot 3 Value 2	6611 C Slot 3 Value 3
List of X.25 remote hosts			
Destination IP address for X.25	132.15.1.1	132.15.1.2	132.15.1.4
Virtual circuit type	SVC	SVC	SVC
Remote SVC address	26240101131900	26240101130900	26240141010300
Logical channel number	NA	NA	NA

Table 4-73. X.25 Port - 6611 D X.25 Remote IP Host Parameters Configured

Parameter	6611 D Slot 3 Value 1	6611 D Slot 3 Value 2	6611 D Slot 3 Value 3
List of X.25 remote hosts			
Destination IP address for X.25	132.15.1.1	132.15.1.2	132.15.1.3
Virtual circuit type	SVC	SVC	SVC
Remote SVC address	26240101131900	26240101130900	26240114123600

Table 4-74. X.25 Port - IPX Parameters Configured

Parameter	6611 A Slot 3	6611 B Slot 3	6611 C Slot 3	6611 D Slot 3
Enable IPX routing on this port	Enable	Enable	Enable	Enable
IPX network number	100	100	100	100
Tick override	Disable	Disable	Disable	Disable
Tick value	None	None	None	None
Split horizon for RIP and SAP updates	On	On	On	On
SAP update interval	1	1	1	1
SAP age multiplier	4	4	4	4
RIP update interval	1	1	1	1
RIP age multiplier	4	4	4	4

Table 4-75. X.25 Port - 6611 A X.25 Remote IPX Host Parameters Configured

Parameter	6611 A Slot 3 Value 1	6611 A Slot 3 Value 2	6611 A Slot 3 Value 3
List of X.25 remote hosts			
Destination IPX address for X.25	6611B	6611C	6611D
Virtual circuit type	SVC	SVC	SVC
Remote SVC address	26240101130900	26240114123600	26240141010300
Logical channel number	NA	NA	NA

Table 4-76. X.25 Port - 6611 B X.25 Remote IPX Host Parameters Configured

Parameter	6611 B Slot 1 Value 1	6611 B Slot 1 Value 2	6611 B Slot 1 Value 3
List of X.25 remote hosts			
Destination IPX address for X.25	6611A	6611C	6611D
Virtual circuit type	SVC	SVC	SVC
Remote SVC address	26240101131900	26240114123600	26240141010300
Logical channel number	NA	NA	NA

Table 4-77. X.25 Port - 6611 C X.25 Remote IPX Host Parameters Configured

Parameter	6611 C Slot 3 Value 1	6611 C Slot 3 Value 2	6611 C Slot 3 Value 3
List of X.25 remote hosts			
Destination IPX address for X.25	6611A	6611B	6611D
Virtual circuit type	SVC	SVC	SVC
Remote SVC address	26240101131900	26240101130900	26240141010300
Logical channel number	NA	NA	NA

Table 4-78. X.25 Port - 6611 D X.25 Remote IPX Host Parameters Configured

Parameter	6611 D Slot 3 Value 1	6611 D Slot 3 Value 2	6611 D Slot 3 Value 3
List of X.25 remote hosts			
Destination IPX address for X.25	6611A	6611B	6611C
Virtual circuit type	SVC	SVC	SVC
Remote SVC address	26240101131900	26240101130900	26240114123600

Token-Ring Ports and the Protocols Running on Them

Table 4-79. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 4 Value	6611 B Slot 4 Value	6611 C Slot 4 Value	6611 D Slot 4 Value
Enable interface	Enable	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA	NA
MAC address format	NA	NA	NA	NA
Token ring data rate	4 Mbps	4 Mbps	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local	Non-local	Non-local

Table 4-80. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 A Slot 4 Value	6611 B Slot 4 Value	6611 C Slot 4 Value	6611 D Slot 4 Value
Enable Source Route Bridging on this port	Enable	Enable	Enable	Enable
Spanning tree mode	Automatic	Automatic	Automatic	Automatic
Path cost	0	0	0	0
Port priority for Translational Bridging	80	80	80	80
Port state	NA	NA	NA	NA
Ring number	0FF	D44	D65	D68
Max. transmission unit	2052	2052	2052	2052

Table 4-81. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 4 Value	6611 B Slot 4 Value	6611 C Slot 4 Value	6611 D Slot 4 Value
Enable IP routing on this port	Enable	Enable	Enable	Enable
IP address	130.51.2.1	130.79.1.1	130.70.1.1	130.71.1.1
Subnet mask	255.255.0.0	255.255.0.0	255.255.0.0	255.255.0.0
Max. transmission unit (octets)	1492	1492	1492	1492
Enable ICMP address mask requests	Enable	Enable	Enable	Enable
Inbound Port Filters	Disable	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable	Disable

Table 4-82. Token-Ring Port - IPX Parameters Configured

Parameter	**6611 A Slot 4 Value**	**6611 B Slot 4 Value**	**6611 C Slot 4 Value**	**6611 D Slot 4 Value**
Enable IPX on this port	Enable	Enable	Enable	Enable
IPX network number	100A	100B	100C	100D
Encapsulation method	Token-Ring 802.5 LLC	Token-Ring 802.5 LLC	Token-Ring 802.5 LLC	Token-Ring 802.5 LLC
Tick override	Disable	Disable	Disable	Disable
Tick value	None	None	None	None
Control SAP and RIP broadcasting				
SAP update interval	1	1	1	1
SAP age multiplier	4	4	4	4
RIP update interval	1	1	1	1
RIP age multiplier	4	4	4	4
Inbound Port Filters	Disable	Disable	Disable	Disable

Table 4-83. Token-Ring Port - SNA Parameters Configured

Parameter	**6611 A Slot 4 Value**	**6611 B Slot 4 Value**	**6611 C Slot 4 Value**	**6611 D Slot 4 Value**
Enable SNA frame forwarding on this port	Enable	Enable	Enable	Enable
SAP value	00, 04	00, 04	00, 04	00, 04

Table 4-84. Token-Ring Port - NetBIOS Parameters Configured

Parameter	**6611 A Slot 4 Value**	**6611 B Slot 4 Value**	**6611 C Slot 4 Value**	**6611 D Slot 4 Value**
Forward on this port				
NetBIOS frames	Enable	Enable	Enable	Enable
NetBIOS Datagram and Datagram Broadcast messages	Enable	Enable	Enable	Enable

Node-Level Parameters Configured

Table 4-85. Node Level - Source Route Bridging Parameters Configured

Parameter	**6611 A Value**	**6611 B Value**	**6611 C Value**	**6611 D Value**
Enable Source Route Bridging	Enable	Enable	Enable	Enable
Bridge number	2	2	2	2
Enable LAN Bridging Protocol	Enable	Enable	Enable	Enable
Designated ring number	0FF	D44	D65	D68
Spanning tree parameters				
Bridge priority	8000	8000	8000	8000
Hello time	2	2	2	2
Forward delay time	15	15	15	15
Max age	20	20	20	20

Table 4-86. Node Level - DLSw Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value
Protocols forwarded by DLSw				
SNA	Enable	Enable	Enable	Enable
NetBIOS	Enable	Enable	Enable	Enable
SNA transmission bias	0	0	0	0
Maximum NetBIOS frame size	2052	2052	2052	2052
DLSw parameters				
Virtual ring segment number	DFF	DFF	DFF	DFF
Destination cache timeout	8	8	8	8
Default DLSw IP address for this 6611	130.51.2.1	130.79.1.1	130.70.1.1	130.71.1.1

Table 4-87. Node Level - DLSw Partners Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value
Accept connections from specific 6611s only	Disable	Disable	Disable	Disable
IP address of remote 6611 router	130.70.1.1	130.51.2.1	130.51.2.1	130.51.2.1
	130.71.1.1	130.70.1.1	130.71.1.1	130.70.1.1
	130.79.1.1	130.71.1.1	130.79.1.1	130.79.1.1

Table 4-88. Node Level - IPX Routing Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value
Enable IPX router	Enable	Enable	Enable	Enable
SAP Filters	Disable	Disable	Disable	Disable
RIP Router Filters	Disable	Disable	Disable	Disable
Inbound RIP Filters	Disable	Disable	Disable	Disable
Outbound RIP Filters	Disable	Disable	Disable	Disable

Port Level Worksheets

To enable the X.25 adapter to transmit and receive packets, you need to enable X.25 routing at the port level.

Use the following tables as worksheets for your port level configurations:

- X.25 Adapter Slot: n Port: n on page 4-63
- Subscription Mapping on page 4-63
- Subscription Mapping Options on page 4-64
- PVC Defaults on page 4-65
- PVC - Detail on page 4-66
- SVC Options on page 4-67
- Facilities Control on page 4-68
- Network Tuning on page 4-70

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-33 on page D-23 for a mapping of parameter names and their associated labels.

Table 4-89. Configuration Worksheet - X.25 Adapter Slot: n Port: n

Parameter Information		Your Value
Parameter	Enable X.25 interface on this port	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables the X.25 DCE. When this parameter is set to **Disable**, the X.25 adapter disconnects from the DCE and does not reconnect until set to **Enable** again.	
Parameter	Type of line	
Valid Values	DTE, back-to-back DTE	
Default Value	DTE	
Description	This parameter indicates whether the adapter is to be configured as a data terminating equipment (DTE) (normal mode of operation) or as a back-to-back DTE.	
Parameter	Locally administered MAC address (IPX only)	
Valid Values	X'0000 0000 0001' to X'FFFF FFFF FFFE'	
Default	None	
Description	This parameter specifies the MAC address assigned to this port that is used to make routing decisions for IPX.	

Table 4-90 (Page 1 of 2). Configuration Worksheet - Subscription Mapping

Parameter Information		Your Value
Parameter	Local DTE address (required)	
Valid Values	1 to 15 decimal digits	
Default Value	None	
Description	This is the address of the local data terminal equipment (DTE).	
Parameter	Country code ID	
Valid Values	Any of the country codes defined by the CCITT standard (strings of up to four digits, any characters, no spaces)	
Default	None	
Description	This parameter identifies the country in which the network is located. This identification is necessary when: • The country ID code is *not* the first three digits of the Local DTE address parameter. • The value of the Network identifier parameter is *not* set to **other private**. For more information about the values that are set by this parameter, see Appendix C on page C-1.	
Parameter	Network identifier	
Valid Values	Datex-P (0), Datapac (1), Telenet (2), DDN (3), Other public (4), Other private (5), PSS Extended Services (6)	
Default Value	Other public (4)	
Description	This parameter indicates the network to which you intend to connect. If none of the listed network identifiers correspond to your network name, select **Other public** or **Other private**.	

Table 4-90 (Page 2 of 2). Configuration Worksheet - Subscription Mapping

Parameter Information	Your Value
Logical Channel Parameters	
Parameter Lowest logical channel number for outgoing SVCs **Valid Values** 1 to 4095 **Default Value** 251 **Description** This parameter indicates the lowest-numbered logical channel that can be used for outgoing switched virtual circuits (SVCs).	
Parameter Number of logical channels for outgoing SVCs **Valid Values** 0 to 64 **Default Value** 0 **Description** This parameter indicates the maximum number of logical channels that can be used for outgoing switched virtual circuits (SVCs).	
Parameter Lowest logical channel number for two-way SVCs **Valid Values** 1 to 4095 **Default Value** 10 **Description** This parameter indicates the lowest-numbered logical channel that can be used for two-way switched virtual circuits (SVCs).	
Parameter Number of logical channels for two-way SVCs **Valid Values** 0 to 64 **Default Value** 20 **Description** This parameter indicates the number of logical channels that can be used for two-way switched virtual circuits (SVCs).	
Parameter Lowest logical channel number for incoming SVCs **Valid Values** 1 to 4095 **Default Value** 5 **Description** This parameter indicates the lowest-numbered logical channel that can be used for an incoming switched virtual circuit (SVC).	
Parameter Number of logical channels for incoming SVCs **Valid Values** 0 to 64 **Default Value** 0 **Description** This parameter indicates the number of logical channels that can be used for incoming switched virtual circuits (SVCs).	
Parameter Lowest logical channel number for PVCs **Valid Values** 1 to 4095 **Default Value** 1 **Description** This parameter indicates the lowest-numbered logical channel that can be configured as a permanent virtual circuit (PVC).	
Parameter Number of logical channels for PVCs **Valid Values** 0 to 64 **Default Value** 0 **Description** This parameter indicates the maximum number of permanent virtual circuits (PVCs) for which the link can be configured. The number depends on your network subscription.	

Table 4-91 (Page 1 of 2). Configuration Worksheet - Subscription Mapping Options

Parameter Information	Your Value
Parameter CCITT support **Valid Values** 1980, 1984 **Default Value** 1984 **Description** This parameter indicates the CCITT X.25 version of your network.	

Table 4-91 (Page 2 of 2). Configuration Worksheet - Subscription Mapping Options

Parameter Information		Your Value
Parameter	Frame window size	
Valid Values	1 to 127	
Default Value	7	
Description	This parameter indicates the window size to be used at the frame level. This is the allowable number of frames to be sent or received before waiting for an acknowledgment.	
Parameter	Frame modulo	
Valid Values	8, 128	
Default Value	8	
Description	This parameter indicates the numbering modulo used by the frame level.	
Parameter	Packet modulo	
Valid Values	8, 128	
Default Value	8	
Description	This parameter indicates the modulo to be used for packet transmission.	
Parameter	Connection mode	
Valid Values	Active, Passive	
Default Value	Active	
Description	This parameter indicates whether the 6611 initiates the link-level connection to the data circuit-terminating equipment (DCE).	
Auto-call Options		
Parameter	Auto-call unit	
Valid Values	None, Outgoing calls, Incoming calls, Two-way calls	
Default Value	None	
Description	This parameter indicates the support provided for an auto-call unit. This allows an auto-dial and auto-answer VX32 modem connected to an X.25 line to automatically dial a phone number or to accept incoming calls on this line.	
Parameter	Auto-call unit disconnection timeout	
Valid Values	0 to 255	
Default Value	0	
Description	This parameter indicates the number of seconds that elapse between the last call cleared and the line becoming disconnected. This applies only if an auto-call unit is attached.	

Table 4-92 (Page 1 of 2). Configuration Worksheet - PVC Defaults

Parameter Information		Your Value
Parameter	Receive packet size	
Valid Values	64, 128, 256, 512, 1024, 2048, 4098. Values 2048 and 4096 are allowed only if the CCITT support parameter is set to **1984**.	
Default Value	128	
Description	This parameter indicates the default receive packet size for permanent virtual circuits (PVCs).	
Parameter	Transmit packet size	
Valid Values	64, 128, 256, 512, 1024, 2048, 4098. Values 2048 and 4096 are allowed only if the CCITT support parameter is set to **1984**.	
Default Value	128	
Description	This parameter indicates the default transmit packet size for permanent virtual circuits (PVCs).	

Table 4-92 (Page 2 of 2). Configuration Worksheet - PVC Defaults

Parameter Information	Your Value
Parameter Receive packet window **Valid Values** If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31 **Default Value** 2 **Description** This parameter indicates the default receive packet window (the number of packets that can be received before an acknowledgment must be sent) on permanent virtual circuits (PVCs).	
Parameter Transmit packet window **Valid Values** If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31 **Default Value** 2 **Description** This parameter indicates the default transmit packet window (the number of packets that can be received before an acknowledgment must be sent) on permanent virtual circuits (PVCs).	
Parameter Autoreset value **Valid Values** X'00' to X'FF' **Default Value** 2 **Description** This parameter indicates whether a reset packet is sent automatically at PVC startup, for the PVC being configured. Enter **00** if you do not want a reset packet to be sent. Otherwise, enter the nonzero diagnostic code that you want to be included in the reset packet.	

Table 4-93 (Page 1 of 2). Configuration Worksheet - PVC - Detail

Parameter Information	Your Value
Parameter Logical channel number **Valid Values** The value of the Lowest PVC LCN parameter through the value of the equation ([Lowest PVC LCN] + [Number of PVCs - 1]). **Default Value** The value of the Lowest PVC LCN parameter. **Description** This parameter defines the logical channel number (LCN) of the PVC to be configured. The value must be in the range supplied by the network provider.	
Parameter Receive packet size **Valid Values** 64, 128, 256, 512, 1024, 2048, 4096. Values 2048 and 4096 are valid only if the CCITT support parameter is set to **1984**. **Default Value** 128 **Description** This parameter indicates the receive packet size for the PVC being configured.	
Parameter Transmit packet size **Valid Values** 64, 128, 256, 512, 1024, 2048, 4096. Values 2048 and 4096 are valid only if the CCITT support parameter is set to **1984**. **Default Value** 128 **Description** This parameter indicates the transmit packet size for the PVC being configured.	
Parameter Receive packet window **Valid Values** If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31 **Default Value** 2 **Description** This parameter indicates the receive packet window size for the PVC being configured.	

Table 4-93 (Page 2 of 2). Configuration Worksheet - PVC - Detail

Parameter Information		Your Value
Parameter	Transmit packet window	
Valid Values	If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31	
Default Value	2	
Description	This parameter indicates the transmit packet window size for the PVC being configured.	
Parameter	Autoreset value	
Valid Values	X'00' to X'FF'	
Default Value	00	
Description	This parameter indicates whether a reset packet is sent automatically at PVC startup, for the PVC being configured. Enter **00** if you do not want a reset packet to be sent. Otherwise, enter the nonzero diagnostic code that you want to be included in the reset packet.	

Table 4-94 (Page 1 of 2). Configuration Worksheet - SVC Options

Parameter Information		Your Value
SVC defaults		
Parameter	Receive packet size	
Valid Values	64, 128, 256, 512, 1024, 2048, 4096. Values 2048 and 4096 are valid only if the CCITT support parameter is set to **1984**.	
Default Value	128	
Description	This is the default receive packet size for switched virtual circuits (SVCs). It is used when no packet size negotiation facility is present in the call request or incoming call packet.	
Parameter	Transmit packet size	
Valid Values	64, 128, 256, 512, 1024, 2048, 4096. Values 2048 and 4096 are valid only if the CCITT support parameter is set to **1984**.	
Default Value	128	
Description	This is the default transmit packet size for switched virtual circuits (SVCs). It is used when no packet size negotiation facility is present in the call request or incoming call packet.	
Parameter	Receive packet window	
Valid Values	If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31	
Default Value	2	
Description	This parameter defines the default receive packet window size for switched virtual circuits (SVCs). This parameter is used when there is no packet window size negotiation present in the call request or incoming call packet.	
Parameter	Transmit packet window	
Valid Values	If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31	
Default Value	2	
Description	This parameter defines the default transmit packet window size for switched virtual circuits (SVCs). This parameter is used when there is no packet window size negotiation present in the call request or incoming call packet.	

Table 4-94 (Page 2 of 2). Configuration Worksheet - SVC Options

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Include calling address in call request packets Include, Do not include Include The value attached to this parameter determines if the calling address is included (Include) or not included (Do not include) when sending a call request packet.	
Parameter **Valid Values** **Default Value** **Description**	Calling address in incoming call packets *, 1 to 14 decimal digits optionally followed by an asterisk (*), 15 decimal digits. For example: * 1234* 123456789012345 If you answer with *, the incoming call packets from any remote DTE are accepted, if the incoming call passes all the other checks. If you answer with a string of decimal digits, the calling address is checked against this string of decimal digits. Placing an asterisk (*) at the end of the string indicates that any digits are acceptable in the remainder of the address. * This parameter determines if the calling DTE address present in an incoming call packet is verified. The incoming call is rejected if no match is found.	
Parameter **Valid Values** **Default Value** **Description**	Allow incoming calls Allow, Forbid Allow This parameter indicates whether incoming calls are allowed. If you forbid incoming calls, they are cleared immediately.	
Parameter **Valid Values** **Default Value** **Description**	Allow outgoing calls Allow, Forbid Allow This parameter indicates whether outgoing calls are allowed or forbidden.	

Table 4-95 (Page 1 of 3). Configuration Worksheet - Facilities Control

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Packet size negotiation facility Enable, Disable Enable Enable this parameter if you are subscribed to the packet size negotiation facility and your network supports this facility. When enabled, the packet size negotiation facility is allowed in call packets. When disabled, calls containing a packet size negotiation facility are cleared.	
Parameter **Valid Values** **Default Value** **Description**	Packet window size negotiation facility Enable, Disable Enable Enable this parameter if you subscribe to the packet window size negotiation facility. If you select **Disable**, calls containing a packet window size negotiation facility are cleared.	
Parameter **Valid Values** **Default Value** **Description**	Packet size and packet window size negotiation Validate, Negotiate Negotiate This parameter indicates whether the packet size and packet window sizes are validated or negotiated.	

Table 4-95 (Page 2 of 3). Configuration Worksheet - Facilities Control

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Reverse charging facility Enable, Disable Enable If your network supports the reverse charging facility and you are subscribed to the facility, select **Enable**. Reverse charging allows the calling DTE to charge the cost of the call to the called DTE; it is similar to a collect call in the telephone system.	
Parameter **Valid Values** **Default Value** **Description**	Allow reverse charging Allow, Forbid Allow This parameter indicates whether reverse charging can be requested in incoming calls.	
Closed User Group (CUG) Selection Facility		
Parameter **Valid Values** **Default Value** **Description**	Basic format Enable, Disable Enable If your network supports the basic format CUG selection facility and you are subscribed to this facility, select **Enable**. When this parameter is set to **Disable**, calls containing a basic format CUG selection facility are cleared. When this parameter is set to **Enable**, this facility permits the DTE to belong to 99 or fewer groups of CUGs.	
Parameter **Valid Values** **Default Value** **Description**	Extended format Enable, Disable Disable If your network supports the extended format CUG selection facility and you are subscribed to this facility, select **Enable**. When this parameter is set to **Enable**, the extended format CUG selection facility is allowed in call packets. When this parameter is set to **Disable**, calls containing an extended format CUG selection facility are cleared.	
Parameter **Valid Values** **Default Value** **Description**	CUG with OA selection facility - basic format Enable, Disable Disable If your network supports the basic format CUG with OA selection facility and you are subscribed to this facility, select **Enable**. When this parameter is set to **Enable**, this facility permits the DTE to belong to 99 or fewer CUGs and to originate virtual calls to DTEs in the open part of the network (DTEs not belonging to any CUG) and to DTEs belonging to other CUGs with the incoming access capability. When this parameter is set to **Disable**, call packets containing a CUG with OA selection in basic format are cleared.	
Parameter **Valid Values** **Default Value** **Description**	CUG with OA selection facility - extended format Enable, Disable Disable If your network supports the extended format CUG with OA selection facility and you are subscribed to this facility, select **Enable**. If this parameter is enabled, this facility permits the DTE to belong to between 100 and 9999 CUGs and to originate virtual calls to DTEs in the open part of the network (DTEs not belonging to any CUG) and to DTEs belonging to other CUGs with the incoming access capability. If this parameter is disabled, call packets containing a CUG with OA selection in extended format are cleared.	

Table 4-95 (Page 3 of 3). Configuration Worksheet - Facilities Control

Parameter Information		Your Value
Parameter	Closed user group	
Valid Values	0, 1, 2, 4, 8, 16, 32, 64	
Default Value	1	
Description	This parameter indicates the closed user group (CUG) subscription parameter setting.	

Table 4-96 (Page 1 of 2). Configuration Worksheet - Network Tuning

Parameter Information		Your Value
Frame-level Tuning		
Parameter	N2 counter	
Valid Values	1 to 255	
Default Value	20	
Description	This parameter indicates the maximum number of times a frame can be transmitted under error conditions. This is the X.25 N2 value.	
Parameter	T1 timer	
Valid Values	1 to 255	
Default Value	60 (3 seconds)	
Description	This parameter indicates the time (in units of 50 milliseconds) after which, if it has not been acknowledged, a frame is retransmitted. This is the X.25 T1 value.	
Parameter	T4 timer	
Valid Values	4 to 255	
Default Value	180 (3 minutes)	
Description	This parameter indicates the time (in seconds) after which, if there has been no activity on a link, a receive ready (RR) frame is sent. Frame-level recovery is started if no answer is received within the T1 time frame.	
Packet-level Tuning		
Parameter	Maximum number of clear packets	
Valid Values	0 to 127	
Default Value	2	
Description	This parameter indicates how many clear packets can be sent consecutively before the virtual circuit is considered to have failed. This is the R23 counter.	
Parameter	Maximum number of reset packets	
Valid Values	0 to 127	
Default Value	2	
Description	This parameter indicates the number of reset packets that can be sent consecutively before the virtual circuit is considered to have failed. This is the R22 counter.	
Parameter	T24 timer	
Valid Values	0 to 255. 0 disables the T24 timer.	
Default Value	180	
Description	This parameter defines a time frame (in seconds). Within this time frame, an RR packet must be sent following the transmission of a packet requesting an acknowledgment.	

Table 4-96 (Page 2 of 2). Configuration Worksheet - Network Tuning

Parameter Information		Your Value
Parameter	T25 timer	
Valid Values	0 to 255. 0 disables the T25 timer.	
Default Value	180	
Description	This parameter indicates the elapsed time in seconds. Within this time period, if an acknowledgment has been received, a packet is retransmitted. This packet is equivalent to the T1 timer.	
Physical-level Tuning		
Parameter	Startup counter	
Valid Values	1 to 255	
Default Value	11	
Description	This parameter indicates the number of tests after which the attempted physical-level connection is considered to have failed.	
Parameter	Poll timer	
Valid Values	10 to 255	
Default Value	10	
Description	This parameter indicates the time (in units of 50 milliseconds) that elapses between each poll of the physical level.	

Chapter 5. Configuring Protocols

This section provides information about the protocols supported by the 6611 and how to configure these protocols. The protocols are grouped as follows:

Each protocol description contains the following information:

Port Types Supported This table illustrates the port types that are supported for the protocol that is routed, bridged, or data link switched by the 6611.

Restrictions This section lists restrictions for configuring the protocol.

Configuration Changes Some of the IBM 6611 configuration parameters can be changed dynamically and do not require a machine restart. This section lists the changes that:

- Require the specific function to restart
- Require the 6611 to restart

Configuration Options This table lists the steps for creating a basic configuration for this protocol, and lists additional configuration options.

Configuration Verification Checklist This checklist helps you verify that two 6611s are correctly configured to perform bridging or routing.

Sample Network Graphic This section includes an illustration of a sample network. The information contained in these examples is presented as is and without warranty.

Summary of All Customized Parameters in Sample This section includes tables that show the values that you configure to enable the protocols to run on the sample network. A value of NA indicates that a parameter is not applicable to the configuration.

Port Level Worksheets This section contains worksheets to be used when configuring the function at the port level. The values on each worksheet correspond to the values displayed on the window of the Configuration Program that is identified by the title of the worksheet.

Node Level Worksheets This section contains worksheets to be used when configuring the function at the node level. The values on each worksheet correspond to the values displayed on the window of the Configuration Program that is identified by the title of the worksheet.

Source Route Bridging

The 6611 supports local and remote source route bridging of all network protocols. Table 5-1 describes the various ways in which source route bridging can be configured on the 6611.

Table 5-1. Source Route Bridging Configurations on the 6611

Configuration	Description
Local source route bridging	The bridging of frames between token-ring LANs directly attached to the same 6611. The 6611 is defined as a source route bridge at the node level.
Remote source route bridging	The bridging of frames between token-ring LANs attached to separate 6611s. Remote source route bridging is supported over a telecommunications link or frame relay network. The 6611 is defined as a source route bridge at the node level and is remotely connected to either another source route bridge or a *translational bridge*. **Note:** This configuration is sometimes referred to as *native mode* bridging.
Remote source route bridging using the LAN Bridging Protocol	The bridging of frames between a 6611 and a PS/2 running either the IBM Token-Ring Network Bridge Program (Version 2.2.4 or higher) or the IBM Remote Token-Ring Bridge/DOS (Version 1.0.1 or higher). The 6611 uses a proprietary telecommunications link protocol to communicate with the PS/2 workstation running the bridge program. The protocol is called the LAN Bridging Protocol. Frames can be exchanged between a 6611 serial port configured to use the LAN Bridging Protocol and any token-ring or serial port on the 6611 configured for source route bridging. **Note:** This configuration is sometimes referred to as *compatibility mode* bridging.
Translational bridging	The bridging of frames between Ethernet and token-ring LANs. When the 6611 is defined as a translational bridge at the node level, frames are bridged between ports that have source route bridging enabled and those that have transparent bridging enabled. If the origin and destination ports use the same bridging scheme, frames are bridged without translation. If the origin and destination ports use different bridging schemes, frames are translated into the proper format and then bridged. See "Translational Bridging" on page 5-75 for more information on this bridging method.
Dual mode bridging	The recommended method for remotely connecting two 6611s configured as translational bridges. When dual mode bridging is configured on both ends of a serial link, frames originating from a LAN port configured for source route bridging are translated only if the destination LAN on the remote 6611 requires a different MAC frame format. See "Translational Bridging" on page 5-75 for more information on dual mode bridging.

Port Types Supported

Table 5-2. Port Types Supported for Source Route Bridging

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	
	IEEE 802.3	LLC	
		SNAP	
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	√
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	

Restrictions

- The source and destination end stations for bridged frames must be on token-ring LANs unless translational bridging is configured.
- When you configure the 6611 as a source route bridge, the bridge must contain at least one enabled source route bridge port with a MAC address. This condition can be met in one of two ways:
  1. By enabling source route bridging on a token-ring port. Each token-ring port has a universally or locally defined MAC address.
  2. By enabling source route bridging on a serial port and configuring the Locally administered MAC address parameter for the serial port's physical interface. (See "Serial Port and V.35/V.36 Serial Port" on page 4-2.) If all of the bridge ports are serial ports, this step is required.

  The 6611 uses the MAC address to generate a bridge identifier for the source route bridge. The bridge identifier is used by the spanning tree algorithm for the source route bridge network.
- The largest transmission unit (LLC PDU) that can be bridged on serial ports using PPP or the LAN Bridging Protocol is 2052 octets.
- When defining source route bridging on a serial port using frame relay, you need to specify at least one data link connection identifier (DLCI) that will be used to transmit bridged frames over the frame relay network. The source route bridging protocol cannot use frame relay's InARP protocol to acquire DLCI numbers dynamically. Each DLCI you define must also be associated with a ring number, which uniquely identifies the frame-relay connection.

  In addition, once you define DLCIs for the bridging protocol, you must explicitly define DLCIs for *all other* protocols running on the same port. First, configure the frame-relay protocol by defining a list of DLCIs assigned to the serial port. Then as you define individual protocols on the port, specify which DLCIs are available for use by each protocol.

Configuration Changes...

That Require the Source Route Bridging Function to Restart

- All node and port-level source route bridging parameters
- Enable LNM communication through this port

That Require the 6611 to Restart

When bridging is configured on a serial port using frame relay, changes to most of the bridging parameters on the frame relay port will cause the 6611 to restart.

Before You Configure...

This section contains additional information to assist you in configuring the source route bridging protocol.

When Are Token-Ring Frames Bridged?

When you configure source route bridging on a token-ring port, the bridge examines each frame received to determine whether the network protocol encapsulated within the frame should be bridged or routed. If the network protocol has been configured for routing and the protocol is denied from being bridged by an inbound source route bridge SAP or SNAP filter, the frame is routed. If the network protocol has not been configured for routing or is not denied by an inbound SAP or SNAP filter, the frame is bridged. When a protocol is not configured for routing, and bridging is disabled, the 6611 discards any packets received for that particular protocol.

On a serial port, a frame received as an encapsulated token-ring packet cannot be routed. If source route bridging is enabled on the port, the frame is bridged. Otherwise, the 6611 discards the frame.

For more information on how the 6611 determines whether to bridge or route a specific frame, refer to the source route bridging description in the *Introduction and Planning Guide*.

Defining Source Route Bridge Port Filters

The source route bridging function on the 6611 provides a set of filters that enables you to control the type of traffic being bridged over a port. Each of the filters can be used to evaluate a different portion of a token-ring frame. When the filters are applied to a frame, the values specified for the filters are compared against the contents of the frame. The result of these comparisons determines whether the frame is rejected or bridged.

The use of bridge filters is optional. However, the source route bridging function does provide three default Source SAP filters that are enabled automatically when a token-ring port is enabled for bridging. "Default Source SAP Filters" on page 5-7 describes the purpose of these filters. Table 5-3 on page 5-6 shows each of the filter types supported by the source route bridging function.

Table 5-3. Source Route Bridge Port Filters

This Filter Type...	Is Compared to...
Hop count	The current hop count recorded within a token-ring frame.
Source SAP	The source service access point (SSAP) field in a token-ring frame. The field is located in frame's logical link control (LLC) protocol data unit. The source SAP identifies the network protocol encapsulated within the frame.
SNAP value	The subnetwork access protocol (SNAP) header in a token-ring frame in which the SSAP field is set to X'AA'. The filter evaluates the Type field within the SNAP header, which identifies the non-IEEE network protocol encapsulated within the frame.
RI field	The routing information (RI) field within a token-ring frame. The filter evaluates the first or next-to-last route designator within the RI field or all route designators. Each route designator consists of a ring and bridge number pair that represents a single hop within a specific route.
MAC address	The source and destination MAC address fields in a token-ring frame.
Sliding window	Any portion of a token-ring frame, as defined by the filter.

Note: Refer to the source route bridging description in the *Introduction and Planning Guide* for an illustration of the token-ring frame format. See Appendix B on page B-1 for a list of common SAPs.

Each port filter, except for the Hop count filter, can be defined as an *inbound* filter or an *outbound* filter. Inbound filters are applied to frames flowing into the bridge port from a LAN segment or link. Outbound filters are applied to frames flowing out of the bridge port onto a LAN segment or link.

Note: The Hop count filter is an inbound filter only.

When a filter is applied to a frame, the outcome is based on one or more of the following criteria, depending on the type of filter chosen:

- Whether the Filtering mode parameter is set to **Permit** or **Deny**. Permit filters allow frames to pass through the port if the contents of the filter and the frame match. Deny filters do not allow frames to pass through the port if the contents of the filter and the frame match.
- Whether the filter is applied to single-route broadcast frames, all-routes broadcast frames, or both types. All source route bridge filters, except for the SNAP value filter, apply to broadcast frames only.
- Whether a *mask* has been specified for the contents of the filter. A mask value can expand the range of the filter to increase the likelihood that a match will occur. (See "Using Mask Values in Filters" on page 5-8 for more information.)

You can define and enable multiple filters on each port. When more than one type of filter is defined and enabled on a bridge port, the filter types are applied in a pre-defined order (as described in the next section). Table 5-4 on page 5-7 summarizes the algorithm used by the 6611 bridge when applying port filters. Port filters are applied in sequence until the frame is rejected or until, after having passed through each filter, the frame is bridged.

Table 5-4. Algorithm Used for Bridge Port Filters

A Filter with Filtering Mode of...	Applied with This Result...	Yields This Outcome...
Deny	Filter and frame contents match	Frame is rejected; no other filters are applied to it.
Deny	Filter and frame contents do not match	Frame is passed to the next filter
Permit	Filter and frame contents match	Frame is passed to the next filter
Permit	Filter and frame contents do not match	Frame is rejected; no other filters are applied to it.

Filtering Example: Suppose the following Deny filters are defined for a port: inbound source SAP filter, X'E0' (to filter IPX frames); and inbound MAC address filters, MAC A and MAC B. By default, the source SAP filter would be applied first. If an inbound frame contained a source SAP value of X'E0', the frame would be rejected by the port. If, however, the frame contained a different source SAP value, the inbound MAC address filters would be applied next in the order in which they were defined in the Configuration program.

If, in the previous example, the source SAP filter were a Permit filter, the outcome would be reversed. If the inbound frame contained a source SAP value of X'E0', the frame would be permitted and the MAC address filters would be applied to the frame. If the inbound frame contained a different source SAP value, the frame would be rejected by the port before the other filters were applied.

Default Source SAP Filters

The source route bridging function on the 6611 provides three inbound source SAP filters that are enabled automatically when a token-ring port is enabled for bridging:

- X'AA' — SNAP
- X'BC' — VINES
- X'E0' — IPX

These filters are configured, by default, as Deny filters. The purpose of the filters is to automatically route network protocols if the same port has been configured for both source route bridging and routing. Frames with denied SAP values will be routed if the encapsulated protocol has been enabled for routing on the port.

Defining the Order of Port Filters

The order in which different types of filters are applied can affect the performance of the source route bridge. As a rule, filter types should be applied in the order in which they are most likely to be effective. The result is that the majority of unwanted traffic is discarded in the shortest amount of time, freeing buffer space to accommodate more traffic.

The node-level parameters for source route bridging enable you to define the order in which inbound and outbound filters should be applied on all 6611 ports configured for source route bridging. The default order, by filter type, is:

1. Hop count filter
2. Source SAP filters
3. SNAP value filters

4. RI field filters
5. MAC address filters
6. Sliding window filters

Notes:

1. The default filter order reflects the order that is likely to be most effective in a typical bridged network. The optimal order, however, depends upon the configuration of your network and your specific filtering requirements.
2. When configuring a translational bridge, you can specify the order in which filters should be applied on both source route bridge and transparent bridge ports on the 6611.

If the default filter order is not appropriate for a specific port, you have the option of overriding the default and reordering the filters on that port. For example, suppose you want to define the following port filters:

- A SNAP value filter to deny all IP frames
- A MAC address filter to deny all frames from a specific MAC address.

In this scenario, IP frames represent the majority of the traffic that must be filtered out. By applying SNAP value filters first, you ensure that the largest percentage of unwanted traffic will be discarded in the shortest amount of time. MAC address filters should be applied second because this filter type is expected to filter out a smaller percentage of traffic.

Using Mask Values in Filters

The following source route bridge filters enable you to use mask values to increase the effectiveness of the filter:

- SNAP value
- RI field
- MAC address
- Sliding window

When you specify a value to be used by a filter, such as a MAC address, that value is compared to the corresponding value in an inbound or outbound frame. A mask value identifies the bits in the filter value that are to be treated as significant. Each bit in the mask corresponds to an identical bit in the filter value. For every bit set to one in the mask, the same bit in the filter value is treated as significant. When the filter is applied, it compares the significant bits in the filter value against the corresponding bits in an inbound or outbound frame. The result of this comparison is determined by the Filtering mode parameter. Frames that correspond to the significant bits in the filter value are either allowed, if the filtering mode is **Permit**, or rejected, if the filtering mode is **Deny**.

In the following example, the filter value is X'FFC1' and the mask for that value is X'FFC1'. The example shows the significant bit positions identified by the mask.

```
Filter value:            X'FFC1' =  B'1111 1111 1100 0001'
Mask:                    X'FFC1' =  B'1111 1111 1100 0001'
Significant bits (X):                 XXXX XXXX XX-- ---X
```

If a mask was not used in the example, the filter could permit or deny only frames containing the value X'FFC1'. By using a mask, the range of the filter is extended to permit or deny all frames with odd number values between X'FFC1' and X'FFFF':

```
X'FFC1' = B'1111 1111 1100 0001'    X'FFD1' = B'1111 1111 1101 0001'
X'FFC3' = B'1111 1111 1100 0011'    X'FFD3' = B'1111 1111 1101 0011'
X'FFC5' = B'1111 1111 1100 0101'    X'FFD5' = B'1111 1111 1101 0101'
X'FFC7' = B'1111 1111 1100 0111'    X'FFD7' = B'1111 1111 1101 0111'
X'FFC9' = B'1111 1111 1100 1001'    X'FFD9' = B'1111 1111 1101 1001'
X'FFCC' = B'1111 1111 1100 1011'    X'FFDC' = B'1111 1111 1101 1011'
X'FFCE' = B'1111 1111 1100 1101'    X'FFDE' = B'1111 1111 1101 1101'
X'FFCF' = B'1111 1111 1100 1111'    X'FFDF' = B'1111 1111 1101 1111'

X'FFE1' = B'1111 1111 1110 0001'    X'FFF1' = B'1111 1111 1111 0001'
X'FFE3' = B'1111 1111 1110 0011'    X'FFF3' = B'1111 1111 1111 0011'
X'FFE5' = B'1111 1111 1110 0101'    X'FFF5' = B'1111 1111 1111 0101'
X'FFE7' = B'1111 1111 1110 0111'    X'FFF7' = B'1111 1111 1111 0111'
X'FFE9' = B'1111 1111 1110 1001'    X'FFF9' = B'1111 1111 1111 1001'
X'FFEC' = B'1111 1111 1110 1011'    X'FFFC' = B'1111 1111 1111 1011'
X'FFEE' = B'1111 1111 1110 1101'    X'FFFE' = B'1111 1111 1111 1101'
X'FFEF' = B'1111 1111 1110 1111'    X'FFFF' = B'1111 1111 1111 1111'
```

Note: Bits that are not significant are ignored by the filter. When a mask of all 0s is used, no bits are considered significant; therefore no filtering occurs. When a mask of all 1s is used, all bits are considered significant; therefore only the value specified for the filter is permitted or denied by the filter.

Configuration Options

Each token-ring LAN is attached to the 6611 by means of a token-ring network 16/4 adapter or serial/token-ring combination adapter. When configuring the 6611 as a source route bridge, the source route bridging function must be configured at the node level and on each token-ring port over which frames will be bridged. In addition, source route bridging needs to be configured on each serial port connected to a remote source route bridge or translational bridge.

Note: To perform remote transparent bridging, you must select either PPP or frame relay as the frame encapsulation method for the serial port.

When configuring the 6611 as a translational bridge, the translational bridging function must be configured at the node level. Source route bridging is configured on each token-ring port over which frames will be bridged. When remotely bridging token-ring frames between the translational bridge and another 6611 bridge, the configuration of the serial port depends upon how the remote bridge is being defined. If the remote bridge is a translational bridge, it is recommended that dual mode bridging be defined on each end of the serial link. Otherwise, source route bridging should be defined on each end of the link.

Table 5-5 on page 5-10 summarizes the configuration options for source route bridging.

Table 5-5. Source Route Bridging Configuration Options

<table>
<tr><th>WHEN configuring Source Route Bridging...</th><th>THEN optionally...</th></tr>
<tr><td>...on a token-ring port, or serial port using PPP or the LAN Bridging Protocol:
Enable source route bridging on the port.
For a token-ring port, specify the ring number of the token-ring network attached to the port.
For a serial port using PPP, specify a unique ring number that represents the serial link.
For a serial port using the LAN Bridging Protocol, specify the ring number of the ring attached to the remote PS/2 bridge.</td><td>Specify how the port state is determined (automatically by the spanning tree algorithm or manually set). The source route bridge network uses a spanning tree to control the forwarding single-route broadcast frames through the network.
If the spanning tree mode is set to Automatic, specify the path cost. The port priority is for translational bridging only.
If the spanning tree mode is set to Manual, specify whether the port is disabled or in the forwarding state.
Specify the maximum transmission unit size.
Define source route bridge port filters. The filters are accessed through a separate push button on the port window.</td></tr>
<tr><td>...on a serial port using frame relay:
Enable source route bridging on the port.
Pair the DLCIs that will be used by the 6611 for remote bridging over a frame relay network with specific ring numbers. The ring numbers represent token-ring networks attached to the 6611.

Note: You need to assign a set of DLCIs to the frame-relay port before specifying the DLCIs that may be used for source route bridging. You assign DLCIs when defining the frame-relay protocol on the port.</td><td>Specify how the port state is determined (automatically by the spanning tree algorithm or manually set). The source route bridge network uses a spanning tree to control the forwarding single-route broadcast frames through the network.
If the spanning tree mode is set to Automatic, specify the path cost. The port priority is for translational bridging only.
If the spanning tree mode is set to Manual, specify whether the port is disabled or in the forwarding state.
Specify the maximum transmission unit size.
Define source route bridge port filters. The filters are accessed through a separate push button on the port window.</td></tr>
<tr><td>...at the node level:
Enable source route bridging if the 6611 is being configured as a source route bridge. (If the 6611 is being configured as a translational bridge, see "Translational Bridging" on page 5-75.)
Specify the bridge number of the 6611.
If any serial ports on the 6611 use the LAN Bridging Protocol to remotely attach to a PS/2 bridge, specify a designated ring number for the 6611. The designated ring number can be the ring number of any 6611 port configured for source route bridging, except a LAN Bridging Protocol port. If your configuration does not require the LAN Bridging Protocol, disable the Enable LAN Bridging Protocol parameter.</td><td>Specify spanning tree parameters:
Bridge priority
Hello time
Forward delay
Max age
Change the order in which port filters are applied.</td></tr>
</table>

Note: The source route bridging function provides three inbound source SAP filters, X'AA', X'BC', and X'E0', that are enabled automatically when a token-ring port has been enabled for bridging. These Deny filters cause network protocols to be routed when the port has been configured for both source route bridging and routing. Frames with denied SAP values will be routed if the encapsulated protocol has been enabled for routing on the port.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform source route bridging. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-6 (Page 1 of 2). Source Route Bridging Configuration Verification Checklist

Source Route Bridging Rule	**Configuration Parameter**	√
Node-Level Parameters:		
Ensure that the Enable source route bridging parameter is enabled.	Enable Source Route Bridging	
Port-Level Parameters:		
Ensure that the Enable source route bridging on this port parameter is enabled on at least two ports on each 6611.	Enable Source Route Bridging on this port	
For a connection between two token-ring ports, ensure that the Enable physical interface parameter is enabled, and following parameters are set to the same value on both 6611s: • Enable physical interface on this port • Token-ring data rate • Data encoding • Framing method	Enable physical interface on this port	
	Token-ring data rate	
	Data encoding	
	Framing method	
For a connection between two serial frame-relay ports, ensure that the value of the frame relay Ring number parameter is the same on each 6611. For a connection between two token-ring ports, ensure that the value of the Ring number parameter is the same.	Ring number (frame relay)	
	Ring number (token ring)	
When there is more than one source route bridging connection between two routers and at least one port has the Enable forwarding of single-route broadcast frames parameter enabled, ensure that all of the ports on this 6611 do not have the Spanning tree mode parameter set to **Manual**.	Enable forwarding of single-route broadcast frames	
	Spanning tree mode	
Ensure that source route bridging is enabled on at least one token-ring on the 6611 and that the physical interface on that port is enabled. If all ports on 6611 are serial ports, each port that performs source route bridging in the network must have a unique sourec route bridging priority.	Enable physical interface on this port	
	Enable Source Route Bridging on this port	
	Bridge priority	
For serial and token-ring source route bridging connections:		
When inbound or outbound source SAP filters are set with the **Deny** option, the list of SAP filters must not contain SAP 00 or the SAP for any protocols to be bridged through that interface.	Enable inbound (outbound) SAP filters on this port	
When inbound or outbound source SAP filters are set with the **Permit** option, the list of SAP filters must contain SAP 00 and the SAP for any protocol to be bridged through that interface.	Filtering mode	
	Source SAP value inbound (outbound)	

Table 5-6 (Page 2 of 2). Source Route Bridging Configuration Verification Checklist

Source Route Bridging Rule	**Configuration Parameter**	√
When inbound or outbound SNAP value filters are set with the **Deny** option, the list must not contain values and masks that block the protocols to be bridged. When inbound or outbound SNAP value filters are set with the **Permit** option, the list must contain the SNAP values and masks that allow the intended protocols to be bridged.	Enable inbound (outbound) SNAP filters on this port	
	Filtering mode	
	SNAP value inbound (outbound)	
	SNAP value mask inbound (outbound)	
When inbound or outbound MAC address filters are set with the **Deny** option, the list must not contain addresses and masks that block the devices intended to communicate. When inbound or outbound MAC address filters are set with the **Permit** option, the list must contain addresses and masks that allow the devices intended to communicate.	Enable inbound (outbound) MAC Address Filters on this port	
	Filtering mode	
	Source MAC address in (out), Destination MAC address in (out)	
	Source MAC address mask in (out), Destination MAC address mask in (out)	
When inbound or outbound RI field filters are set with the **Deny** option, the list must not contain the bridge number of the other router or the ring number of a port on the other router that is configured for SRB. This assumes that the two ports are intended to communicate. When inbound or outbound RI field filters are set with the **Permit** option, the list must contain the bridge number of the other router or the ring number of a port on the other router that is configured for SRB. This assumes the 2 ports are intended to communicate.	Enable inbound (outbound) RI field filters on this port	
	Filtering mode	
	Route designator inbound (outbound)	
	Ring number inbound (outbound)	
	Bridge number inbound (outbound)	
When hop count filters are configured, they must be set so that the intended traffic is not blocked.	Hop count filter	

Sample Network Graphic

Figure 5-1 shows two 6611s (6611 A and 6611 B) that are configured to transport SNA using source route bridging.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running PPP, IP, Hello, and source route bridging
  - A token-ring port running IP, Hello, and source route bridging
- 6611 B, which has the following port types and protocols running:
  - A serial port running PPP, IP, Hello, and source route bridging
  - A token-ring port running IP, Hello, and source route bridging

The following information is shown in Figure 5-1:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

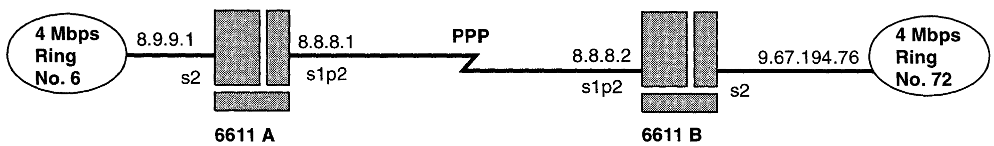


Figure 5-1. Sample Network for Bridging SNA over Serial Ports

The sample network shows the configuration for:

- Source route bridging of SNA
- Serial and token-ring ports

Note: The configuration of the IP protocol is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to bridge frames.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-1. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and the Protocols Running on Them

Table 5-7. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-8. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table 5-9. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-10. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-11. Serial Port - Source Route Bridging Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Source Route Bridging on this port	Enable	Enable
Spanning tree mode	Automatic	Automatic
Path cost	0	0
Port priority for Translational Bridging	80	80
Port state	NA	NA
Ring number	101	101
Max. transmission unit (octets)	2052	2052

Token-Ring Ports and the Protocols Running on Them

Table 5-12. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-13. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable Source Route Bridging on this port	Enable	Enable
Spanning tree mode	Automatic	Automatic
Path cost	0	0
Port priority for Translational Bridging	80	80
Port state	NA	NA
Ring number	6	72
Max. transmission unit (octets)	2052	2052

Table 5-14. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.9.9.1	9.67.194.76
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Disable	Disable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-15. Node Level - Source Route Bridging Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Source Route Bridging	Enable	Enable
Bridge number	4	4
Enable LAN Bridging Protocol	Enable	Enable
Designated ring number	6	72
Spanning tree parameters		
Bridge priority	8000	8000
Hello time	2	2
Forward delay	15	15
Max age	20	20

Port Level Worksheets

Figure 5-2 and Figure 5-3 on page 5-17 show the paths for configuring source route bridging and source route bridge filters through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-2 and Figure 5-3 on page 5-17.

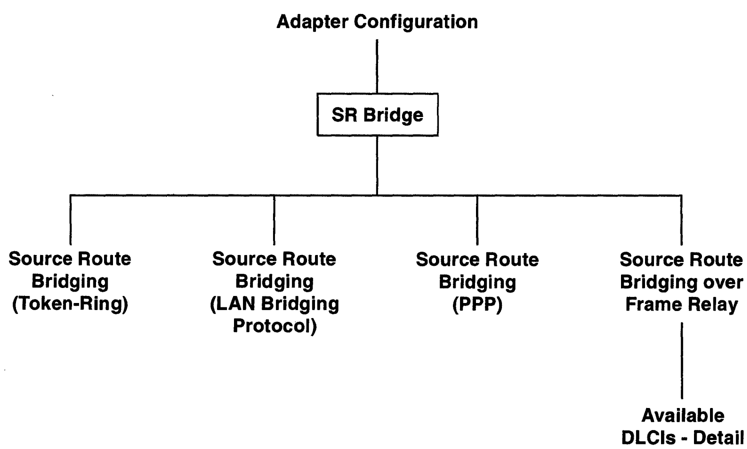


Figure 5-2. Flow of Port-Level Source Route Bridge Windows

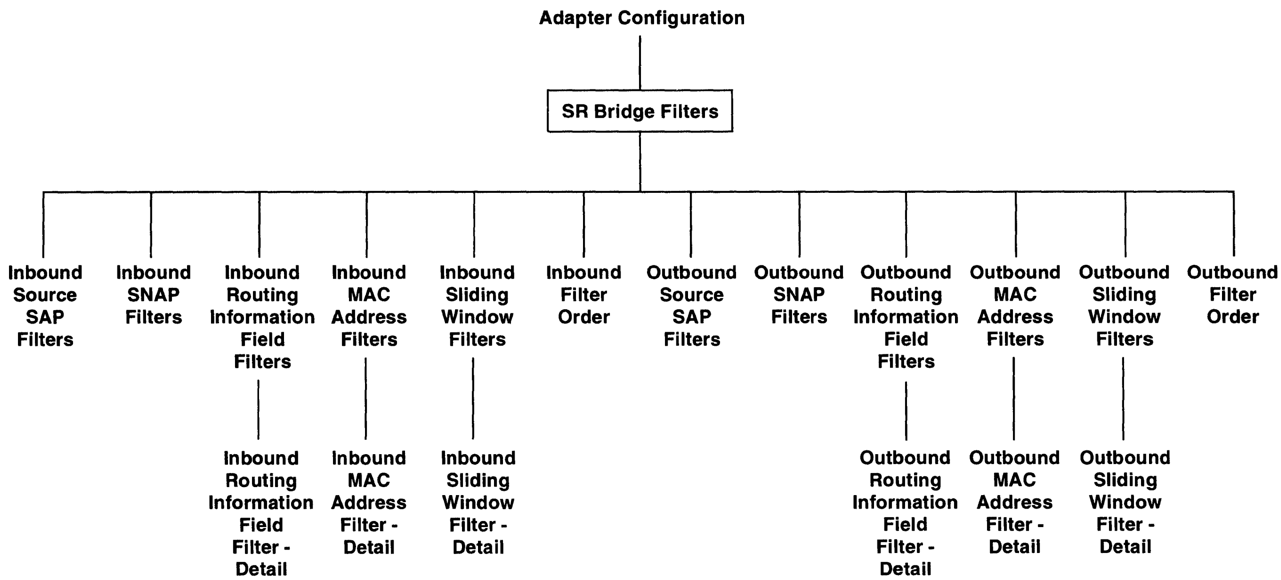


Figure 5-3. Flow of Port-Level Source Route Bridge Filter Windows

Use the following tables as worksheets to configure source route bridging at the port level:

- Source Route Bridging - Token-Ring Port on page 5-17
- Source Route Bridging - Serial Port (LAN Bridging Protocol) on page 5-19
- Source Route Bridging - Serial Port (PPP) on page 5-21
- Source Route Bridging - Serial Port (Frame Relay) on page 5-22

- Source Route Bridge Filters on page 5-24
- Inbound Source SAP Filters on page 5-24
- Inbound SNAP Filters on page 5-25
- Inbound Routing Information Field Filters on page 5-26
- Inbound MAC Address Filters on page 5-28
- Inbound Sliding Window Filters on page 5-29
- Inbound Filter Order on page 5-31

- Outbound Source SAP Filters on page 5-32
- Outbound SNAP Filters on page 5-32
- Outbound Routing Information Field Filters on page 5-33
- Outbound MAC Address Filters on page 5-35
- Outbound Sliding Window Filters on page 5-36
- Outbound Filter Order on page 5-38

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-6 on page D-7 for a mapping of parameter names and their associated labels.

Table 5-16 (Page 1 of 3). Configuration Worksheet - Source Route Bridging (Token-Ring Port)

Parameter Information		Your Value
Parameter	Enable Source Route Bridging on this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables source route bridging on the port.	

Table 5-16 (Page 2 of 3). Configuration Worksheet - Source Route Bridging (Token-Ring Port)

Parameter Information		Your Value
Parameter	Spanning tree mode (see table note)	
Valid Values	Automatic, Manual	
Default Value	Automatic	
Description	This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually configured. When **Automatic** is selected, the spanning tree determines the port state using information provided by the Path cost parameter. When **Manual** is selected, you can control the state of the port by configuring the Port state parameter.	
Parameter	Path cost	
Valid Values	0 to 65535	
Default Value	0 (cost calculated automatically)	
Description	When the Spanning tree mode parameter is set to **Automatic**, this parameter specifies the contribution of the port to the total cost of a path to the root bridge. For a value of zero, the path cost is calculated using the formula: 1000 / (media speed in Mbps) The media speed used for token ring is 4 Mbps or 16 Mbps, depending on the ring speed you select.	
Parameter	Port priority for Translational Bridging	
Valid Values	X'00' to X'FF', where X'00' is the *highest* priority value and X'FF' is the *lowest* priority value	
Default Value	X'80'	
Description	When you configure the 6611 as a translational bridge, this parameter specifies the priority of the bridge port. The port priority is used to select the *preferred port* when: • Two or more translational bridge ports are connected to the same LAN segment in a redundant configuration. (The spanning tree allows a path through only one of the ports.) • Two or more translational bridge ports have equal path costs to the root bridge and represent paths through the same *designated bridge*. The designated bridge is the next-closest bridge to the root bridge. If ports have equal priorities, then the port with the lowest port number is the preferred port. Port numbers are assigned automatically by the 6611.	
Parameter	Port state	
Valid Values	Forwarding, Disabled	
Default Value	Forwarding	
Description	When the Spanning tree mode parameter is set to **Manual**, this parameter specifies the port state. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames. When the 6611 is configured as source route bridge, the port state determines whether the port will forward single-route broadcast frames. When the 6611 is configured as a translational bridge, the port state determines whether the port will forward *both* single-route and all-routes broadcast frames. **Note:** When this parameter is set to **Forwarding**, it overrides the port state that would have been selected by the spanning tree algorithm. Because the spanning tree algorithm cannot automatically disable the port, you must ensure that the port does not cause a loop in the network when it is in the forwarding state.	

Table 5-16 (Page 3 of 3). Configuration Worksheet - Source Route Bridging (Token-Ring Port)

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Ring number (required) X'001' to X'FFF' None This parameter specifies a ring number that uniquely identifies the token ring attached to the port within the bridged network.	
Parameter **Valid Values** **Default** **Description**	Maximum transmission unit For a 4 Mbps token-ring port: 516, 1500, 2052, or 4472 octets. For a 16 Mbps token-ring port: 516, 1500, 2052, 4472, 8144, 11 407, or 17 800 octets. 2052 This parameter specifies the size of the largest transmission unit that the bridge can transmit and receive on a token-ring port. The transmission unit is the logical link control (LLC) PDU in the frame.	

Table 5-17 (Page 1 of 2). Configuration Worksheet - Source Route Bridging (Serial Port - LAN Bridging Protocol)

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable source route bridging on this port Enable, Disable Disable This parameter enables or disables source route bridging on the port.	
Parameter **Valid Values** **Default Value** **Description**	Spanning tree mode Automatic, Manual Automatic This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually configured. When **Automatic** is selected, the spanning tree determines the port state using information provided by the Path cost parameter. When **Manual** is selected, you can control the state of the port by configuring the Port state parameter.	
Parameter **Valid Values** **Default Value** **Description**	Path cost 0 to 65 535 0 When the Spanning tree mode parameter is set to **Automatic**, this parameter specifies the contribution of the port to the total cost of a path to the root bridge. For a value of zero, the path cost is calculated using the formula: 800 + (1.536000 / (media speed in Mbps)) This formula results in a minimum path cost of 800 and is the formula used by the bridge program running on the PS/2 workstation.	

Table 5-17 (Page 2 of 2). Configuration Worksheet - Source Route Bridging (Serial Port - LAN Bridging Protocol)

Parameter Information		Your Value
Parameter	Port priority for translational bridging	
Valid Values	X'00' to X'FF', where X'00' is the *highest* priority value and X'FF' is the *lowest* priority value	
Default Value	X'80'	
Description	When you configure the 6611 as a translational bridge, this parameter specifies the priority of the bridge port. The port priority is used to select the *preferred port* when: • Two or more translational bridge ports are connected to the same LAN segment in a redundant configuration. (The spanning tree allows a path through only one of the ports.) • Two or more translational bridge ports have equal path costs to the root bridge and represent paths through the same *designated bridge*. The designated bridge is the next-closest bridge to the root bridge. If ports have equal priorities, then the port with the lowest port number is the preferred port. Port numbers are assigned automatically by the 6611.	
Parameter	Port state	
Valid Values	Forwarding, Disabled	
Default Value	Forwarding	
Description	When the Spanning tree mode parameter is set to **Manual**, this parameter specifies the port state. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames. When the 6611 is configured as source route bridge, the port state determines whether the port will forward single-route broadcast frames. When the 6611 is configured as a translational bridge, the port state determines whether the port will forward *both* single-route and all-routes broadcast frames. **Note:** When this parameter is set to **Forwarding**, it overrides the port state that would have been selected by the spanning tree algorithm. Because the spanning tree algorithm cannot automatically disable the port, you must ensure that the port does not cause a loop in the network when it is in the forwarding state.	
Parameter	Ring number (required)	
Valid Values	X'001' to X'FFF'	
Default Value	None	
Description	This parameter specifies the unique ring number of the token ring attached to the remote PS/2 bridge.	
Parameter	Maximum transmission unit	
Valid Values	516, 1500, or 2052 octets	
Default	2052	
Description	This parameter specifies the size of the largest transmission unit that the source route bridge can transmit and receive on a serial port using the LAN Bridging Protocol. The transmission unit is the logical link control (LLC) PDU in the frame.	

Table 5-18 (Page 1 of 2). Configuration Worksheet - Source Route Bridging (Serial Port - PPP)

<table>
<tr><th colspan="2">Parameter Information</th><th>Your Value</th></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Enable source route bridging on this port
Enable, Disable
Disable
This parameter enables or disables source route bridging on the port.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Spanning tree mode
Automatic, Manual
Automatic
This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually configured. When Automatic is selected, the spanning tree determines the port state using information provided by the Path cost parameter. When Manual is selected, you can control the state of the port by configuring the Port state parameter.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Path cost
0 to 65535
0
When the Spanning tree mode parameter is set to Automatic, this parameter specifies the contribution of the port to the total cost of a path to the root bridge. For a value of zero, the path cost is calculated using the formula:

1000 / (media speed in Mbps)

The media speed for a serial port using PPP is 0.0096 (9600 bps) to 2.048 Mbps, depending on the serial line speed configured for the port.</td><td></td></tr>
<tr><td>Parameter
Valid Values

Default Value
Description</td><td>Port priority for translational bridging
X'00' to X'FF', where X'00' is the highest priority value and X'FF' is the lowest priority value
X'80'
When you configure the 6611 as a translational bridge, this parameter specifies the priority of the bridge port. The port priority is used to select the preferred port when:

• Two or more translational bridge ports are connected to the same LAN segment in a redundant configuration. (The spanning tree allows a path through only one of the ports.)

• Two or more translational bridge ports have equal path costs to the root bridge and represent paths through the same designated bridge. The designated bridge is the next-closest bridge to the root bridge.

If ports have equal priorities, then the port with the lowest port number is the preferred port. Port numbers are assigned automatically by the 6611.</td><td></td></tr>
</table>

Table 5-18 (Page 2 of 2). Configuration Worksheet - Source Route Bridging (Serial Port - PPP)

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Port state Forwarding, Disabled Forwarding When the Spanning tree mode parameter is set to **Manual**, this parameter specifies the port state. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames. When the 6611 is configured as source route bridge, the port state determines whether the port will forward single-route broadcast frames. When the 6611 is configured as a translational bridge, the port state determines whether the port will forward *both* single-route and all-routes broadcast frames. **Note:** When this parameter is set to **Forwarding**, it overrides the port state that would have been selected by the spanning tree algorithm. Because the spanning tree algorithm cannot automatically disable the port, you must ensure that the port does not cause a loop in the network when it is in the forwarding state.	
Parameter **Valid Values** **Default Value** **Description**	Ring number (required) X'001' to X'FFF' None This parameter specifies a number that is interpreted as the ring number for the serial link attached to the port. This number, which must be unique within the bridged network, is placed in the routing information (RI) field of route discovery frames transmitted over the serial link.	
Parameter **Valid Values** **Default** **Description**	Maximum transmission unit 516, 1500, or 2052 octets 2052 This parameter specifies the size of the largest transmission unit that the source route bridge can transmit and receive on a serial port using PPP. The transmission unit is the logical link control (LLC) PDU in the frame.	

Table 5-19 (Page 1 of 3). Configuration Worksheet - Source Route Bridging over Frame Relay

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable source route bridging on this port Enable, Disable Disable This parameter enables or disables source route bridging on the port.	
Parameter **Valid Values** **Default Value** **Description**	Spanning tree mode Automatic, Manual Automatic This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually configured. When **Automatic** is selected, the spanning tree determines the port state using information provided by the Path cost parameter. When **Manual** is selected, you can control the state of the port by configuring the Port state parameter.	

Table 5-19 (Page 2 of 3). Configuration Worksheet - Source Route Bridging over Frame Relay

Parameter Information	Your Value
Parameter Path cost **Valid Values** 0 to 65 535 **Default Value** 0 **Description** When the Spanning tree mode parameter is set to **Automatic**, this parameter specifies the contribution of the port to the total cost of a path to the root bridge. For a value of zero, the path cost is calculated using the formula: 1000 / (media speed in Mbps) The media speed for a frame relay serial port is 0.0096 (9600 bps) to 2.048 Mbps, depending on the serial line speed configured for the port.	
Parameter Port priority for translational bridging **Valid Values** X'00' to X'FF', where X'00' is the *highest* priority value and X'FF' is the *lowest* priority value **Default Value** X'80' **Description** When you configure the 6611 as a translational bridge, this parameter specifies the priority of the bridge port. The port priority is used to select the *preferred port* when: • Two or more translational bridge ports are connected to the same LAN segment in a redundant configuration. (The spanning tree allows a path through only one of the ports.) • Two or more translational bridge ports have equal path costs to the root bridge and represent paths through the same *designated bridge*. The designated bridge is the next-closest bridge to the root bridge. If ports have equal priorities, then the port with the lowest port number is the preferred port. Port numbers are assigned automatically by the 6611.	
Parameter Port state **Valid Values** Forwarding, Disabled **Default Value** Forwarding **Description** When the Spanning tree mode parameter is set to **Manual**, this parameter specifies the port state. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames. When the 6611 is configured as source route bridge, the port state determines whether the port will forward single-route broadcast frames. When the 6611 is configured as a translational bridge, the port state determines whether the port will forward *both* single-route and all-routes broadcast frames. **Note:** When this parameter is set to **Forwarding**, it overrides the port state that would have been selected by the spanning tree algorithm. Because the spanning tree algorithm cannot automatically disable the port, you must ensure that the port does not cause a loop in the network when it is in the forwarding state.	
Parameter Maximum transmission unit **Valid Values** 516, 1500, 2052, 4472, 8144, 11 407, or 17 800 octets **Default** 2052 **Description** This parameter specifies the size of the largest transmission unit that the source route bridge can transmit and receive on a serial port using frame relay. The transmission unit is the logical link control (LLC) PDU in the frame.	

Table 5-19 (Page 3 of 3). Configuration Worksheet - Source Route Bridging over Frame Relay

Parameter Information	Your Value
DLCI List - Parameters configured for each DLCI-ring number pair defined	
Parameter DLCI number (required for each ring number-DLCI pair defined) **Valid Values** Any DLCI value in the port list **Default Value** None **Description** This parameter specifies a DLCI that will be used to remotely bridge frames across a frame relay network. The value specified by this parameter is paired with a ring number, which identifies the frame-relay connection between this bridge and a remote bridge.	
Parameter Ring number (required for each ring number-DLCI pair defined) **Valid Values** X'001' to X'FFF' **Default Value** None **Description** This parameter assigns a unique ring number to a specific frame-relay connection. The frame-relay connection is identified by a DLCI. The ring number allows the frame-relay connection to be treated as a virtual ring between the 6611 and a remote bridge. One ring number can be assigned to each available DLCI. You can create a maximum of 240 DLCI-ring number pairs. Each pair must be unique. In addition, each ring number must be unique within this 6611.	

Table 5-20. Configuration Worksheet - Source Route Bridge Filters

Parameter Information	Your Value
Parameter Hop count **Valid Values** 1 to 7 **Default Value** 7 **Description** This parameter specifies the maximum hop count allowed for each inbound frame being bridged. The hop count for each frame is the number of bridges through which the frame has traveled so far. If the hop count in the frame is equal to or greater than the value in this parameter, the frame is discarded.	
Parameter Frame type **Valid Values** Single route broadcast (SRB), All routes broadcast (ARB), Both SRB and ARB **Default Value** All routes broadcast (ARB) **Description** This parameter specifies the type of inbound frame filtered by the hop count filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	

Table 5-21 (Page 1 of 2). Configuration Worksheet - Inbound Source SAP Filters

Parameter Information	Your Value
Parameter Enable inbound source SAP filters on this port **Valid Values** Enable, Disable **Default Value** Enable **Description** This parameter enables or disables all inbound source SAP filters defined for a source route bridge port.	

Table 5-21 (Page 2 of 2). Configuration Worksheet - Inbound Source SAP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the inbound source SAP filters you define affect broadcast frames identified by the Frame type parameter. When this parameter is set to **Permit**, filtered frames that contain the source SAP values you specify are bridged over the port. All other filtered frames are rejected. When this parameter is set to **Deny**, all filtered frames *except* those that contain the source SAP values you specify are bridged over the port.	
Parameter **Valid Values** **Default Value** **Description**	Frame type Single route broadcast (SRB), All routes broadcast (ARB), Both SRB and ARB Both SRB and ARB This parameter specifies the type of frame filtered by the inbound source SAP filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	
Filter List - Parameter configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Source SAP value (required for each filter defined) X'00' to X'FE', in increments of 2 None This parameter specifies the source service access point (SSAP) value used in this filter. The source SAP identifies the protocol contained in the frame. The filter compares this SAP value against the source SAP values in inbound broadcast frames identified by the Frame type parameter. The result of the comparison is determined by the setting of the Filtering mode parameter.	

| **Note:** A maximum of 128 inbound source SAP filters can be defined on a port. The source route bridging function on each token-ring port provides three default inbound source SAP filters: X'AA', X'BC', X'E0'. These filters are enabled automatically when the token-ring port is enabled for bridging.

Table 5-22 (Page 1 of 2). Configuration Worksheet - Inbound SNAP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable inbound SNAP filters on this port Enable, Disable Disable This parameter enables or disables all inbound SNAP filters defined for a source route bridge port.	
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the inbound SNAP filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the SNAP values you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the SNAP values you specify are bridged over the port.	

Table 5-22 (Page 2 of 2). Configuration Worksheet - Inbound SNAP Filters

Parameter Information		Your Value
Filter List - Parameters configured for each filter defined		
Parameter	SNAP value (required for each filter defined)	
Valid Values	X'0000' to X'FFFF'	
Default Value	None	
Description	This parameter specifies the SNAP value used in the filter. The filter compares this SNAP value against the SNAP values in all inbound frames. The result of the comparison is determined by the setting of the Filtering mode parameter. SNAP values are found only in frames where the source and destination SAPs equal X'AA'.	
Parameter	SNAP value mask	
Valid Values	X'0000' to X'FFFF'	
Default Value	X'FFFF'	
Description	This parameter is a mask that identifies the significant bits in the SNAP value defined for the filter. The mask enables you to specify a range of SNAP values to be filtered.	

Note: A maximum of 32 inbound SNAP value filters can be defined on a port.

Table 5-23 (Page 1 of 3). Configuration Worksheet - Inbound Routing Information Field Filters

Parameter Information		Your Value
Parameter	Enable inbound routing information field filters on this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables all inbound RI field filters defined for a source route bridge port.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default Value	Deny	
Description	This parameter specifies how the inbound RI field filters you define affect broadcast frames identified by the Frame type parameter. When this parameter is set to **Permit**, filtered frames with the RI field characteristics you define are bridged over the port. All other filtered frames are rejected. When this parameter is set to **Deny**, all filtered frames *except* those that contain the RI field characteristics you define are bridged over the port.	
Parameter	Frame type	
Valid Values	Single route broadcast (SRB), All routes broadcast (ARB), Both SRB and ARB	
Default Value	Both SRB and ARB	
Description	This parameter specifies the type of frame filtered by the inbound RI field filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	

Table 5-23 (Page 2 of 3). Configuration Worksheet - Inbound Routing Information Field Filters

Parameter Information		Your Value
Filter List - Parameters configured for each filter defined		
Parameter	Select route designator (see table notes)	
Valid Values	First route designator, Next-to-last route designator, All route designators	
Default Value	First route designator	
Description	This parameter selects the route designator in an inbound frame to which this filter is applied. A route designator is a subfield within a frame's RI field. The route designator consists of a ring and bridge number pair that represents a hop within a specific route. The first route designator represents the first hop from the station originating the frame (the ring sending the frame and the first bridge to receive it). The next-to-last route designator represents the last hop taken on the route. For an inbound frame, the bridge portion of the next-to-last route designator specifies the last bridge through which the frame passed. The ring portion of the next-to-last route designator specifies the next-to-last ring through which the frame passed.	
Parameter	Filter on	
Valid Values	Ring number, Bridge number, Both	
Default Value	Both	
Description	This parameter specifies the portion of the route designator in an inbound frame to which this filter is applied. The route designator consists of a ring number and bridge number pair. This filter can apply to the ring number or bridge number in the route designator, or to both. The route designator to which this filter is applied is specified in the Select route designator parameter.	
Parameter	Ring number	
Valid Values	X'001' to X'FFF'	
Default Value	None	
Description	This parameter specifies the ring number used in the filter. The filter compares this ring number against one or more ring numbers in the RI field of filtered broadcast frames. The setting of the Select route designator parameter determines which ring numbers in a frame are affected by the filter.	
Parameter	Ring number mask	
Valid Values	X'000' to X'FFF'	
Default Value	X'FFF'	
Description	This parameter is a mask that identifies the significant bits in the ring number defined for the filter. The mask enables you to specify a range of ring numbers to be filtered.	
Parameter	Bridge number	
Valid Values	X'0' to X'F'	
Default Value	None	
Description	This parameter specifies the bridge number used in the filter. The bridge number uniquely identifies a bridge connecting two rings. The filter compares this bridge number against one or more bridge numbers in the RI field of filtered broadcast frames. The setting of the Select route designator parameter determines which bridge numbers in a frame are affected by this filter.	

Table 5-23 (Page 3 of 3). Configuration Worksheet - Inbound Routing Information Field Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Bridge number mask X'0' to X'F' X'F' This parameter is a mask that identifies the significant bits in the bridge number defined for the filter. The mask enables you to specify a range of bridge numbers to be filtered.	

Note:

- A maximum of 32 inbound RI field filters can be defined on a port.
- The last route designator in an inbound frame consists of a bridge portion, which is not used, and a ring portion, which specifies the ring from which the frame was received.

Table 5-24 (Page 1 of 2). Configuration Worksheet - Inbound MAC Address Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable inbound MAC address filters on this port Enable, Disable Disable This parameter enables or disables all inbound MAC address filters defined for a source route bridge port.	
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the inbound MAC address filters you define affect broadcast frames identified by the Frame type parameter. When this parameter is set to **Permit**, filtered frames that contain the MAC addresses you specify are bridged over the port. All other filtered frames are rejected. When this parameter is set to **Deny**, all filtered frames *except* those that contain the MAC addresses you specify are bridged over the port.	
Parameter **Valid Values** **Default Value** **Description**	Frame type Single route broadcast (SRB), All routes broadcast (ARB), Both SRB and ARB Both SRB and ARB This parameter specifies the type of frame filtered by the inbound MAC address filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	
Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default Value** **Description**	Source MAC address (required for each filter defined) X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter specifies the source MAC address used in this filter. The filter compares this MAC address against the source MAC addresses in inbound broadcast frames identified by the Frame type parameter. The result of the comparison is determined by the setting of the Filtering mode parameter.	

Table 5-24 (Page 2 of 2). Configuration Worksheet - Inbound MAC Address Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Destination MAC address (required for each filter defined) X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter specifies the destination MAC address used in this filter. The filter compares this MAC address against the destination MAC addresses in inbound broadcast frames identified by the Frame type parameter. The result of the comparison is determined by the setting of the Filtering mode parameter.	
Parameter **Valid Values** **Default Value** **Description**	Source MAC address mask X'0000 0000 0000' to X'7FFF FFFF FFFF' X'7FFF FFFF FFFF' This parameter is a mask that identifies the significant bits in the source MAC address defined for the filter. The mask enables you to specify a range of source MAC addresses to be filtered.	
Parameter **Valid Values** **Default Value** **Description**	Destination MAC address mask X'0000 0000 0000' to X'FFFF FFFF FFFF' X'FFFF FFFF FFFF' This parameter is a mask that identifies the significant bits in the destination MAC address defined for the filter. The mask enables you to specify a range of destination MAC addresses to be filtered.	
Parameter **Valid Values** **Default Value** **Description**	Form of MAC addresses Canonical, Noncanonical Noncanonical This parameter specifies the format of the MAC addresses defined for this filter.	

Note: A maximum of 32 inbound MAC address filters can be defined on a port.

Table 5-25 (Page 1 of 2). Configuration Worksheet - Inbound Sliding Window Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable inbound sliding window filters on this port Enable, Disable Disable This parameter enables or disables all inbound sliding window filters defined for a source route bridge port.	
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the inbound sliding window filters you define affect broadcast frames identified by the Frame type parameter. When this parameter is set to **Permit**, filtered frames that contain the sliding window bytes you specify are bridged over the port. All other filtered frames are rejected. When this parameter is set to **Deny**, all filtered frames *except* those that contain the sliding window bytes you specify are bridged over the port.	
Parameter **Valid Values** **Default Value** **Description**	Frame type Single route broadcast, All routes broadcast, Both SRB and ARB Both SRB and ARB This parameter specifies the type of frame filtered by the inbound sliding window filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	

Table 5-25 (Page 2 of 2). Configuration Worksheet - Inbound Sliding Window Filters

Parameter Information	Your Value
Filter List - Parameters configured for each filter defined	
Parameter Filter name (required for each filter defined) **Valid Values** 1 to 16 characters **Default Value** None **Description** This parameter specifies the name of the sliding window filter.	
Parameter Offset starting field **Valid Values** MAC, SAP **Default Value** MAC **Description** This parameter specifies where the sliding window filter should be applied in an inbound frame. When you select **MAC**, the sliding window filter is applied at an offset calculated from the beginning of the Access Control field in the MAC header. When you select **SAP**, the sliding window filter is applied at an offset calculated from the beginning of the destination SAP (DSAP) field in the frame. The size of the offset is determined by the Offset into frame parameter. **Note:** The source route bridging frame contains a routing information field that is variable in length. When **SAP** is selected, the offset is calculated from the beginning of the destination SAP field, which is after the variable RI field.	
Parameter Offset into frame **Valid Values** 0 to 2084 bytes **Default Value** 0 **Description** This parameter specifies a byte offset used in calculating where the sliding window filter should be applied in an inbound frame.	
Parameter Sliding window contents (required for each filter defined) **Valid Values** A string of up to 30 hexadecimal bytes. Each byte contains two hexadecimal digits (00 to FF). The string must end on a byte boundary. **Default Value** None **Description** This parameter specifies the contents of the sliding window. A sliding window filter can be used to filter any portion of an inbound broadcast frame.	
Parameter Sliding window mask **Valid Values** A string of up to 30 hexadecimal bytes. Each byte contains two hexadecimal digits (00 to FF). Any bytes in the mask beyond what is specified for the sliding window contents are ignored. When the mask contains fewer bytes than the number of bytes specified for the sliding window contents, the missing bytes will be treated as zeros and the corresponding bytes in the sliding window contents will not be treated as significant. **Default Value** A string of 30 hexadecimal bytes, each with a value of X'FF' **Description** This parameter is a mask that identifies the significant bits in the string defined for the Sliding window contents parameter. The mask enables you to specify a range of strings to be filtered.	

Note: A maximum of 16 inbound sliding window filters can be defined on a port.

Table 5-26. Configuration Worksheet - Inbound Filter Order

Parameter Information		Your Value
Parameter	Override the default filter order set at the node level	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	When this parameter is enabled, you can change the order in which inbound filter types are applied on the source route bridge port being configured. The order you specify overrides the order defined for the bridge at the node level.	
Parameter	Hop count filter (required to reorder filters)	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first*, and 6 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the inbound hop count filter type is to be applied on the source route bridge port being configured.	
Parameter	Source SAP filter (required to reorder filters)	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first*, and 6 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the inbound source SAP filter type is to be applied on the source route bridge port being configured.	
Parameter	SNAP value filter (required to reorder filters)	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first*, and 6 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the inbound SNAP value filter type is to be applied on the source route bridge port being configured.	
Parameter	RI field filter (required to reorder filters)	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first*, and 6 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the inbound RI field filter type is to be applied on the source route bridge port being configured.	
Parameter	MAC address filter (required to reorder filters)	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first*, and 6 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the inbound MAC address filter type is to be applied on the source route bridge port being configured.	
Parameter	Sliding window filter (required to reorder filters)	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first*, and 6 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the inbound sliding window filter type is to be applied on the source route bridge port being configured.	

Note: To override the default filter order established at the node level, you must specify a new value for each port filter type parameter.

Table 5-27. Configuration Worksheet - Outbound Source SAP Filters

Parameter Information		Your Value
Parameter	Enable outbound source SAP filters on this port	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables all outbound source SAP filters defined for a source route bridge port.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default Value	Deny	
Description	This parameter specifies how the outbound source SAP filters you define affect broadcast frames identified by the Frame type parameter. When this parameter is set to **Permit**, filtered frames that contain the source SAP values you specify are bridged over the port. All other filtered frames are rejected. When this parameter is set to **Deny**, all filtered frames *except* those that contain the source SAP values you specify are bridged over the port.	
Parameter	Frame type	
Valid Values	Single route broadcast (SRB), All routes broadcast (ARB), Both SRB and ARB	
Default Value	Both SRB and ARB	
Description	This parameter specifies the type of frame filtered by the outbound source SAP filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	
Filter List - Parameter configured for each filter defined		
Parameter	Source SAP value (required for each filter defined)	
Valid Values	X'00' to X'FE' in increments of 2	
Default	None	
Description	This parameter specifies the source service access point (SSAP) value used in this filter. The source SAP identifies the protocol contained in the frame. The filter compares this SAP value against the source SAP values in outbound broadcast frames identified by the Frame type parameter. The result of the comparison is determined by the setting of the Filtering mode parameter.	

Note: A maximum of 128 outbound source SAP filters can be defined on a port.

Table 5-28 (Page 1 of 2). Configuration Worksheet - Outbound SNAP Filters

Parameter Information		Your Value
Parameter	Enable outbound SNAP filters on this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables all outbound SNAP filters defined on a source route bridge port.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default Value	Deny	
Description	This parameter specifies how the outbound SNAP filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the SNAP values you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the SNAP values you specify are bridged over this port.	

Table 5-28 (Page 2 of 2). Configuration Worksheet - Outbound SNAP Filters

Parameter Information		Your Value
Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default Value** **Description**	SNAP value (required for each filter defined) X'0000' to X'FFFF' None This parameter specifies the SNAP value used in the filter. The filter compares this SNAP value against the SNAP values in all outbound frames. The result of the comparison is determined by the setting of the Filtering mode parameter. SNAP values are found only in frames where the source and destination SAPs equal X'AA'.	
Parameter **Valid Values** **Default Value** **Description**	SNAP value mask X'0000' to X'FFFF' X'FFFF' This parameter is a mask that identifies the significant bits in the SNAP value defined for the filter. The mask enables you to specify a range of SNAP values to be filtered.	

Table 5-29 (Page 1 of 3). Configuration Worksheet - Outbound Routing Information Field Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable outbound routing information field filters on this port Enable, Disable Disable This parameter enables or disables all outbound RI field filters defined for a source route bridge port.	
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the outbound RI field filters you define affect broadcast frames identified by the Frame type parameter. When this parameter is set to **Permit**, filtered frames with the RI field characteristics you define are bridged over the port. All other filtered frames are rejected. When this parameter is set to **Deny**, all filtered frames *except* those that contain the RI field characteristics you define are bridged over the port.	
Parameter **Valid Values** **Default Value** **Description**	Frame type Single route broadcast (SRB), All routes broadcast (ARB), Both SRB and ARB Both SRB and ARB This parameter specifies the type of frame filtered by the outbound RI field filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	

Table 5-29 (Page 2 of 3). Configuration Worksheet - Outbound Routing Information Field Filters

Parameter Information	Your Value
Filter List - Parameters configured for each filter defined	
Parameter Select route designator (see table notes) **Valid Values** First route designator, Next-to-last route designator, All route designators **Default Value** First route designator **Description** This parameter selects the route designator in an outbound frame to which this filter is applied. A route designator is a subfield within a frame's RI field. The route designator consists of a ring and bridge number pair that represents a hop within a specific route. The first route designator represents the first hop from the station originating the frame (the ring sending the frame and the first bridge to receive it). The next-to-last route designator represents the last hop taken on the route. For an outbound frame, the bridge portion of the next-to-last route designator specifies this 6611 bridge. The ring portion of the next-to-last route designator specifies the last ring through which the frame passed; this is the ring from which the frame was received.	
Parameter Filter on **Valid Values** Ring number, Bridge number, Both **Default Value** Both **Description** This parameter specifies the portion of the route designator in an outbound frame to which this filter is applied. The route designator consists of a ring number and bridge number pair. This filter can apply to the ring number or bridge number in the route designator, or to both. The route designator to which this filter is applied is specified in the Select route designator parameter.	
Parameter Ring number **Valid Values** X'001' to X'FFF' **Default Value** None **Description** This parameter specifies the ring number used in the filter. The filter compares this ring number against one or more ring numbers in the RI field of filtered broadcast frames. The setting of the Select route designator parameter determines which ring numbers in a frame are affected by the filter.	
Parameter Ring number mask **Valid Values** X'000' to X'FFF' **Default Value** X'FFF' **Description** This parameter is a mask that identifies the significant bits in the ring number defined for the filter. The mask enables you to specify a range of ring numbers to be filtered.	
Parameter Bridge number **Valid Values** X'0' to X'F' **Default Value** None **Description** This parameter specifies the bridge number used in the filter. The bridge number uniquely identifies a bridge connecting two rings. The filter compares this bridge number against one or more bridge numbers in the RI field of filtered broadcast frames. The setting of the Select route designator parameter determines which bridge numbers in a frame are affected by this filter.	

Table 5-29 (Page 3 of 3). Configuration Worksheet - Outbound Routing Information Field Filters

Parameter Information	Your Value
Parameter Bridge number mask **Valid Values** X'0' to X'F' **Default Value** X'F' **Description** This parameter is a mask that identifies the significant bits in the bridge number defined for the filter. The mask enables you to specify a range of bridge numbers to be filtered.	

Note:

- A maximum of 32 outbound RI field filters can be defined on a port.
- The last route designator in an outbound frame consists of a bridge portion, which is not used, and a ring portion, which specifies the next ring on the route.

Table 5-30 (Page 1 of 2). Configuration Worksheet - Outbound MAC Address Filters

Parameter Information	Your Value
Parameter Enable outbound MAC address filters on this port **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables all outbound MAC address filters defined for a source route bridge port.	
Parameter Filtering mode **Valid Values** Deny, Permit **Default Value** Deny **Description** This parameter specifies how the outbound MAC address filters you define affect broadcast frames identified by the Frame type parameter. When this parameter is set to **Permit**, filtered frames that contain the MAC addresses you specify are bridged over the port. All other filtered frames are rejected. When this parameter is set to **Deny**, all filtered frames *except* those that contain the MAC addresses you specify are bridged over the port.	
Parameter Frame type **Valid Values** Single route broadcast (SRB), All routes broadcast (ARB), Both SRB and ARB **Default Value** Both SRB and ARB **Description** This parameter specifies the type of frame filtered by the outbound MAC address filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	
Filter List - Parameters configured for each filter defined	
Parameter Source MAC address (required for each filter defined) **Valid Values** X'0000 0000 0000' to X'FFFF FFFF FFFF' **Default Value** None **Description** This parameter specifies the source MAC address used in this filter. The filter compares this MAC address against the source MAC addresses in outbound broadcast frames identified by the Frame type parameter. The result of the comparison is determined by the setting of the Filtering mode parameter.	

Table 5-30 (Page 2 of 2). Configuration Worksheet - Outbound MAC Address Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Destination MAC address (required for each filter defined) X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter specifies the destination MAC address used in this filter. The filter compares this MAC address against the destination MAC addresses in outbound broadcast frames identified by the Frame type parameter. The result of the comparison is determined by the setting of the Filtering mode parameter.	
Parameter **Valid Values** **Default Value** **Description**	Source MAC address mask X'0000 0000 0000' to X'7FFF FFFF FFFF' X'7FFF FFFF FFFF' This parameter is a mask that identifies the significant bits in the source MAC address defined for the filter. The mask enables you to specify a range of source MAC addresses to be filtered.	
Parameter **Valid Values** **Default Value** **Description**	Destination MAC address mask X'0000 0000 0000' to X'FFFF FFFF FFFF' X'FFFF FFFF FFFF' This parameter is a mask that identifies the significant bits in the destination MAC address defined for the filter. The mask enables you to specify a range of destination MAC addresses to be filtered.	
Parameter **Valid Values** **Default Value** **Description**	Form of MAC addresses Canonical, Noncanonical Noncanonical This parameter specifies the format of the MAC addresses defined for this filter.	

Note: A maximum of 32 outbound MAC address filters can be defined on a port.

Table 5-31 (Page 1 of 2). Configuration Worksheet - Outbound Sliding Window Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable outbound sliding window filters on this port Enable, Disable Disable This parameter enables or disables all outbound sliding window filters defined for a source route bridge port.	
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the outbound sliding window filters you define affect broadcast frames identified by the Frame type parameter. When this parameter is set to **Permit**, filtered frames that contain the sliding window bytes you specify are bridged over the port. All other filtered frames are rejected. When this parameter is set to **Deny**, all filtered frames *except* those that contain the sliding window bytes you specify are bridged over the port.	
Parameter **Valid Values** **Default Value** **Description**	Frame type Single route broadcast, All routes broadcast, Both SRB and ARB Both SRB and ARB This parameter specifies the type of frame filtered by the outbound sliding window filter. **Note:** Only broadcast frames can be filtered; specifically-routed frames are never filtered.	

Table 5-31 (Page 2 of 2). Configuration Worksheet - Outbound Sliding Window Filters

Parameter Information		Your Value
Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default Value** **Description**	Filter name(required for each filter defined) 1 to 16 characters None This parameter specifies the name of the sliding window filter.	
Parameter **Valid Values** **Default Value** **Description**	Offset starting field MAC, SAP MAC This parameter specifies where the sliding window filter should be applied in an outbound frame. When you select **MAC**, the sliding window filter is applied at an offset calculated from the beginning of the Access Control field in the MAC header. When you select **SAP**, the sliding window filter is applied at an offset calculated from the beginning of the destination SAP (DSAP) field in the frame. The size of the offset is determined by the Offset into frame parameter. **Note:** The source route bridging frame contains a routing information field that is variable in length. When **SAP** is specified, the offset is calculated from the beginning of the destination SAP field, which is after the variable RI field.	
Parameter **Valid Values** **Default Value** **Description**	Offset into frame 0 to 2084 bytes 0 This parameter specifies a byte offset used in calculating where the sliding window filter should be applied in an outbound frame.	
Parameter **Valid Values** **Default Value** **Description**	Sliding window contents (required for each filter defined) A string of up to 30 hexadecimal bytes. Each byte contains two hexadecimal digits (00 to FF). The string must end on a byte boundary. None This parameter specifies the contents of the sliding window. A sliding window filter can be used to filter any portion of an inbound broadcast frame.	
Parameter **Valid Values** **Default Value** **Description**	Sliding window mask A string of up to 30 hexadecimal bytes. Each byte contains two hexadecimal digits (00 to FF). Any bytes in the mask beyond what is specified for the sliding window contents are ignored. When the mask contains fewer bytes than the number of bytes specified for the sliding window contents, the missing bytes will be treated as zeros and the corresponding bytes in the sliding window contents will not be treated as significant. A string of 30 hexadecimal bytes, each with a value of X'FF' This parameter is a mask that identifies the significant bits in the string defined for the Sliding window contents parameter. The mask enables you to specify a range of strings to be filtered.	

Note: A maximum of 16 outbound sliding window filters can be defined on a port.

Table 5-32. Configuration Worksheet - Outbound Filter Order

Parameter Information		Your Value
Parameter	Override the default filter order set at the node level	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	When this parameter is enabled, you can change the order in which outbound filter types are applied on the source route bridge port being configured. The order you specify overrides the order defined for the bridge at the node level.	
Parameter	Source SAP filter (required to reorder filters)	
Valid Values	1 to 5, where 1 specifies that this filter type should be applied *first*, and 5 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the outbound source SAP filter type is to be applied on the source route bridge port being configured.	
Parameter	SNAP value filter (required to reorder filters)	
Valid Values	1 to 5, where 1 specifies that this filter type should be applied *first*, and 5 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the outbound SNAP value filter type is to be applied on the source route bridge port being configured.	
Parameter	RI field filter (required to reorder filters)	
Valid Values	1 to 5, where 1 specifies that this filter type should be applied *first*, and 5 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the outbound RI field filter type is to be applied on the source route bridge port being configured.	
Parameter	MAC address filter (required to reorder filters)	
Valid Values	1 to 5, where 1 specifies that this filter type should be applied *first*, and 6 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the outbound MAC address filter type is to be applied on the source route bridge port being configured.	
Parameter	Sliding window filter (required to reorder filters)	
Valid Values	1 to 5, where 1 specifies that this filter type should be applied *first*, and 5 specifies that this filter type should be applied *last*	
Default Value	None	
Description	This parameter controls when the outbound sliding window filter type is to be applied on the source route bridge port being configured.	

Note: To override the default filter order established at the node level, you must specify a new value for each port filter type parameter.

Node Level Worksheets

Figure 5-4 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-4.

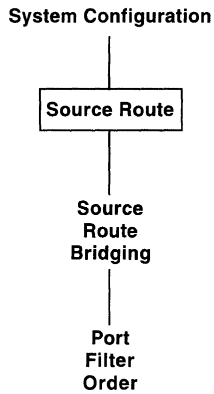


Figure 5-4. Flow of Node Level Source Route Bridging Help Windows

Use the following tables as worksheets for configuring source route bridging at the node level:

- Source Route Bridging on page 5-39
- Port Filter Order on page 5-41

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-6 on page D-7 for a mapping of parameter names and their associated labels.

Table 5-33 (Page 1 of 2). Configuration Worksheet - Source Route Bridging

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable Source Route Bridging Enable, Disable Disable This parameter enables or disables source route bridging on the 6611. Source route bridging also must be enabled on individual adapter ports.	
Parameter **Valid Values** **Default Value** **Description**	Bridge number (required) 0 to 15. Bridge numbers must be unique among bridges that connect a particular pair of LAN segments. None This parameter specifies a bridge number for the translational bridge. The bridge number uniquely identifies the bridge when it and one or more other bridges are used to connect two LAN segments.	
Parameter **Valid Values** **Default Value** **Description**	Enable LAN Bridging Protocol Enable, Disable Enable When this parameter is enabled, remote source route bridging over a serial link to an IBM token-ring bridge program is permitted. The bridge program operates on a PS/2 workstation.	

Table 5-33 (Page 2 of 2). Configuration Worksheet - Source Route Bridging

Parameter Information		Your Value
Parameter	Designated ring number (required when the LAN Bridging Protocol is enabled)	
Valid Values	X'001' to X'FFE'	
Default Value	None	
Description	This parameter specifies the ring number of the 6611 bridge port that serves as the target ring for all remotely attached PS/2 workstations running an IBM token-ring bridge program. The designated ring number can be the ring number of any 6611 source route bridge port, except a LAN Bridging Protocol port. The designated ring number appears as a route designator in the RI field of all frames forwarded to and received from the remotely attached PS/2 bridges.	
Spanning tree parameters		
Parameter	Bridge priority	
Valid Values	X'0000' to X'FFFF', where X'0000' is the *highest* priority value and X'FFFF' is the *lowest* priority value.	
Default Value	X'8000'	
Description	This parameter specifies the priority of this source route bridge. When this bridge is activated, its priority value is compared to the priority values of other active bridges in the network. The bridge with the highest priority becomes the root bridge of the spanning tree. If the highest priority value in the network is shared by two or more bridges, the bridges compare port MAC addresses (one port on each bridge is selected for this purpose). The bridge with the lowest value MAC address becomes the root bridge.	
Parameter	Hello time	
Valid Values	1 to 10 seconds	
Default Value	2 seconds	
Description	When this bridge is selected as the root bridge of a spanning tree, this parameter specifies how often this bridge transmits configuration bridge protocol data units (BPDUs). BPDUs contain information about the topology of the spanning tree and reflect changes to the topology.	
Parameter	Forward delay time	
Valid Values	4 to 30 seconds	
Default Value	15 seconds	
Description	When this bridge is selected as the root bridge, the value of this parameter specifies how long active ports in all bridges remain in a listening state. When the forward delay time expires, ports in the listening state go into the forwarding state.	
Parameter	Max age	
Valid Values	6 to 40 seconds	
Default Value	20 seconds	
Description	When this bridge is selected as the root bridge, the value of this parameter specifies how long other active bridges are to store the topology information received from BPDUs. When this information reaches its maximum age limit without being replaced, the active bridges in the network discard it and assume the root bridge or the path to the root bridge has failed. A new root bridge or path is then selected.	

Note: In a source route bridge network, the spanning tree is used to forward single-route broadcast frames. These frames can be used to discover a route between a source station and a destination station.

Table 5-34. Configuration Worksheet - Port Filter Order

Parameter Information		Your Value
Parameter	Hop count filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	1	
Description	This parameter controls when the hop count filter type is to be applied on all 6611 ports that support source route bridging. The hop count filter is applied to inbound frames only.	
Parameter	Source SAP filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	2	
Description	This parameter controls when the source SAP filter type is to be applied on all 6611 ports that support source route bridging.	
Parameter	SNAP value filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridge ports, and 6 specifies that this filter type should be applied *last*	
Default Value	3	
Description	This parameter controls when the SNAP value filter type is to be applied on all 6611 ports that support source route bridging.	
Parameter	RI field filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	4	
Description	This parameter controls when the RI field filter type is to be applied on all 6611 ports that support source route bridging.	
Parameter	MAC address filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	5	
Description	This parameter controls when the MAC address filter type is to be applied on all 6611 ports that support source route bridging.	
Parameter	Sliding window filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	6	
Description	This parameter controls when the sliding window filter type is to be applied on all 6611 ports that support source route bridging.	

Transparent Bridging

The 6611 supports both local and remote Ethernet transparent bridging, as defined in the IEEE standard for Media Access Control Bridges (802.1D). The 6611 also supports local and remote transparent bridging of all network protocols.

Table 5-35 describes the various ways in which transparent bridging can be configured on the 6611.

Table 5-35. Transparent Bridging Configurations on the 6611

Configuration	Description
Local transparent bridging	The bridging of frames between Ethernet LANs directly attached to the same 6611. The 6611 is defined as a transparent bridge at the node level.
Remote transparent bridging	The bridging of frames between Ethernet LANs attached to separate 6611s. Remote transparent bridging is supported over a telecommunications link or frame relay network. The 6611 is defined as a transparent bridge at the node level and is remotely connected to either another transparent bridge or a *translational bridge*.
Translational bridging	The bridging of frames between Ethernet and token-ring LANs. When the 6611 is defined as a translational bridge at the node level, frames are bridged between ports that have transparent bridging enabled and those that have source route bridging enabled. If the origin and destination ports use the same bridging scheme, frames are bridged without translation. If the origin and destination ports use different bridging schemes, frames are translated into the proper format and then bridged. See "Translational Bridging" on page 5-75 for more information on this bridging method.
Dual mode bridging	The recommended method for remotely connecting two 6611s configured as translational bridges. When dual mode bridging is configured on both ends of a serial link, frames originating from a LAN port configured for transparent bridging are translated only if the destination LAN on the remote 6611 requires a different MAC frame format. See "Translational Bridging" on page 5-75 for more information on dual mode bridging.

Port Types Supported

Table 5-36. Port Types Supported for Transparent Bridging

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	√
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	
		SNAP	
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	

Restrictions

- The source and destination end stations for bridged frames must be on Ethernet LANs unless translational bridging is configured.
- When you configure the 6611 as a transparent bridge, the bridge must contain at least one enabled transparent bridge port with a MAC address. This condition can be met in one of two ways:
  1. By enabling transparent bridging on an Ethernet port. Each Ethernet port has a universally or locally defined MAC address.
  2. By enabling transparent bridging on a serial port and configuring the Locally administered MAC address parameter for the serial port's physical interface. (See "Serial Port and V.35/V.36 Serial Port" on page 4-2.) If all of the bridge ports are serial ports, this step is required.

  The 6611 uses the MAC address to generate a bridge identifier for the transparent bridge. The bridge identifier is used by the spanning tree algorithm for the transparent bridge network.
- When defining transparent bridging on a serial adapter port using frame relay, you need to specify at least one data link connection identifier (DLCI) that will be used to transmit bridged frames over the frame relay network. The transparent bridging protocol cannot use frame relay's InARP protocol to acquire DLCI numbers dynamically.

  In addition, once you define DLCIs for the bridging protocol, you must explicitly define DLCIs for *all other* protocols running on the same port. First, configure the frame-relay protocol by defining a list of DLCIs assigned to the serial port. Then as you define individual protocols on the port, specify which DLCIs are available for use by each protocol.
- The 6611 bridge interprets Ethernet frames using Novell's proprietary format as Ethernet 802.3 frames because the Novell frames contain a Length field. The bridge interprets the X'FFFF' sequence following the Length field as DSAP and SSAP values, respectively. As a result, if you define a source SAP filter of X'FE' on a transparent bridge port, it is applied to these frames (the filter ignores the low-order command/response bit in the SSAP field).

  To filter Ethernet frames in Novell's proprietary format, define a sliding window filter on the transparent bridge port with a contents field of X'FFFF' and an Offset starting field of **Data**. If you also want to filter IPX traffic on the same port, define a second sliding window filter with an Offset starting field of **Data**, an Offset into frame value of 1 (to filter on the SSAP), a contents field of X'E0', and a mask of X'FE'.

Configuration Changes...

That Require the Transparent Bridging Function to Restart

All node and port-level transparent bridging parameters

That Require the 6611 to Restart

When bridging is configured on a serial port using frame relay, changes to most of the bridging parameters on the frame relay port will cause the 6611 to restart.

Before You Configure...

This section contains additional information to assist you in configuring the transparent bridging protocol.

Specifying Ethernet Addresses

Ethernet addresses are typically represented in canonical form. Canonical form is the address format defined as the standard MAC address representation by the IEEE. In this format, the bit within each octet that is to be transmitted first on a LAN is represented as the least significant bit. For addresses in noncanonical form, the bit within each octet that is transmitted first is represented as the most significant bit.

To illustrate, the following bit string is shown in both noncanonical and canonical forms:

B'00010011 00000000 01011010 00000000 00000000 00000001'

- In noncanonical form: X'13 00 5A 00 00 01'
- In canonical form: X'C8 00 5A 00 00 80'

When Are Ethernet Frames Bridged?

When transparent bridging has been defined on an Ethernet port, the bridge examines each frame to determine whether the network protocol encapsulated within the frame should be bridged or routed. If the network protocol has been configured for routing, the frame is routed. If the network protocol has not been configured for routing, the frame is bridged. When a protocol is not configured for routing, and bridging is disabled, the 6611 discards any packets received for that particular protocol.

On a serial port, a frame received as an encapsulated Ethernet packet cannot be routed. If transparent bridging is enabled on the port, the frame is bridged. If transparent bridging is not enabled, the 6611 discards the frame

Note: Ethernet packets received on serial ports cannot be forwarded to data link switching.

For more information on how the 6611 examines an Ethernet frame to determine whether the frame should be bridged or routed, refer to the transparent bridging description in the *Introduction and Planning Guide*.

Defining Transparent Bridge Port Filters

The transparent bridging function on the 6611 provides a set of filters that enables you to control the type of traffic being bridged over a port. Each of the filters can be used to evaluate a different portion of an Ethernet frame. When the filters are applied to an Ethernet frame, the values specified for the filters are compared against the contents of the frame. The result of these comparisons determines whether the frame is rejected or bridged.

The use of bridge port filters is optional. Table 5-37 on page 5-45 shows each of the port filter types supported by the 6611 transparent bridge.

Table 5-37. Transparent Bridge Port Filters

This Filter Type...	Is Compared to...
Source SAP	The source service access point (SSAP) field in an IEEE 802.3 frame. The source SAP identifies the network protocol encapsulated within the frame.
Ethernet Type	The Type field in an Ethernet V2.0 frame or an IEEE 802.3 frame with a subnetwork access protocol (SNAP) header. The Type field identifies the non-IEEE network protocol encapsulated within the frame.
MAC address	The source and destination MAC address fields in an Ethernet frame. You can filter out a destination MAC address on all ports by defining a static destination address filter for the bridge. See "Defining Static Destination Address Filters" on page 5-48 for more information.
Sliding window	Any portion of an Ethernet frame, as defined by the filter.

Note: Refer to the transparent bridging description in the *Introduction and Planning Guide* for an illustration of the different Ethernet frame formats.

Each port filter can be defined as an *inbound* filter or an *outbound* filter. Inbound filters are applied to frames flowing into the bridge port from a LAN segment or link. Outbound filters are applied to frames flowing out of the bridge port onto a LAN segment or link. When a filter is applied to a frame, the outcome is based on one or both of the following criteria, depending on the type of filter chosen:

- Whether the Filtering mode parameter is set to **Permit** or **Deny**. Permit filters allow frames to pass through the port if the contents of the filter and the frame match. Deny filters do not allow frames to pass through the port if the contents of the filter and the frame match.
- Whether a *mask* has been specified for the contents of the filter. A mask value can expand the range of the filter to increase the likelihood that a match will occur. (See "Using Mask Values in Filters" on page 5-47 for more information.)

You can define and enable multiple filters on each port. When more than one type of filter is defined and enabled on a bridge port, the filter types are applied in a pre-defined order (as described in the next section). Table 5-38 summarizes the algorithm used by the 6611 bridge when applying port filters. Port filters are applied in sequence until the frame is rejected or until, having passed through each filter, the frame is bridged.

Table 5-38. Algorithm Used for Bridge Port Filters

A Filter with Filtering Mode of...	Applied with This Result...	Yields This Outcome...
Deny	Filter and frame contents match	Frame is rejected; no other filters are applied to it.
Deny	Filter and frame contents do not match	Frame is passed to the next filter
Permit	Filter and frame contents match	Frame is passed to the next filter
Permit	Filter and frame contents do not match	Frame is rejected; no other filters are applied to it.

Filtering Example: Suppose the following Deny filters are defined for a port: inbound source SAP filter, X'E0' (to filter IPX frames); and inbound MAC address filters, MAC A and MAC B. By default, the source SAP filter would be applied first. If an inbound frame contained a source SAP value of X'E0', the frame would be rejected by the port. If, however, the frame contained a different source SAP value, the inbound MAC address filters would be applied next in the order in which they were defined in the Configuration program.

If, in the previous example, the source SAP filter were a Permit filter, the outcome would be reversed. If the inbound frame contained a source SAP value of X'E0', the frame would be permitted and the MAC address filters would be applied to the frame. If the inbound frame contained a different source SAP value, the frame would be rejected by the port before the other filters were applied.

Defining the Order of Port Filters

The order in which different types of filters are applied can affect the performance of the transparent bridge. As a rule, filter types should be applied in the order in which they are most likely to be effective. The result is that the majority of unwanted traffic is discarded in the shortest amount of time, freeing buffer space to accommodate more traffic.

The node-level parameters for transparent bridging enable you to define the order in which inbound and outbound filters should be applied on all 6611 ports configured for transparent bridging. The default order, by filter type, is:

1. Source SAP filters
2. Ethernet Type filters
3. MAC address filters
4. Sliding window filters

Notes:

1. The default filter order reflects the order that is likely to be most effective in a typical bridged network. The optimal order, however, depends upon the configuration of your network and your specific filtering requirements.
2. When configuring a translational bridge, you can specify the order in which filters should be applied on both transparent bridge and source route bridge ports on the 6611.

If the default filter order is not appropriate for a specific port, you have the option of overriding the default and reordering the filters on that port. For example, suppose you want to define the following port filters:

- An Ethernet Type filter to deny all IP frames
- A MAC address filter to deny all frames from a specific MAC address.

In this scenario, IP frames represent the majority of the traffic that must be filtered out. By applying Ethernet Type filters first, you ensure that the largest percentage of unwanted traffic will be discarded in the shortest amount of time. MAC address filters should be applied second because this filter type is expected to filter out a smaller percentage of traffic.

Using Mask Values in Filters

The following transparent bridge filters enable you to use mask values to increase the effectiveness of the filter:

- Ethernet Type
- MAC address
- Sliding window

When you specify a value to be used by a filter, such as a MAC address, that value is compared to the corresponding value in an inbound or outbound frame. A mask value identifies the bits in the filter value that are to be treated as significant. Each bit in the mask corresponds to an identical bit in the filter value. For every bit set to one in the mask, the same bit in the filter value is treated as significant. When the filter is applied, it compares the significant bits in the filter value against the corresponding bits in an inbound or outbound frame. The result of this comparison is determined by the Filtering mode parameter. Frames that correspond to the significant bits in the filter value are either allowed, if the filtering mode is **Permit**, or rejected, if the filtering mode is **Deny**.

In the following example, the filter value is X'FFC1' and the mask for that value is X'FFC1'. The example shows the significant bit positions identified by the mask.

```
Filter value:              X'FFC1' =  B'1111 1111 1100 0001'
Mask:                      X'FFC1' =  B'1111 1111 1100 0001'
Significant bits (X):                   XXXX XXXX XX-- ---X
```

If a mask was not used in the example, the filter could permit or deny only frames containing the value X'FFC1'. By using a mask, the range of the filter is extended to permit or deny all frames with odd number values between X'FFC1' and X'FFFF':

```
X'FFC1' = B'1111 1111 1100 0001'    X'FFD1' = B'1111 1111 1101 0001'
X'FFC3' = B'1111 1111 1100 0011'    X'FFD3' = B'1111 1111 1101 0011'
X'FFC5' = B'1111 1111 1100 0101'    X'FFD5' = B'1111 1111 1101 0101'
X'FFC7' = B'1111 1111 1100 0111'    X'FFD7' = B'1111 1111 1101 0111'
X'FFC9' = B'1111 1111 1100 1001'    X'FFD9' = B'1111 1111 1101 1001'
X'FFCC' = B'1111 1111 1100 1011'    X'FFDC' = B'1111 1111 1101 1011'
X'FFCE' = B'1111 1111 1100 1101'    X'FFDE' = B'1111 1111 1101 1101'
X'FFCF' = B'1111 1111 1100 1111'    X'FFDF' = B'1111 1111 1101 1111'

X'FFE1' = B'1111 1111 1110 0001'    X'FFF1' = B'1111 1111 1111 0001'
X'FFE3' = B'1111 1111 1110 0011'    X'FFF3' = B'1111 1111 1111 0011'
X'FFE5' = B'1111 1111 1110 0101'    X'FFF5' = B'1111 1111 1111 0101'
X'FFE7' = B'1111 1111 1110 0111'    X'FFF7' = B'1111 1111 1111 0111'
X'FFE9' = B'1111 1111 1110 1001'    X'FFF9' = B'1111 1111 1111 1001'
X'FFEC' = B'1111 1111 1110 1011'    X'FFFC' = B'1111 1111 1111 1011'
X'FFEE' = B'1111 1111 1110 1101'    X'FFFE' = B'1111 1111 1111 1101'
X'FFEF' = B'1111 1111 1110 1111'    X'FFFF' = B'1111 1111 1111 1111'
```

Note: Bits that are not significant are ignored by the filter. When a mask of all 0s is used, no bits are considered significant; therefore no filtering occurs. When a mask of all 1s is used, all bits are considered significant; therefore only the value specified for the filter is permitted or denied by the filter.

Defining Static Destination Address Filters

The filtering database that the 6611 maintains for transparent bridging can contain up to 4096 static destination address filters. These filters are applied to inbound frames received on ports enabled for transparent bridging.

The IEEE 802.1D standard for MAC bridges defines 16 default static destination address filters, which are automatically included in the filtering database. The 16 default filters include the bridge group address X'01 80 C2 00 00 00' and reserved MAC addresses X'01 80 C2 00 00 01' through X'01 80 C2 00 00 0F' (in canonical form). You can define an additional 4080 filters using the node-level parameters for transparent bridging. When a frame is received on a transparent bridge port with a destination MAC address that matches one of these filters, the frame is discarded by the bridge.

Note: If the 6611 is being defined as a translational bridge, you can define static destination address filters using the node-level parameters for translational bridging.

Because static destination address filters are processed before individual port filters, these filters offer a performance advantage. However, because static destination address filters apply to all transparent bridge ports, these filters should be used only if a destination address needs to be filtered on all ports for inbound frames.

Configuration Options

Each Ethernet LAN is attached to the 6611 by means of an Ethernet adapter or serial/Ethernet combination adapter. When configuring the 6611 as a transparent bridge, the transparent bridging function must be configured at the node level and on each Ethernet port over which frames will be bridged. In addition, transparent bridging needs to be configured on each serial port connected to a remote transparent bridge or translational bridge.

Note: To perform remote transparent bridging, you must select either PPP or frame relay as the frame encapsulation method for the serial port.

When configuring the 6611 as a translational bridge, the translational bridging function must be configured at the node level. Transparent bridging is configured on each Ethernet port over which frames will be bridged. When remotely bridging Ethernet frames between the translational bridge and another 6611 bridge, the configuration of the serial port depends upon how the remote bridge is being defined. If the remote bridge is a translational bridge, it is recommended that dual mode bridging be defined on each end of the serial link. Otherwise, transparent bridging should be defined on each end of the link.

Table 5-39 on page 5-49 summarizes the configuration options for transparent bridging.

Table 5-39. Transparent Bridging Configuration Options

WHEN configuring Transparent Bridging...	THEN optionally...
...on an Ethernet port, or a serial port using PPP: • Enable transparent bridging on the port. • When the 6611 is being defined as a translational bridge, specify an emulated ring number for the port.	• Specify the maximum transmission unit size. • Specify how the port state is determined (automatically by the spanning tree algorithm or manually set). – If the spanning tree mode is set to **Automatic**, specify the port priority and path cost. – If the spanning tree mode is set to **Manual**, specify whether the port is disabled or in the forwarding state. • Define transparent bridge port filters. The filters are accessed through a separate push button on the port window.
...on an serial port using frame relay: • Enable transparent bridging on the port. • Specify the DLCIs that will be used by the 6611 for remote transparent bridging over a frame relay network. When the 6611 is being defined as a translational bridge, each DLCI must be mapped to an emulated ring number, which identifies the frame-relay connection. **Note:** You need to assign a set of DLCIs to the frame-relay port before specifying which DLCIs may be used for transparent bridging. You assign DLCIs when defining the frame-relay protocol on the port.	• Specify the maximum transmission unit size. • Specify how the port state is determined (automatically by the spanning tree algorithm or manually set). – If the spanning tree mode is set to **Automatic**, specify the port priority and path cost. – If the spanning tree mode is set to **Manual**, specify whether the port is disabled or in the forwarding state. • Define transparent bridge port filters. The filters are accessed through a separate push button on the port window.
...at the node level: • Enable transparent bridging if the 6611 is being configured as a transparent bridge. (If the 6611 is being configured as a translational bridge, see "Translational Bridging" on page 5-75.)	• Specify whether the Duplicate Address Check protocol is supported • Specify filtering database options: – Overflow policy – Aging time – Static destination address filters • Specify spanning tree parameters: – Bridge priority – Hello time – Forward delay – Max age • Change the order in which port filters are applied.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform transparent bridging. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-40 (Page 1 of 2). Transparent Bridging Configuration Verification Checklist

Transparent Bridging Rule	**Configuration Parameter**	√
Node-Level Parameters:		
Ensure that the Enable transparent bridging parameter is enabled.	Enable Transparent Bridging	
Ensure that the Duplicate address check parameter is set to the same value on both 6611s.	Duplicate address check	
Port-Level Parameters:		
Ensure that transparent bridging is enabled on at least one token-ring or Ethernet port on the 6611 and that the physical interface on that port is enabled. If all ports on 6611 are serial ports, each port that performs transparent bridging in the network must have a unique transparent bridging priority.	Enable physical interface on this port	
	Enable Transparent Bridging on this port	
	Bridge priority	
Ensure that at least one Ethernet or token-ring port has a valid MAC address configured.	MAC address	
Ensure that the Enable transparent bridging on this port parameter is enabled on two or more ports on each 6611.	Enable Transparent Bridging on this port	
If there is more than one transparent bridging connection between two 6611s: • The Determine port state automatically parameter should be disabled. • The Port state parameter should be set to **Forwarding**.	Determine port state automatically	
	Port state	
Ensure that the transparent bridging connection between the two 6611s includes at least one pair of Ethernet or serial ports that have the Physical interface parameter enabled.	Physical interface	
Ethernet and serial ports configured for transparent bridging should be configured for IP.	Enable IP routing on this port	
	IP address	
For transparent bridging across serial connections, the following parameters must be the same: • Data encoding • Framing method	Data encoding	
	Framing method	
For Ethernet connections only:		
When inbound or outbound source SAP filters are set with the **Deny** option, the list of SAP filters must not contain SAP 00 or the SAP for any protocol to be bridged through that interface. When inbound or outbound source SAP filters are set with the **Permit** option, the list of SAP filters must contain SAP 00 and the SAPs for each protocol to be bridged through that interface.	Source SAP value	
	Filtering mode	

Table 5-40 (Page 2 of 2). Transparent Bridging Configuration Verification Checklist		
Transparent Bridging Rule	**Configuration Parameter**	√
When inbound or outbound Ethernet type filters are configured with the **Deny** option, the list must not contain types and masks that block the protocols that are to be bridged. When inbound or outbound Ethernet type filters are configured with the **Permit** option, the list must contain types and masks that allow the intended protocols to be bridged.	Type field	
	Type mask	
When inbound or outbound MAC address filters are configured with the **Deny** option, the list must not contain source addresses, destination addresses, and masks that block the devices that are intended to communicate via bridging. When inbound or outbound MAC address filters are configured with the **Permit** option,the list must contain source addresses, destination addresses, and masks that block the devices that are intended to communicate via bridging.	Source	
	Destination	
	Source mask	
	Destination mask	

Sample Network Graphic

Figure 5-5 on page 5-52 shows two 6611s configured to perform remote transparent bridging over a pair of serial links, one a primary link and the other a backup link.

The sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running PPP and configured for remote transparent bridging
  - An Ethernet port configured for transparent bridging
- 6611 B, which has the following port types and protocols running:
  - A serial port running PPP and configured for remote transparent bridging
  - An Ethernet port configured for transparent bridging

Slot and port numbers in Figure 5-5 on page 5-52 are abbreviated S*x* P*y*.

In this sample configuration, the primary link is attached to serial port port 1 on both 6611 A and 6611 B. The backup link is attached to serial port port 2 on each 6611. The primary link will forward transparent bridge frames, while the backup link is in a standby or *blocking* state and does not forward frames. If the primary link fails, the spanning tree automatically causes the backup link to become active and begin forwarding frames.

Note: In bridging, the port with the numerically lower port priority has the higher spanning tree forwarding priority. In the sample configuration, the network administrator has assigned a lower port priority to the link associated with serial port 1. Therefore, that link becomes the primary serial link in the configuration.

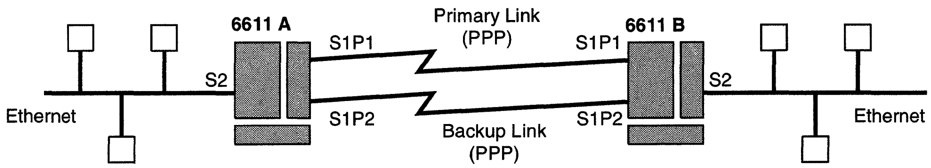


Figure 5-5. Sample Network Using Remote Transparent Bridging over PPP

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-5. The following tables list the configuration parameters for the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 5-41. Serial Port Parameter Configured - Primary Link

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Data link protocol	PPP	PPP

Table 5-42. Serial Port - Physical Interface Parameters Configured - Primary Link

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink Serial Number	None	None
Transmit clock source	DTE	DTE
Serial Line Speed	56000	56000
Data Encoding	NRZI	NRZI
Locally Administered MAC Address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-43. Serial Port - PPP Parameters Configured - Primary Link

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size (octets)	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-44. Serial Port - Transparent Bridging Parameters Configured - Primary Link

Parameter	6611 A Slot 1 Port 1 Value	6611 B Slot 1 Port 1 Value
Enable Transparent Bridging on this port	Enable	Enable
Maximum transmission unit size	1500	1500
Spanning tree mode	Automatic	Automatic
Port priority	80	80
Path cost	0	0
Port state	NA	NA
Required for Translational Bridging only		
Emulated ring number	None	None

Table 5-45. Serial Port Parameter Configured - Backup Link

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-46. Serial Port - Physical Interface Parameters Configured - Backup Link

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56000	56000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-47. Serial Port - PPP Parameters Configured - Backup Link

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size (octets)	1500	1500
Use magic number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-48. Serial Port - Transparent Bridging Parameters Configured - Backup Link

Parameter	**6611 A Slot 1 Port 2 Value**	**6611 B Slot 1 Port 2 Value**
Enable Transparent Bridging on this port	Enable	Enable
Maximum transmission unit size (octets)	1500	1500
Spanning tree mode	Automatic	Automatic
Port priority	80	80
Path cost	0	0
Port state	NA	NA
Required for Translational Bridging only		
Emulated ring number	None	None

Ethernet Ports and the Protocols Running on Them

Table 5-49. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	NA	NA

Table 5-50. Ethernet Port - Transparent Bridging Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Transparent Bridging on this port	Enable	Enable
Maximum transmission unit size	1500	1500
Spanning tree mode	Automatic	Automatic
Port priority	80	80
Path cost	0	0
Port state	NA	NA
Emulated ring number (for Translational Bridging only)	None	None

Node-Level Parameters Configured

Table 5-51. Node Level - Transparent Bridge Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Transparent Bridging	Enable	Enable
Duplicate address check	Filter	Filter
Overflow policy	Learn	Learn
Aging time	300	300
Spanning tree parameters		
Bridge priority	8000	8000
Hello time	2	2
Forward delay	15	15
Max age	20	20

Port Level Worksheets

Figure 5-6 on page 5-56 and Figure 5-7 on page 5-56 show the paths for configuring transparent bridging and transparent bridge filters through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-6 on page 5-56 and Figure 5-7 on page 5-56.

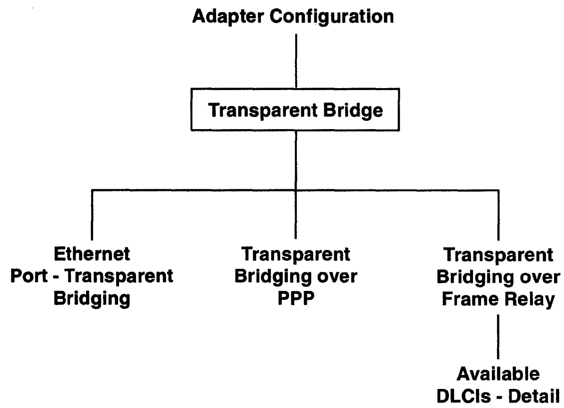


Figure 5-6. Flow of Port-Level Transparent Bridge Windows

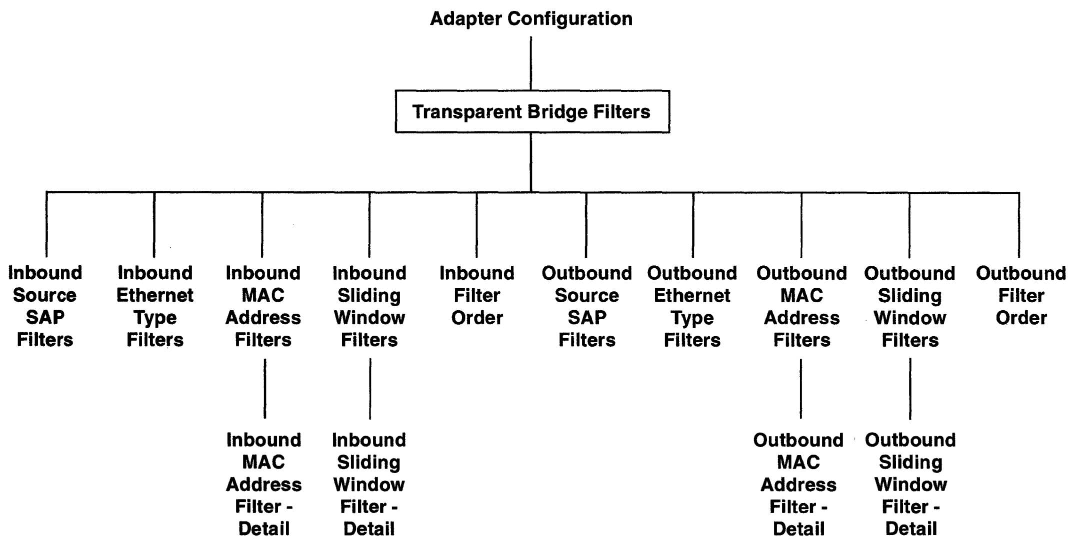


Figure 5-7. Flow of Port-Level Transparent Bridge Filter Windows

Use the following tables as worksheets to configure transparent bridging at the port level:

- Ethernet Port - Transparent Bridging on page 5-57
- Transparent Bridging over PPP on page 5-58
- Transparent Bridging over Frame Relay on page 5-60

- Inbound Source SAP Filters on page 5-62
- Inbound Ethernet Type Filters on page 5-63
- Inbound MAC Address Filters on page 5-63
- Inbound Sliding Window Filters on page 5-64
- Inbound Filter Order on page 5-66

- Outbound Source SAP Filters on page 5-66
- Outbound Ethernet Type Filters on page 5-67
- Outbound MAC Address Filters on page 5-68
- Outbound Sliding Window Filters on page 5-69
- Outbound Filter Order on page 5-70

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter.

If you are working with an ASCII-formatted configuration file, refer to Table D-22 on page D-17 for a mapping of parameter names and their associated labels.

Table 5-52 (Page 1 of 2). Configuration Worksheet - Ethernet Port - Transparent Bridging

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable Transparent Bridging on this port Enable, Disable Disable This parameter enables or disables transparent bridging on a port.	
Parameter **Valid Values** **Default Value** **Description**	Maximum transmission unit size 128 to 1500 bytes 1500 bytes This parameter specifies the size of the largest transmission unit that the transparent bridge can transmit and receive on a port. For an Ethernet V2.0 frame, the transmission unit is the Data field in the frame. For an IEEE 802.3 frame, the transmission unit is the logical link control (LLC) PDU in the frame.	
Parameter **Valid Values** **Default Value** **Description**	Spanning tree mode Automatic, Manual Automatic This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually configured. When **Automatic** is selected, the spanning tree determines the port state using: • The spanning tree parameters for the bridge configured at the node level • Information received from other bridges in BPDUs • Information provided by the Port priority and Path cost parameters When **Manual** is selected, you can control the forwarding of frames through the port by configuring the Port state parameter.	
Parameter **Valid Values** **Default Value** **Description**	Port priority X'00' to X'FF', where X'00' is the *highest* priority value and X'FF' is the *lowest* priority value X'80' This parameter specifies the priority of the transparent bridge port. The port priority is used to select the *preferred port* when: • Two or more transparent bridge ports are connected to the same Ethernet segment in a redundant configuration. (The spanning tree allows a path through only one of the ports.) • Two or more transparent bridge ports have equal path costs to the root bridge and represent paths through the same *designated bridge*. The designated bridge is the next closest bridge to the root bridge. If ports have equal priorities, then the port with the lowest port number is the preferred port. Port numbers are assigned automatically by the 6611.	
Parameter **Valid Values** **Default Value** **Description**	Path cost 0 to 65535 0 (cost calculated using path cost formula) This parameter is the contribution of the port to the total cost of the paths to the root bridge. For a value of zero, the path cost is calculated using the formula: 1000 / (media speed in Mbps) The media speed used for Ethernet is 10 Mbps.	

Table 5-52 (Page 2 of 2). Configuration Worksheet - Ethernet Port - Transparent Bridging

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Port state Forwarding, Disabled Disabled When the spanning tree mode is set to **Manual**, this parameter specifies the port state. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames. When this parameter is configured, it overrides the port state that would have been selected by the spanning tree algorithm. Because the spanning tree algorithm cannot automatically disable a port, you must ensure that the port does not cause a loop in the network when it is in the forwarding state.	
Parameter **Valid Values** **Default Value** **Description**	Emulated ring number (required for Translational bridging only) X'001' to X'FFF' None When the 6611 is operating as a translational bridge, this parameter specifies a value that is interpreted as the ring number for the LAN segment attached to the port. This value is placed in the routing information (RI) field of route discovery frames transmitted from source route bridge ports. The value is stored in the token-ring database maintained by the translational bridge and is used to forward token-ring frames to this port from ports configured for source route bridging. The ring number value is not used for transparent bridging. **Note:** The emulated ring number you specify must be unique within the bridged network and the 6611. Even if two ports on a 6611 are attached to the same Ethernet LAN segment, they require different emulated ring numbers because the emulated ring numbers identify these ports to other ports configured for source route bridging.	

Table 5-53 (Page 1 of 3). Configuration Worksheet - Transparent Bridging over PPP

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable Transparent Bridging on this port Enable, Disable Disable This parameter enables or disables transparent bridging on a port.	
Parameter **Valid Values** **Default Value** **Description**	Maximum transmission unit size 128 to 1500 bytes 1500 bytes This parameter specifies the size of the largest transmission unit that the transparent bridge can transmit and receive on a port. For an Ethernet V2.0 frame, the transmission unit is the Data field in the frame. For an IEEE 802.3 frame, the transmission unit is the logical link control (LLC) PDU in the frame.	

Table 5-53 (Page 2 of 3). Configuration Worksheet - Transparent Bridging over PPP

<table>
<tr><th colspan="2">Parameter Information</th><th>Your Value</th></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Spanning tree mode
Automatic, Manual
Automatic
This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually configured. When Automatic is selected, the spanning tree determines the port state using:
• The spanning tree parameters for the bridge configured at the node level
• Information received from other bridges in BPDUs
• Information provided by the Port priority and Path cost parameters

When Manual is selected, you can control the forwarding of frames through the bridge by configuring the Port state parameter.</td><td></td></tr>
<tr><td>Parameter
Valid Values

Default Value
Description</td><td>Port priority
X'00' to X'FF', where X'00' is the highest priority value and X'FF' is the lowest priority value.
X'80'
This parameter specifies the priority of the transparent bridge port. The port priority is used to select the preferred port when:
• Two or more transparent bridge ports are connected to the same Ethernet segment in a redundant configuration. (The spanning tree allows a path through only one of the ports.)
• Two or more transparent bridge ports have equal path costs to the root bridge and represent paths through the same designated bridge. The designated bridge is the next closest bridge to the root bridge.

If ports have equal priorities, then the port with the lowest port number is the preferred port. Port numbers are assigned automatically by the 6611.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Path cost
0 to 65535
0 (cost calculated using path cost formula)
This parameter is the contribution of the port to the total cost of the paths to the root bridge. For a value of zero, the path cost is calculated using the formula:
1000 / (media speed in Mbps)

The media speed for PPP is 0.0096 (9600 bps) to 2.048 Mbps, depending on the line speed configured for the serial port.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Port state
Forwarding, Disabled
Disabled
When the spanning tree mode is set to Manual, this parameter specifies the port state. Select Forwarding to have the port permanently participate in frame forwarding. Select Disabled to permanently stop the port from forwarding frames. When this parameter is configured, it overrides the port state that would have been selected by the spanning tree algorithm. Because the spanning tree algorithm cannot automatically disable a port, you must ensure that the port does not cause a loop in the network when it is in the forwarding state.</td><td></td></tr>
</table>

Table 5-53 (Page 3 of 3). Configuration Worksheet - Transparent Bridging over PPP

Parameter Information		Your Value
Parameter	Emulated ring number (required for Translational Bridging only)	
Valid Values	X'001' to X'FFF'	
Default Value	None	
Description	When the 6611 is operating as a translational bridge, this parameter specifies a value that is interpreted as the ring number for the link attached to the port. This value is placed in the routing information (RI) field of route discovery frames transmitted from source route bridge ports. The value is stored in the token-ring database maintained by the translational bridge and is used to forward token-ring frames to this port from ports configured for source route bridging. The ring number value is not used for transparent bridging. **Note:** The emulated ring number you specify must be unique within the bridged network and the 6611. Each emulated ring number identifies a specific port to other ports configured for source route bridging.	

Table 5-54 (Page 1 of 3). Configuration Worksheet - Transparent Bridging over Frame Relay

Parameter Information		Your Value
Parameter	Enable Transparent Bridging on this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables transparent bridging on a port.	
Parameter	Maximum transmission unit size	
Valid Values	128 to 1500 bytes	
Default Value	1500 bytes	
Description	This parameter specifies the size of the largest transmission unit that the transparent bridge can transmit and receive on a port. For an Ethernet V2.0 frame, the transmission unit is the Data field in the frame. For an IEEE 802.3 frame, the transmission unit is the logical link control (LLC) PDU in the frame.	
Parameter	Spanning tree mode	
Valid Values	Automatic, Manual	
Default Value	Automatic	
Description	This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually configured. When **Automatic** is selected, the spanning tree determines the port state using: • The spanning tree parameters for the bridge configured at the node level • Information received from other bridges in BPDUs • Information provided by the Port priority and Path cost parameters When **Manual** is selected, you can control the forwarding of frames through the bridge by configuring the Port state parameter.	

Table 5-54 (Page 2 of 3). Configuration Worksheet - Transparent Bridging over Frame Relay

Parameter Information	Your Value
Parameter Port priority **Valid Values** X'00' to X'FF', where X'00' is the *highest* priority value and X'FF' is the *lowest* priority value. **Default Value** X'80' **Description** This parameter specifies the priority of the transparent bridge port. The port priority is used to select the *preferred port* when: • Two or more transparent bridge ports are connected to the same Ethernet segment in a redundant configuration. (The spanning tree allows a path through only one of the ports.) • Two or more transparent bridge ports have equal path costs to the root bridge and represent paths through the same *designated bridge*. The designated bridge is the next closest bridge to the root bridge. If ports have equal priorities, then the port with the lowest port number is the preferred port. Port numbers are assigned automatically by the 6611.	
Parameter Path cost **Valid Values** 0 to 65535 **Default Value** 0 (cost calculated using path cost formula) **Description** This parameter is the contribution of the port to the total cost of the paths to the root bridge. For a value of zero, the path cost is calculated using the formula: 1000 / (media speed in Mbps) The media speed for frame relay is 0.0096 (9600 bps) to 2.048 Mbps, depending on the line speed configured for the serial port.	
Parameter Port state **Valid Values** Forwarding, Disabled **Default Value** Disabled **Description** When the spanning tree mode is set to **Manual**, this parameter specifies the port state. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames. When this parameter is configured, it overrides the port state that would have been selected by the spanning tree algorithm. Because the spanning tree algorithm cannot automatically disable a port, you must ensure that the port does not cause a loop in the network when it is in the forwarding state.	
DLCI List - Parameter(s) configured for each DLCI defined	
Parameter DLCI number (required for each DLCI defined) **Valid Values** Any available DLCI in the port list **Default Value** None **Description** This parameter identifies a DLCI that will be used to transmit transparent bridge frames over a frame relay network. You can select any of the DLCIs defined for the frame relay port. (See Table 4-21 on page 4-16 for information on defining DLCIs for the port.) You must select at least one DLCI to successfully configure transparent bridging on the port.	

Table 5-54 (Page 3 of 3). Configuration Worksheet - Transparent Bridging over Frame Relay

Parameter Information		Your Value
Parameter	Emulated ring number (required for Translational Bridging only)	
Valid Values	X'001' to X'FFF'	
Default Value	None	
Description	When the 6611 is operating as a translational bridge, each DLCI defined must be mapped to an emulated ring number. The ring number uniquely identifies a frame-relay connection between this bridge and a remote bridge. The emulated ring number is placed in the routing information (RI) field of route discovery frames transmitted from source route bridge ports. The value is stored in the token-ring database maintained by the translational bridge and is used to forward token-ring frames to this port from ports configured for source route bridging. The ring number value is not used for transparent bridging. **Note:** The emulated ring number you specify must be unique within the bridged network and the 6611. Each emulated ring number identifies a specific DLCI on this port to other ports configured for source route bridging.	

Note: A maximum of 240 DLCIs can be specified for transparent bridging on a port.

Table 5-55. Configuration Worksheet - Inbound Source SAP Filters

Parameter Information		Your Value
Parameter	Enable inbound source SAP filters on this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables all inbound source SAP filters defined for a transparent bridge port.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default Value	Deny	
Description	This parameter specifies how the inbound source SAP filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the source SAP values you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the SAP values you specify are bridged over the port.	
Filter List - Parameter configured for each filter defined		
Parameter	Source SAP value (required for each filter defined)	
Valid Values	X'00' to X'FE', in increments of 2	
Default Value	None	
Description	This parameter specifies the source SAP value used in the filter. The source SAP identifies the protocol contained in the frame. The filter compares this SAP value against all inbound source SAP values. The result of the comparison is determined by the setting of the Filtering mode parameter.	

Note:

- A maximum of 128 inbound source SAP filters can be defined on a port.
- The Null SAP value (00) is often used for session establishment by end stations regardless of the higher-layer protocol being used. Therefore, when the Filtering mode parameter is set to **Permit**, it is recommended that SAP X'00' be included in the list of filtered SAP values in addition to any specific protocol SAPs that are being allowed.

Table 5-56. Configuration Worksheet - Inbound Ethernet Type Filters

Parameter Information		**Your Value**
Parameter	Enable inbound Ethernet Type filters on this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables all inbound Ethernet Type filters defined for a transparent bridge port.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default Value	Deny	
Description	This parameter specifies how the inbound Ethernet Type filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the Ethernet Type values you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the Ethernet Type values you specify are bridged over the port.	
Filter List - Parameters configured for each filter defined		
Parameter	Type field (required for each filter defined)	
Valid Values	X'0000' to X'FFFF'	
Default Value	None	
Description	This parameter specifies the Ethernet Type field value used in the filter. The filter compares this value against the contents of the Type field in all inbound Ethernet frames. The Type field identifies the type of data encapsulated within an Ethernet V2.0 frame or an IEEE 802.3 frame with a SNAP header. The result of the comparison is determined by the setting of the Filtering mode parameter.	
Parameter	Type mask	
Valid Values	X'0000' to X'FFFF'	
Default Value	X'FFFF'	
Description	This parameter is a mask that identifies the significant bits in the Ethernet Type field value defined for the filter. The mask enables you to specify a range of Ethernet Type field values to be filtered.	

Note: A maximum of 32 inbound Ethernet Type filters can be defined on a port.

Table 5-57 (Page 1 of 2). Configuration Worksheet - Inbound MAC Address Filters

Parameter Information		**Your Value**
Parameter	Enable inbound MAC address filters on this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables all inbound MAC address filters defined for a transparent bridge port.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default Value	Deny	
Description	This parameter specifies how the inbound MAC address filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the MAC addresses you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the MAC addresses you specify are bridged over the port.	

Table 5-57 (Page 2 of 2). Configuration Worksheet - Inbound MAC Address Filters

Parameter Information	Your Value
Filter List - Parameters configured for each filter defined	
Parameter Source MAC address (required for each filter defined) **Valid Values** X'0000 0000 0000' to X'FFFF FFFF FFFF' **Default Value** None **Description** This parameter specifies the source MAC address used in the filter. The filter compares this MAC address against all inbound source MAC addresses. The result of the comparison is determined by the setting of the Filtering mode parameter.	
Parameter Destination MAC address (required for each filter defined) **Valid Values** X'0000 0000 0000' to X'FFFF FFFF FFFF' **Default Value** None **Description** This parameter specifies the destination MAC address used in the filter. The filter compares this MAC address against all inbound destination MAC addresses. The result of the comparison is determined by the setting of the Filtering mode parameter.	
Parameter Source MAC address mask **Valid Values** X'0000 0000 0000' to X'FFFF FFFF FFFF' **Default Value** X'FFFF FFFF FFFF' **Description** This parameter is a mask that identifies the significant bits in the source MAC address for the filter. The mask enables you to specify a range of source MAC addresses to be filtered.	
Parameter Destination MAC address mask **Valid Values** X'0000 0000 0000' to X'FFFF FFFF FFFF' **Default Value** X'FFFF FFFF FFFF' **Description** This parameter is a mask that identifies the significant bits in the destination MAC address for the filter. The mask enables you to specify a range of destination MAC addresses to be filtered.	
Parameter Form of MAC addresses **Valid Values** Canonical, Noncanonical **Default Value** Canonical **Description** This parameter specifies the format of the MAC addresses defined for this filter.	

Note: A maximum of 32 inbound MAC address filters can be defined on a port.

Table 5-58 (Page 1 of 2). Configuration Worksheet - Inbound Sliding Window Filters

Parameter Information	Your Value
Parameter Enable inbound sliding window filters on this port **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables all inbound sliding window filters defined for a transparent bridge port. A sliding window filter enables you to create a filter for any portion of an inbound frame. You define the contents of a *window area* (which is a block of bytes) and an appropriate offset value. The filter compares the window you define against a byte area at the same offset in an inbound frame. The result of this comparison is determined by the setting of the Filtering mode parameter.	

Table 5-58 (Page 2 of 2). Configuration Worksheet - Inbound Sliding Window Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the inbound sliding window filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the sliding window bytes you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the sliding window bytes you specify are bridged over the port.	
Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default Value** **Description**	Filter name (required for each filter defined) 1 to 16 characters None This parameter specifies the name of the sliding window filter.	
Parameter **Valid Values** **Default Value** **Description**	Offset starting field MAC, Data MAC This parameter specifies where the sliding window filter should be applied in an inbound frame. When you select **MAC**, the sliding window filter is applied at an offset calculated from the beginning of the frame. When you select **Data**, the sliding window filter is applied at an offset calculated from the beginning of the Data field in the frame. The size of the offset is determined by the Offset into frame parameter.	
Parameter **Valid Values** **Default Value** **Description**	Offset into frame 0 to 1513 bytes 0 This parameter specifies a byte offset used in calculating where the sliding window filter should be applied in an inbound frame.	
Parameter **Valid Values** **Default Value** **Description**	Sliding window contents (required for each filter defined) A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). The string must end on a byte boundary. None This parameter specifies the contents of the sliding window.	
Parameter **Valid Values** **Default Value** **Description**	Sliding window mask A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). Any bytes in the mask beyond what is specified for the sliding window contents are ignored. When the mask contains fewer bytes than the number of bytes specified for the sliding window contents, the missing bytes will be treated as zeros and the corresponding bytes in the sliding window contents will not be treated as significant. A string of 30 hexadecimal bytes, each with a value of X'FF' This parameter is a mask that identifies the significant bits in the string defined for the Sliding window contents parameter. The mask enables you to specify a range of strings to be filtered.	

Note: A maximum of 16 inbound sliding window filters can be defined on a port.

Table 5-59. Configuration Worksheet - Inbound Filter Order

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Override the default filter order set at the node level Enable, Disable Disable When this parameter is enabled, you can change the order in which inbound filter types are applied on the transparent bridge port being configured. The order you specify overrides the order defined for the bridge at the node level.	
Parameter **Valid Values** **Default Value** **Description**	Source SAP filter (required to reorder filters) 1 to 4, where 1 specifies that this filter type should be applied *first*, and 4 specifies that this filter type should be applied *last*. None This parameter controls when the inbound source SAP filter type is to be applied on the transparent bridge port being configured.	
Parameter **Valid Values** **Default Value** **Description**	Ethernet Type filter (required to reorder filters) 1 to 4, where 1 specifies that this filter type should be applied *first*, and 4 specifies that this filter type should be applied *last*. None This parameter controls when inbound Ethernet Type filters are to be applied on the transparent bridge port being configured.	
Parameter **Valid Values** **Default Value** **Description**	MAC address filter (required to reorder filters) 1 to 4, where 1 specifies that this filter type should be applied *first*, and 4 specifies that this filter type should be applied *last*. None This parameter controls when the inbound MAC address filter type is to be applied on the transparent bridge port being configured.	
Parameter **Valid Values** **Default Value** **Description**	Sliding window filter (required to reorder filters) 1 to 4, where 1 specifies that this filter type should be applied *first*, and 4 specifies that this filter type should be applied *last*. None This parameter controls when the inbound sliding window filter type is to be applied on the transparent bridge port being configured.	

Note: To override the default filter order established at the node level, you must specify a new value for each port filter type parameter.

Table 5-60 (Page 1 of 2). Configuration Worksheet - Outbound Source SAP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable outbound source SAP filters on this port Enable, Disable Disable This parameter enables or disables all outbound source SAP filters defined for a transparent bridge port.	
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the outbound source SAP filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames that contain the SAP values you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the SAP values you specify are bridged over the port.	

Table 5-60 (Page 2 of 2). Configuration Worksheet - Outbound Source SAP Filters

Parameter Information	Your Value
Filter List - Parameter configured for each filter defined	
Parameter Source SAP value (required for each filter defined) **Valid Values** X'00' to X'FE', in increments of 2 **Default Value** None **Description** This parameter specifies the source SAP value used in the filter. The source SAP identifies the protocol contained in the frame. The filter compares this SAP value against all outbound source SAP values. The result of the comparison is determined by the setting of the Filtering mode parameter.	

Note:

- A maximum of 128 outbound source SAP filters can be defined on a port.
- The Null SAP value (00) is often used for session establishment by end stations regardless of the higher-layer protocol being used. Therefore, when the Filtering mode parameter is set to **Permit**, it is recommended that SAP X'00' be included in the list of filtered SAP values in addition to any specific protocol SAPs that are being allowed.

Table 5-61. Configuration Worksheet - Outbound Ethernet Type Filters

Parameter Information	Your Value
Parameter Enable outbound Ethernet Type filters on this port **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables all outbound Ethernet Type filters defined for a transparent bridge port.	
Parameter Filtering mode **Valid Values** Deny, Permit **Default Value** Deny **Description** This parameter specifies how the outbound Ethernet Type filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames that contain the Ethernet Type values you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the Ethernet Type values you specify are bridged over the port.	
Filter List - Parameters configured for each filter defined	
Parameter Type field (required for each filter defined) **Valid Values** X'0000' to X'FFFF' **Default Value** None **Description** This parameter specifies the Ethernet Type field value used in the filter. The filter compares this value against the contents of the Type field in all outbound Ethernet frames. The Type field identifies the type of data encapsulated within an Ethernet V2.0 frame or an IEEE 802.3 frame with a SNAP header. The result of the comparison is determined by the setting of the Filtering mode parameter.	
Parameter Type mask **Valid Values** X'0000' to X'FFFF' **Default Value** X'FFFF' **Description** This parameter is a mask that identifies the significant bits in the Ethernet Type field value defined for the filter. The mask enables you to specify a range of Ethernet Type field values to be filtered.	

Note: A maximum of 32 outbound Ethernet Type filters can be defined on a port.

Table 5-62. Configuration Worksheet - Outbound MAC Address Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable outbound MAC address filters on this port Enable, Disable Disable This parameter enables or disables all outbound MAC address filters defined for a transparent bridge port.	
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the outbound MAC address filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames that contain the MAC addresses you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the MAC addresses you specify are bridged over the port.	
Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default Value** **Description**	Source MAC address (required for each filter defined) X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter specifies the source MAC address used in the filter. The filter compares this MAC address against all outbound source MAC addresses. The result of the comparison is determined by the setting of the Filtering mode parameter.	
Parameter **Valid Values** **Default Value** **Description**	Destination MAC address (required for each filter defined) X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter specifies the destination MAC address used in the filter. The filter compares this MAC address against all outbound destination MAC addresses. The result of the comparison is determined by the setting of the Filtering mode parameter.	
Parameter **Valid Values** **Default Value** **Description**	Source MAC address mask X'0000 0000 0000' to X'FFFF FFFF FFFF' X'FFFF FFFF FFFF' This parameter is a mask that identifies the significant bits in the source MAC address for the filter. The mask enables you to specify a range of source MAC addresses to be filtered.	
Parameter **Valid Values** **Default Value** **Description**	Destination MAC address mask X'0000 0000 0000' to X'FFFF FFFF FFFF' X'FFFF FFFF FFFF' This parameter is a mask that identifies the significant bits in the destination MAC address for the filter. The mask enables you to specify a range of destination MAC addresses to be filtered.	
Parameter **Valid Values** **Default Value** **Description**	Form of MAC addresses Canonical, Noncanonical Canonical This parameter specifies the format of the MAC addresses defined for this filter.	

Note: A maximum of 32 outbound MAC address filters can be defined on a port.

Table 5-63 (Page 1 of 2). Configuration Worksheet - Outbound Sliding Window Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable outbound sliding window filters on this port Enable, Disable Disable This parameter enables or disables all outbound sliding window filters defined for a transparent bridge port. A sliding window filter enables you to create a filter for any portion of an outbound frame. You define the contents of a *window area* (which is a block of bytes) and an appropriate offset value. The filter compares the window you define against a byte area at the same offset in an outbound frame. The result of this comparison is determined by the setting of the Filtering mode parameter.	
Parameter **Valid Values** **Default Value** **Description**	Filtering mode Deny, Permit Deny This parameter specifies how the outbound sliding window filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the sliding window bytes you specify are bridged over the port. All other frames are rejected. When this parameter is set to **Deny**, all frames *except* those that contain the sliding window bytes you specify are bridged over the port.	
Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default Value** **Description**	Filter name (required for each filter defined) 1 to 16 characters None This parameter specifies the name of the sliding window filter.	
Parameter **Valid Values** **Default Value** **Description**	Offset starting field MAC, Data MAC This parameter specifies where the sliding window filter should be applied in an outbound frame. When you select **MAC**, the sliding window filter is applied at an offset calculated from the beginning of the frame. When you select **Data**, the sliding window filter is applied at an offset calculated from the beginning of the Data field in the frame. The size of the offset is determined by the Offset into frame parameter.	
Parameter **Valid Values** **Default Value** **Description**	Offset into frame 0 to 1513 bytes 0 This parameter specifies a byte offset used in calculating where the sliding window filter should be applied in an outbound frame.	
Parameter **Valid Values** **Default Value** **Description**	Sliding window contents (required for each filter defined) A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). The string must end on a byte boundary. None This parameter specifies the contents of the sliding window.	

Table 5-63 (Page 2 of 2). Configuration Worksheet - Outbound Sliding Window Filters

Parameter Information		Your Value
Parameter	Sliding window mask	
Valid Values	A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). Any bytes in the mask beyond what is specified for the sliding window contents are ignored. When the mask contains fewer bytes than the number of bytes specified for the sliding window contents, the missing bytes will be treated as zeros and the corresponding bytes in the sliding window contents will not be treated as significant.	
Default Value	A string of 30 hexadecimal bytes, each with a value of X'FF'	
Description	This parameter is a mask that identifies the significant bits in the string defined for the Sliding window contents parameter. The mask enables you to specify a range of strings to be filtered.	

Note: A maximum of 16 outbound sliding window filters can be defined on a port.

Table 5-64. Configuration Worksheet - Outbound Filter Order

Parameter Information		Your Value
Parameter	Override the default filter order set at the node level	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	When this parameter is enabled, you can change the order in which outbound filter types are applied on the transparent bridge port being configured. The order you specify overrides the order defined for the bridge at the node level.	
Parameter	Source SAP filter (required to reorder filters)	
Valid Values	1 to 4, where 1 specifies that this filter type should be applied *first*, and 4 specifies that this filter type should be applied *last*.	
Default Value	None	
Description	This parameter controls when the outbound source SAP filter type is to be applied on the transparent bridge port being configured.	
Parameter	Ethernet Type filter (required to reorder filters)	
Valid Values	1 to 4, where 1 specifies that this filter type should be applied *first*, and 4 specifies that this filter type should be applied *last*.	
Default Value	None	
Description	This parameter controls when outbound Ethernet Type filters are to be applied on the transparent bridge port being configured.	
Parameter	MAC address filter (required to reorder filters)	
Valid Values	1 to 4, where 1 specifies that this filter type should be applied *first*, and 4 specifies that this filter type should be applied *last*.	
Default Value	None	
Description	This parameter controls when the outbound MAC address filter type is to be applied on the transparent bridge port being configured.	
Parameter	Sliding window filter (required to reorder filters)	
Valid Values	1 to 4, where 1 specifies that this filter type should be applied *first*, and 4 specifies that this filter type should be applied *last*.	
Default Value	None	
Description	This parameter controls when the outbound sliding window filter type is to be applied on the transparent bridge port being configured.	

Note: To override the default filter order established at the node level, you must specify a new value for each port filter type parameter.

Node Level Worksheets

Figure 5-8 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-8.

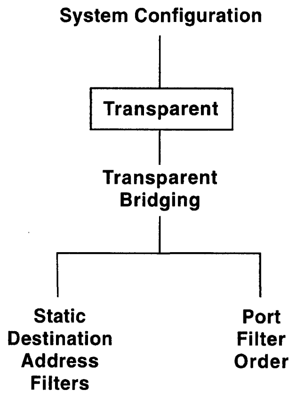


Figure 5-8. Flow of Node-Level Transparent Bridging Help Windows

Use the following tables as worksheets to configure transparent bridging at the node level:

- Transparent Bridging on page 5-71
- Static Destination Address Filters on page 5-73
- Port Filter Order on page 5-73

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-22 on page D-17 for a mapping of parameter names and their associated labels.

Table 5-65 (Page 1 of 3). Configuration Worksheet - Transparent Bridging

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable Transparent Bridging Enable, Disable Disable This parameter enables or disables transparent bridging on the 6611. Transparent bridging also must be enabled on individual adapter ports.	
Parameter **Valid Values** **Default Value** **Description**	Duplicate address check Forward, Filter Filter This parameter specifies whether the transparent bridge supports the IEEE 802.2 Duplicate Address Check protocol for Ethernet frames. Select **Forward** to instruct the bridge to forward all frames that have identical source and destination MAC addresses. This option allows the detection of duplicate MAC addresses in the network. Select **Filter** to instruct the bridge to discard frames that have identical source and destination MAC addresses. This option reduces the amount of traffic in the network.	

Table 5-65 (Page 2 of 3). Configuration Worksheet - Transparent Bridging

Parameter Information	**Your Value**
Filtering Database	
Parameter Overflow policy **Valid Values** Learn, Do not learn **Default Value** Learn **Description** This parameter specifies how the transparent bridge should handle a new entry for the filtering database if the database is full. Select **Learn** to instruct the bridge to discard an old entry in the database and replace it with the new entry. Select **Do not learn** to instruct the bridge to discard the new entry, leaving the database unchanged. The filtering database can contain up to 4096 entries.	
Parameter Aging time **Valid Values** 10 to 1 000 000 seconds **Default Value** 300 seconds **Description** This parameter specifies the number of seconds that a dynamic entry can remain in the filtering database without the transparent bridge observing any activity from that address. When the age of an entry equals the aging time, the bridge deletes the entry from the filtering database.	
Spanning Tree Parameters	
Parameter Bridge priority **Valid Values** X'0000' to X'FFFF', where X'0000' is the *highest* priority value and X'FFFF' is the *lowest* priority value **Default Value** X'8000' **Description** This parameter specifies the priority of this transparent bridge. When this bridge is activated, its priority value is compared to the priority values of other active bridges in the network. The bridge with the highest priority becomes the root bridge of the spanning tree. When the highest priority value in the network is shared by two or more bridges, the bridges compare port MAC addresses (one port on each bridge is selected for this purpose). The bridge with the lowest value MAC address becomes the root bridge.	
Parameter Hello time **Valid Values** 1 to 10 seconds **Default Value** 2 seconds **Description** When this bridge is selected as the root bridge, this parameter specifies how often this bridge transmits configuration bridge protocol data units (BPDUs). BPDUs contain information about the topology of the spanning tree and reflect changes to the topology.	
Parameter Forward delay **Valid Values** 4 to 30 seconds **Default Value** 15 seconds **Description** When this bridge is selected as the root bridge, the value of this parameter specifies how long ports in all bridges remain in either a listening state or learning state. When the forward delay time expires, ports in the listening state go into the learning state and ports in the learning state go into the forwarding state. State changes occur as the result of changes in the topology of the spanning tree, such as when an active bridge fails or is shut down. To keep the information in the filtering database current, the value of this parameter also is used as the value of the Aging time parameter for a short period after a topology change occurs.	

Table 5-65 (Page 3 of 3). Configuration Worksheet - Transparent Bridging

Parameter Information		Your Value
Parameter	Max age	
Valid Values	6 to 40 seconds	
Default Value	20 seconds	
Description	When this bridge is selected as the root bridge, the value of this parameter specifies how long other active bridges are to store the topology information received from configuration bridge protocol data units (BPDUs). When this information reaches its maximum age limit without being replaced, the active bridges in the network discard it and assume the root bridge or the path to the root bridge has failed. A new root bridge or path is then selected.	

Table 5-66. Configuration Worksheet - Static Destination Address Filters

Parameter Information		Your Value
Destination MAC Address List - Parameters configured for each filter defined		
Parameter	Static destination MAC address (required for each filter defined)	
Valid Values	X'0000 0000 0000' to X'FFFF FFFF FFFF'	
Default Value	None	
Description	This parameter specifies a static destination MAC address that is placed in the filtering database. The bridge discards any frame it receives on a bridge port with the specified destination address. This address is *static* because it remains in the filtering database until you remove or change it. Each static address you define reduces the amount of space available in the filtering database for dynamic entries. This parameter affects only frames handled by the transparent bridge. Routed frames are not affected by this parameter.	
Parameter	Form of MAC address	
Valid Values	Canonical, Noncanonical	
Default Value	Canonical	
Description	This parameter specifies how the 6611 should interpret the static destination MAC address defined for the filter. The address can be in canonical form or noncanonical form.	

Note: A maximum of 4080 static destination address filters can be defined.

Table 5-67 (Page 1 of 2). Configuration Worksheet - Port Filter Order

Parameter Information		Your Value
Parameter	Source SAP filter	
Valid Values	1 to 4, where 1 specifies that this filter type should be applied *first* on all transparent bridge ports, and 4 specifies that this filter type should be applied *last*.	
Default Value	1	
Description	This parameter controls when the source SAP filter type is to be applied on all 6611 ports that support transparent bridging.	
Parameter	Ethernet Type filter	
Valid Values	1 to 4, where 1 specifies that this filter type should be applied *first* on all transparent bridge ports, and 4 specifies that this filter type should be applied *last*.	
Default Value	2	
Description	This parameter controls when Ethernet Type filters are to be applied on all 6611 ports that support transparent bridging.	

Table 5-67 (Page 2 of 2). Configuration Worksheet - Port Filter Order

Parameter Information		**Your Value**
Parameter	MAC address filter	
Valid Values	1 to 4, where 1 specifies that this filter type should be applied *first* on all transparent bridge ports, and 4 specifies that this filter type should be applied *last*.	
Default Value	3	
Description	This parameter controls when the MAC address filter type is to be applied on all 6611 ports that support transparent bridging.	
Parameter	Sliding window filter	
Valid Values	1 to 4, where 1 specifies that this filter type should be applied *first* on all transparent bridge ports, and 4 specifies that this filter type should be applied *last*.	
Default Value	4	
Description	This parameter controls when the sliding window filter type is to be applied on all 6611 ports that support transparent bridging.	

Translational Bridging

The 6611 supports local and remote bridging of all network protocols. When the 6611 is configured as a *translational* bridge, frames can be bridged between ports that have source route bridging enabled and those that have transparent bridging enabled. Bridges of this type are sometimes referred to as source route to transparent bridging (SRTB or SR-TB) bridges.

Note: The 6611 translational bridging function is compatible with functions provided by the IBM 8209 and 8229 LAN Bridge products. The 6611 does not provide support for source routing transparent (SRT) bridging.

Translational bridging operates in the following manner:

- When the source and destination ports for a frame use the same bridging scheme, the frame is bridged between the ports without translation.
- When the source and destination ports for a frame use different bridging schemes, the translational bridge performs frame conversion, as needed, to ensure that the frame header is appropriate for the destination LAN. Frames in Token-Ring 802.5 format will be converted to either Ethernet V2.0 or Ethernet 802.3 format as required. Ethernet frames will be converted to Token-Ring 802.5 format as required.

Because many network protocols are implemented differently for token ring and Ethernet, translational bridging offers frame conversion options that extend beyond MAC-layer bridging, such as:

- Converting broadcast addresses into token-ring or Ethernet format
- Encapsulating LLC-based protocols from token-ring frames (such as SNA and NetBIOS) into Ethernet V2.0 frames (using IBM LLC-on-Ethernet format with Ethernet protocol type X'80D5')
- Converting hardware addresses contained in ARP and RARP frames into token-ring or Ethernet format
- Converting Novell NetWare frames containing IPX protocol data into token-ring or Ethernet format
- Converting AppleTalk frames into token-ring or Ethernet format
- Mapping token-ring functional addresses to Ethernet group addresses
- Mapping individual token-ring addresses to individual Ethernet addresses

Port Options for Translational Bridging

Token-ring ports on the bridge can be configured for source route bridging and Ethernet ports can be configured for transparent bridging. Serial ports using PPP can be configured to support a single bridging method: source route bridging, transparent bridging, or *dual mode bridging*.

Dual mode bridging is the recommended method for remotely connecting two 6611s configured as translational bridges. When dual mode bridging is configured on both ends of a serial link, frames originating from a bridge port on the 6611 are translated only if the destination LAN on the remote 6611 requires a different MAC frame format.

Serial ports using frame relay can be configured to support all three bridging methods on the same port. However, you must assign a separate set of DLCIs to each bridging method defined. Serial ports using the LAN Bridging Protocol can be configured for source route bridging only.

Note: A PPP port can be defined as a source route bridge port and a transparent bridge port when the 6611 operates as both a source route bridge and a transparent bridge, instead of as a translational bridge. Dual mode bridging can be defined only when the 6611 operates as a translational bridge.

Port Types Supported

Table 5-68. Port Types Supported for Translational Bridging

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	√
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	√
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	

Restrictions

- The 6611 translational bridge requires at least one enabled bridge port with a MAC address. When you enable bridging on a token-ring or Ethernet port, the 6611 can use the universally or locally defined MAC address on the port. If the 6611 does not have at least one LAN interface enabled for bridging, you must:

  1. Enable bridging on a serial port
  2. Configure the Locally administered MAC address parameter on the serial port's physical interface. (See "Serial Port and V.35/V.36 Serial Port" on page 4-2.)

  The MAC address is combined with the bridge priority to form a unique identifier for the bridge within the network spanning tree.

- When the 6611 is configured as a translational bridge:

  – You cannot enable source route bridging or transparent bridging at the node level. By selecting translational bridging, you have already enabled source route bridging and transparent bridging functions on the 6611.

  – You can configure only one type of bridging on a serial port using PPP. The options are source route bridging, transparent bridging, or dual mode bridging.

  – You must specify a locally administered MAC address on each serial port that has source routing bridging enabled. This address is used as the source address of BPDUs transmitted on the serial port.

- When defining dual mode bridging on a serial port using frame relay, you need to specify at least one data link connection identifier (DLCI) that will be used to transmit bridged frames over the frame relay network. Bridging protocols cannot use frame relay's InARP protocol to acquire DLCI numbers dynamically.

Each DLCI you define also must be associated with an emulated ring number. The emulated ring number uniquely identifies the frame relay connection for source route bridging.

In addition, once you define DLCIs for the bridging protocol, you must explicitly define DLCIs for *all other* protocols running on the same port. First, configure the frame relay protocol by defining a list of DLCIs assigned to the serial port. Then as you define individual protocols on the port, specify which DLCIs are available for use by each protocol.

- The 6611 bridge interprets Ethernet frames using Novell's proprietary format as Ethernet 802.3 frames because the Novell frames contain a Length field. The bridge interprets the X'FFFF' sequence following the Length field as DSAP and SSAP values, respectively. As a result, if a source SAP filter of X'FE' is defined on the transparent bridge port, it is applied to these frames (the filter ignores the low-order command/response bit in the SSAP field).

  To filter Ethernet frames in Novell's proprietary format, define a sliding window filter on the transparent bridge port with a contents field of X'FFFF' and an Offset starting field of **Data**. If you also want to filter IPX traffic on the same port, define a second sliding window filter with an Offset starting field of **Data**, an Offset into frame value of 1 (to filter on the SSAP), a contents field of X'E0' and a mask of X'FE'.

Configuration Changes...

That Require the Translational Bridging Function to Restart

- All node and port-level bridging parameters
- Enable LNM communication through this port

That Require the 6611 to Restart

When bridging is configured on a serial port using frame relay, changes to most of the bridging parameters on the frame relay port will cause the 6611 to restart.

Before You Configure...

This section contains additional information to assist you in configuring the translational bridging protocol.

Specifying Ethernet Addresses

Ethernet addresses are typically represented in canonical form. Canonical form is the address format defined as the standard MAC address representation by the IEEE. In this format, the bit within each octet that is to be transmitted first on a LAN is represented as the least significant bit. For addresses in noncanonical form, the bit within each octet that is transmitted first is represented as the most significant bit.

To illustrate, the following bit string is shown in both noncanonical and canonical forms:

B'00010011 00000000 01011010 00000000 00000000 00000001'

- In noncanonical form: X'13 00 5A 00 00 01'
- In canonical form: X'C8 00 5A 00 00 80'

When Are Frames Bridged?

When bridging has been defined on an Ethernet or token-ring, port, the bridge examines each frame to determine whether the network protocol encapsulated within the frame should be bridged or routed.

- On Ethernet ports, if the network protocol has been configured for routing, the frame is routed. If the network protocol has not been configured for routing, the frame is bridged.
- On token-ring ports, if the network protocol has been configured for routing and the protocol is denied from being bridged by an inbound source route bridge SAP or SNAP filter, the frame is routed. If the network protocol has not been configured for routing or is not denied by an inbound SAP or SNAP filter, the frame is bridged.

When a protocol is not configured for routing, and bridging is disabled, the 6611 discards any packets received for that particular protocol.

When bridging has been defined on a serial port, the adapter examines each frame received to determine how it was encapsulated when it was transmitted. If a frame was encapsulated for a network protocol, such as IP, the frame is routed by that protocol. If the network protocol has not been configured for routing, the frame is discarded. If a frame was encapsulated as a bridged token-ring or Ethernet frame, it is bridged.

For more information on how the 6611 determines whether to bridge or route a specific frame, refer to the bridging protocol descriptions in the *Introduction and Planning Guide*.

Spanning Tree Considerations

The 6611 spanning tree participates in the IEEE 802.1D spanning tree protocol on ports configured for transparent and dual mode bridging. On ports configured for source route bridging, the translational bridge encapsulates IEEE 802.1D bridge protocol data unit (BPDU) frames in token-ring single-route broadcast frames for transport through a source route network to other translational bridges, such as other 6611's configured for translational bridging or IBM 8209 or 8229 LAN Bridges that are configured to provide translation functions.

Unlike a source route bridge, the translational bridge does not forward token-ring all-routes broadcast frames through ports that have been placed in a blocking state by the network spanning tree. This restriction is necessary to prevent duplicate frames from entering the transparent bridge network. In a source route bridge, the port state determined by the spanning tree applies only to single-route broadcast frames received on the port.

Defining Bridge Filters

Filters can be defined on each port that is part of the translational bridge to help you control the type of traffic being bridged over the port. See "Defining Transparent Bridge Port Filters" on page 5-44 for a description of the port filters provided by the transparent bridging function. See "Defining Source Route Bridge Port Filters" on page 5-5 for a description of the port filters provided by the source route bridging function.

When configuring dual mode bridging on a serial port, you have the option of defining both transparent bridge and source route bridge filters on the port.

Transparent bridge filters are applied to frames bridged in Ethernet format. Source route bridge filters are applied to frames bridged in token-ring format.

Defining the Order of Port Filters

The order in which different types of port filters are applied can affect the performance of the translational bridge. As a rule, filter types should be applied in the order in which they are most likely to be effective. The result is that the majority of unwanted traffic is discarded in the shortest amount of time, freeing buffer space to accommodate more traffic.

The node-level parameters for translational bridging enable you to define the order in which filters should be applied on all 6611 ports configured for bridging. The default order, by filter type, is:

1. Hop count filter
2. Source SAP filters
3. Ethernet Type or SNAP value filters
4. Routing information (RI) field filters
5. MAC address filters
6. Sliding window filters

Note: The default filter order reflects the order that is likely to be most effective in a typical bridged network. The optimal order, however, depends upon the configuration of your network and your specific filtering requirements.

If the default filter order is not appropriate for a specific port, you have the option of overriding the default and reordering the filters on that port.

Defining Static Destination Address Filters

The filtering database that the 6611 maintains for transparent bridging can contain up to 4096 static destination address filters. These filters are applied to inbound frames received on ports enabled for transparent bridging.

The IEEE 802.1D standard for MAC bridges defines 16 default static destination address filters, which are automatically included in the filtering database. The 16 default filters include the bridge group address X'01 80 C2 00 00 00' and reserved MAC addresses X'01 80 C2 00 00 01' through X'01 80 C2 00 00 0F' (in canonical form). You can define an additional 4080 filters using the node-level parameters for translational bridging. When a frame is received on a transparent bridge port with a destination MAC address that matches one of these filters, the frame is discarded by the bridge.

Because static destination address filters are processed before individual port filters, these filters offer a performance advantage. However, because static destination address filters apply to all ports configured for transparent bridging, these filters should be used only if a destination address needs to be filtered on all ports for inbound frames.

Configuration Options

Table 5-69 summarizes the configuration options for source route bridging.

Table 5-69. Translational Bridging Configuration Options

WHEN configuring Translational Bridging...	THEN optionally...
...configure each LAN port for the bridge: • See Table 5-39 on page 5-49 for information on configuring ports for transparent bridging. • See Table 5-5 on page 5-10 for information on configuring ports for source route bridging.	• Define bridge port filters. The filters are accessed through a separate push button on the port window.
...configure each serial port for the bridge: • See Table 5-39 on page 5-49 for information on configuring ports for transparent bridging. • See Table 5-5 on page 5-10 for information on configuring ports for source route bridging. • Enable dual mode bridging on a PPP or frame relay serial port that connects two 6611s configured as translational bridges. The link will transport frames in both source route and transparent bridging formats. Dual mode bridging must be defined on each end of the link. **Note:** When dual mode bridging is enabled on a serial port using PPP, transparent bridging and source route bridging cannot be enabled on the same port. – For dual mode bridging over PPP, specify an emulated ring number for the link. – For dual mode bridging over frame relay, pair each DLCI to be used for remote bridging with an emulated ring number that uniquely identifies the frame relay connection.	• Define bridge port filters. The filters are accessed through separate push buttons on the port window.
...configure node level parameters: • Enable translational bridging. • Specify the bridge number of the translational bridge. • If any serial ports on the 6611 use the LAN Bridging Protocol to remotely attach to a PS/2 bridge, specify a designated ring number for the 6611. The designated ring number can be the ring number of any 6611 translational bridge port, except a LAN Bridging Protocol port. If your configuration does not require the LAN Bridging Protocol, disable the Enable LAN Bridging Protocol parameter.	• Select the type of broadcast frame to be used by the bridge for route discovery. • Configure options for performing frame translation and mapping token-ring addresses to Ethernet addresses. • Configure transparent bridging parameters. • Configure spanning tree parameters. • Change the order in which port filters are applied.

Sample Network Graphic Two

Figure 5-9 shows two 6611 translational bridges configured to perform dual mode bridging over a serial link.

The sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running PPP and configured for dual mode bridging and IP
  - A token-ring port configured for source route bridging and IP
  - An Ethernet port configured for transparent bridging and IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running PPP and configured for dual mode bridging and IP
  - A token-ring port configured for source route bridging and IP
  - An Ethernet port configured for transparent bridging and IP

Slot and port numbers in Figure 5-9 are abbreviated s*x* p*y*.

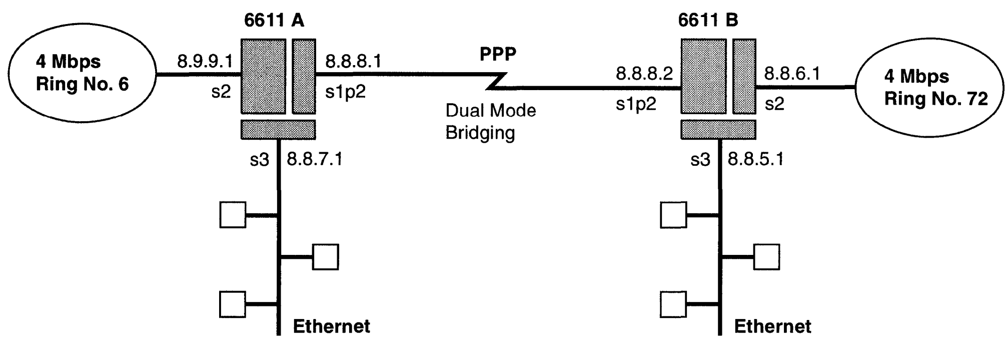


Figure 5-9. Sample Network Using Dual Mode Bridging over PPP

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-9. The following tables list the configuration parameters for the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Note: The configuration of the IP protocol is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to bridge frames.

Serial Ports and Protocols Running on Them

Table 5-70. Serial Port Parameter Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-71. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56 000	56 000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-72. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size (octets)	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-73. Serial Port - Dual Mode Bridging Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Dual Mode Bridging on this port	Enable	Enable
Spanning tree mode	Automatic	Automatic
Port priority	80	80
Path cost	0	0
Port state	NA	NA
Emulated ring number	FAB	FAB
Max. tranmission units (octets)	2052	2052

Table 5-74. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table 5-75. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-76. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable Source Route Bridging on this port	Enable	Enable
Spanning tree mode	Automatic	Automatic
Path cost	0	0
Port priority for Translational Bridging	80	80
Port state	NA	NA
Ring number	6	72
Max. transmission unit (octets)	2052	2052

Table 5-77. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.9.9.1	8.8.6.1
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Disable	Disable
Directed broadcast	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Ports and the Protocols Running on Them

Table 5-78. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	NA	NA

Table 5-79. Ethernet Port - Transparent Bridging Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable Transparent Bridging on this port	Enable	Enable
Maximum transmission unit size	1500	1500
Spanning tree mode	Automatic	Automatic
Port priority	80	80
Path cost	0	0
Port state	NA	NA
Required for Translational Bridging Only		
Emulated ring number	D0	EC

Table 5-80. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.7.1	8.8.5.1
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-81. Node Level - Translational Bridging Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Translational Bridging	Enable	Enable
Bridge number	4	11
Enable LAN Bridging Protocol	Disable	Disable
Designated ring number	NA	NA
Route discovery mode	Single-route broadcast	Single-route broadcast
Address Mapping	Enable	Enable
Enable ARP/RARP conversion	Enable	Enable
Enable AppleTalk coversion	Disable	Disable
Enable IPX coversion	Disable	Disable

Sample Network Graphic One

Figure 5-10 on page 5-86 shows a 6611 translational bridge, 6611 A, configured to perform remote bridging with a transparent bridge, 6611 B. The two bridges communicate over a serial link configured for transparent bridging. End stations on the LAN segments attached to 6611 A, both token-ring and Ethernet, can communicate with Ethernet end stations attached to 6611 B.

The sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running PPP and configured for translational bridging and IP
  - An token-ring port configured for source route bridging and IP
  - An Ethernet port configured for transparent bridging and IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running PPP and configured for remote dual mode bridging and IP
  - Two Ethernet ports configured for transparent bridging and IP

Slot and port numbers in Figure 5-10 on page 5-86 are abbreviated s*x* p*y*.

Notes:

1. The configuration of the IP protocol is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to bridge frames.
2. Dual mode bridging cannot be configured on the serial link in this sample because 6611 B is not a translational bridge. The translation is performed by 6611 A, which is configured for translational bridging.

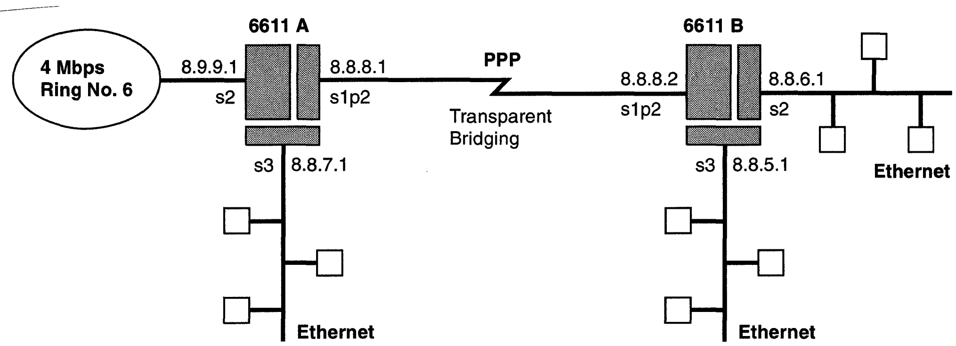


Figure 5-10. Sample Network Showing Remote Bridging between a Translational Bridge and a Nontranslational Bridge

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-10. The following tables list the configuration parameters for the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 5-82. Serial Port Parameter Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-83. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56 000	56 000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-84. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size (octets)	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-85. Serial Port - Transparent Bridging Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Transparent Bridging on this port	Enable	Enable
Maximum transmission unit size	1500	1500
Spanning tree mode	Automatic	Automatic
Port priority	80	80
Path cost	0	0
Port state	NA	NA
Emulated ring number	001	001

Table 5-86. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table 5-87. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	NA
MAC address format	NA
Token ring data rate	4 Mbps
Broadcast type	Non-local

Table 5-88. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 A Slot 2 Value
Enable Source Route Bridging on this port	Enable
Spanning tree mode	Automatic
Path cost	0
Port priority for Translational Bridging	80
Port state	NA
Ring number	6
Max. transmission unit (octets)	1500

Table 5-89. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value
Enable IP routing on this port	Enable
IP address	8.9.9.1
Subnet mask	255.255.255.0
Max. transmission unit (octets)	1492
Enable ICMP address mask requests	Disable
Directed broadcast	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Ethernet Ports and the Protocols Running on Them

Table 5-90. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 2 Value	6611 B Slot 3 Value
Enable physical interface on this port	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA
Enable additional multicast addresses	Disable	Disable	Disable
Multicast MAC address	NA	NA	NA

Table 5-91. Ethernet Port - Transparent Bridging Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 2 Value	6611 B Slot 3 Value
Enable Transparent Bridging on this port	Enable	Enable	Enable
Maximum transmission unit size	1500	1500	1500
Spanning tree mode	Automatic	Automatic	Automatic
Port priority	80	80	80
Path cost	0	0	0
Port state	NA	NA	NA
Emulated ring number	D0	5A	EC

Table 5-92. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 2 Value	6611 B Slot 3 Value
Enable IP routing on this port	Enable	Enable	Enable
IP address	8.8.7.1	8.8.6.1	8.8.5.1
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable	Enable
Directed broadcast	Enable	Enable	Enable
Inbound Port Filters	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable

Node-Level Parameters Configured

Table 5-93. Node Level - Translational Bridging Parameters Configured

Parameter	6611 A
Enable Translational Bridging	Enable
Bridge number	15
Enable LAN Bridging Protocol	Disable
Designated ring number	NA
Route discovery mode	Single-route broadcast
Address Mapping	Enable
Enable ARP/RARP conversion	Enable
Enable AppleTalk conversion	Disable
Enable IPX conversion	Disable

Table 5-94. Node Level - Transparent Bridging Parameters Configured

Parameter	6611 B
Enable Transparent Bridging	Enable
Duplicate address check	Filter
Overflow policy	Learn
Aging time	300
Bridge priority	8000
Hello time	2
Forward delay	15
Max age	20

Port Level Worksheets

Figure 5-11 on page 5-90 shows the path for configuring dual mode bridging through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-11 on page 5-90.

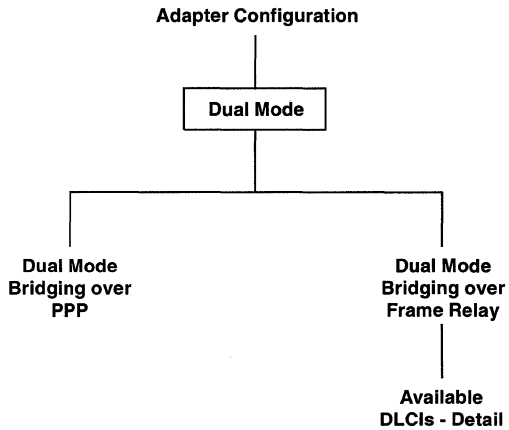


Figure 5-11. Flow of Port Level Dual Mode Bridging Windows

Use the following tables as worksheets to configure translational bridging at the port level:

- Dual Mode Bridging over PPP on page 5-90
- Dual Mode Bridging over Frame Relay on page 5-92

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-21 on page D-17 for a mapping of parameter names and their associated labels.

Table 5-95 (Page 1 of 2). Configuration Worksheet - Dual Mode Bridging over PPP

Parameter Information		Your Value
Parameter	Enable Dual Mode Bridging on this port (see table notes)	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables dual mode bridging on the serial port. Dual mode bridging can only be used when the 6611 is being defined as a translational bridge.	
Parameter	Spanning tree mode	
Valid Values	Automatic, Manual	
Default Value	Automatic	
Description	This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually set by the network administrator. When **Automatic** is selected, the transparent bridge spanning tree determines the port state using information provided by the Port priority and Path cost parameters. When **Manual** is selected, the network administrator can control the forwarding of frames through the bridge by configuring the Port state parameter.	

Table 5-95 (Page 2 of 2). Configuration Worksheet - Dual Mode Bridging over PPP

Parameter Information	Your Value
Parameter Port priority **Valid Values** X'00' to X'FF', where X'00' is the *highest* priority value and X'FF' is the *lowest* priority value **Default Value** X'80' **Description** This parameter specifies the priority of the transparent bridge port. The port priority is used to select the *preferred port* when two or more bridge ports have the same path cost to the root bridge and represent paths through the same designated bridge. The designated bridge is the next-closest bridge to the root bridge. (The transparent bridge spanning tree allows a path through only one of these ports.) **Note:** When ports have equal priorities, the port with the lowest port number is the preferred port. Port numbers are assigned automatically by the 6611.	
Parameter Path cost **Valid Values** 0 to 65535 **Default Value** 0 **Description** This parameter specifies the contribution of the port to the total cost of a path to the root bridge. For a value of zero, the path cost is calculated as 1000/(media speed in Mbps), as recommended by the IEEE. The media speed for PPP or frame-relay ports is from 0.0096 (9600 bps) to 2.048 Mbps, depending on the serial line speed configured for the serial port.	
Parameter Port state **Valid Values** Forwarding, Disabled **Default Value** Disabled **Description** This parameter specifies the state of the port. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames. When this parameter is set to **Forwarding**, it overrides the port state that would have been selected by the transparent bridge spanning tree. Because the spanning tree algorithm cannot automatically disable a port, the network administrator must ensure the port does not cause a loop in the network when it is in the forwarding state.	
Parameter Emulated ring number (required) **Valid Values** X'001' to X'FFF' **Default Value** None **Description** This parameter specifies a value that is interpreted as the ring number for link attached to this port. This value is placed in the routing information (RI) field of route discovery frames transmitted from source route or dual mode bridge ports. The ring number value is not used for transparent bridging.	
Parameter Maximum transmission unit **Valid Values** 516, 1500, or 2052 octets **Default Value** 2052 octets **Description** This parameter specifies the size of the largest transmission unit that can be transmitted or received on the port. In an Ethernet V2.0 frame, the transmission unit is the Data field in the frame. In an IEEE 802.3 or 802.5 frame, the transmission unit is the logical link control (LLC) PDU in the frame.	

Note:

- Dual mode bridging allows frames in both source route bridging and transparent bridging formats to be forwarded on the same port.
- When dual mode bridging is enabled on a serial port configured for PPP, source route bridging and transparent bridging cannot be enabled on the same port.

Table 5-96 (Page 1 of 2). Configuration Worksheet - Dual Mode Bridging over Frame Relay

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable Dual Mode Bridging on this port (see table notes) Enable, Disable Disable This parameter enables or disables dual mode bridging on the serial port. Dual mode bridging can only be used when the 6611 is being defined as a translational bridge.	
Parameter **Valid Values** **Default Value** **Description**	Spanning tree mode Automatic, Manual Automatic This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually set by the network administrator. When **Automatic** is selected, the transparent bridge spanning tree determines the port state using information provided by the Port priority and Path cost parameters. When **Manual** is selected, the network administrator can control the forwarding of frames through the bridge by configuring the Port state parameter.	
Parameter **Valid Values** **Default Value** **Description**	Port priority X'00' to X'FF', where X'00' is the *highest* priority value and X'FF' is the *lowest* priority value X'80' This parameter specifies the priority of the transparent bridge port. The port priority is used to select the *preferred port* when two or more bridge ports have the same path cost to the root bridge and represent paths through the same designated bridge. The designated bridge is the next-closest bridge to the root bridge. (The transparent bridge spanning tree allows a path through only one of these ports.) **Note:** When ports have equal priorities, the port with the lowest port number is selected as the preferred port. Port numbers are assigned automatically by the 6611.	
Parameter **Valid Values** **Default Value** **Description**	Path cost 0 to 65535 0 This parameter specifies the contribution of the port to the total cost of a path to the root bridge. For a value of zero, the path cost is calculated as 1000/(media speed in Mbps), as recommended by the IEEE. The media speed for PPP or frame-relay ports is from 0.0096 (9600 bps) to 2.048 Mbps, depending on the serial line speed configured for the serial port.	
Parameter **Valid Values** **Default Value** **Description**	Port state Forwarding, Disabled Disabled This parameter specifies the state of the port. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames. When this parameter is set to **Forwarding**, it overrides the port state that would have been selected by the transparent bridge spanning tree. Because the spanning tree algorithm cannot automatically disable a port, the network administrator must ensure the port does not cause a loop in the network when it is in the forwarding state.	

Table 5-96 (Page 2 of 2). Configuration Worksheet - Dual Mode Bridging over Frame Relay

Parameter Information		Your Value
Parameter	Maximum transmission unit	
Valid Values	516, 1500, or 2052 octets	
Default Value	2052 octets	
Description	This parameter specifies the size of the largest transmission unit that can be transmitted or received on the port. In an Ethernet V2.0 frame, the transmission unit is the Data field in the frame. In an IEEE 802.3 or 802.5 frame, the transmission unit is the logical link control (LLC) PDU in the frame.	
DLCI-Ring Number Pairs List - Parameters configured for each pair defined		
Parameter	DLCI number (see table notes)	
Valid Values	Any available DLCI in the port list	
Default Value	None	
Description	This parameter identifies a DLCI that will be used to transmit bridged frames over a frame relay network. You can select any of the DLCIs defined for the frame relay port. (See Table 4-21 on page 4-16 for information on defining DLCIs for the port.) Each DLCI must be mapped to an emulated ring number. The ring number uniquely identifies a frame relay connection between this translational bridge and a remote translational bridge.	
Parameter	Emulated ring number (see table notes)	
Valid Values	X'001' to X'FFF'	
Default Value	None	
Description	This parameter specifies an emulated ring number that uniquely identifies a frame relay connection between two 6611 translational bridges. A ring number must be assigned to each DLCI used by the translational bridge to bridge frames on this port. The emulated ring number is placed in the routing information (RI) field of route discovery frames transmitted from source route or dual mode bridge ports. The ring number value is not used for transparent bridging.	

Note:

- Dual mode bridging allows frames in both source route bridging and transparent bridging formats to be forwarded on the same port.
- When dual mode bridging is enabled on a serial port configured for frame relay, source route bridging and transparent bridging also *can* be enabled on the port. However, you must assign a separate set of DLCIs to each bridging method defined.
- At least one DLCI-emulated ring number pair must be defined when dual mode bridging is enabled on the port. A maximum of 240 DLCI-ring number pairs can be defined.

Node Level Worksheets

Figure 5-12 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-12.

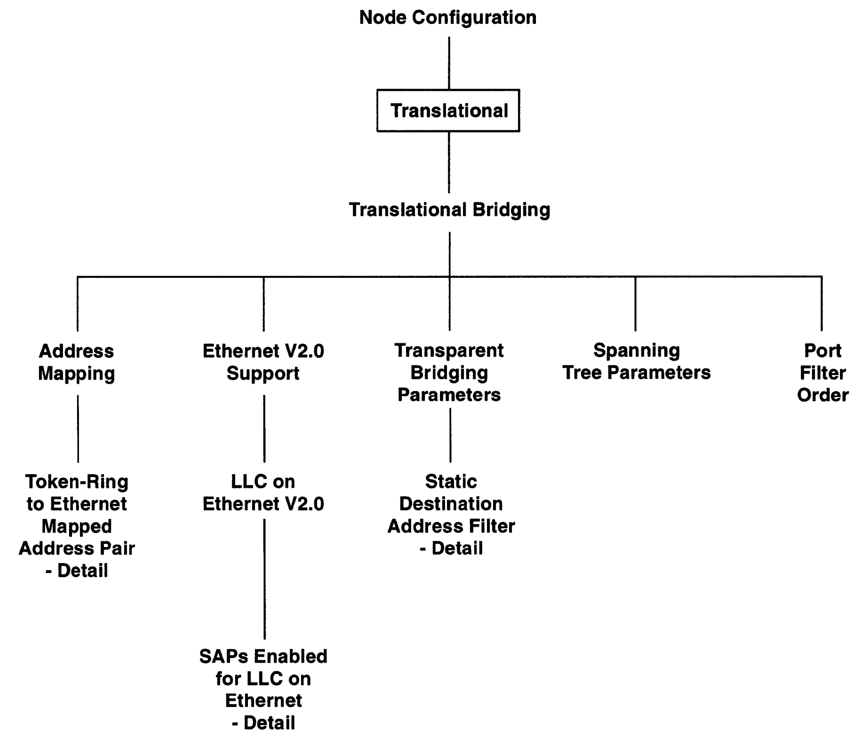


Figure 5-12. Flow of Node Level Translational Bridging Windows

Use the following tables as worksheets for configuring translational bridging at the node level:

- Translational Bridging on page 5-95
- Address Mapping on page 5-96
- Ethernet V2.0 Support on page 5-97
- LLC on Ethernet V2.0 on page 5-98
- Transparent Bridging Parameters on page 5-99
- Spanning Tree Parameters on page 5-100
- Port Filter Order on page 5-101

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-21 on page D-17 for a mapping of parameter names and their associated labels.

Table 5-97 (Page 1 of 2). Configuration Worksheet - Translational Bridging

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable Translational Bridging Enable, Disable Disable This parameter enables or disables translational bridging on the 6611. When translational bridging is enabled at the node level, frames will be bridged between ports that have source route bridging enabled and those that have transparent bridging enabled. When this parameter is enabled, source route bridging and transparent bridging cannot be configured individually at the node level.	
Parameter **Valid Values** **Default Value** **Description**	Bridge number (required) 0 to 15. Bridge numbers must be unique among bridges that connect a particular pair of LAN segments. None This parameter specifies a bridge number for the translational bridge. The bridge number uniquely identifies the bridge when it and one or more other bridges are used to connect two LAN segments.	
Parameter **Valid Values** **Default Value** **Description**	Enable LAN Bridging Protocol Enable, Disable Enable When this parameter is enabled, remote source route bridging over a serial link to an IBM token-ring bridge program is permitted. The bridge program operates on a PS/2 workstation.	
Parameter **Valid Values** **Default Value** **Description**	Designated ring number (required when LAN Bridging Protocol is enabled) X'001' to X'FFF' None This parameter specifies the ring number of the 6611 bridge port that serves as the target ring for all remotely attached PS/2 workstations running an IBM token-ring bridge program. The designated ring number can be the ring number of any 6611 translational bridge port, except a LAN Bridging Protocol port. The designated ring number appears as a route designator in the RI field of all frames forwarded to and received from the remotely attached PS/2 bridges.	
Parameter **Valid Values** **Default Value** **Description**	Route discovery mode Single-route broadcast, All-routes broadcast Single-route broadcast This parameter specifies whether the translational bridge should forward a frame for a token-ring station as a single-route broadcast frame or an all-routes broadcast frame when the destination address of the station is not in the token-ring database maintained by the bridge. A single-route broadcast frame is forwarded along the source route spanning tree path. If the destination station is reached, it replies with an all-routes broadcast frame. An all-routes broadcast frame is forwarded along all possible paths to the destination station. If the destination station is reached, it replies to each all-routes broadcast received with a specifically routed frame that retraces the path of the all-routes broadcast.	

Table 5-97 (Page 2 of 2). Configuration Worksheet - Translational Bridging

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable ARP/RARP conversion Enable, Disable Enable When enabled, this parameter instructs the translational bridge to convert TCP/IP ARP and RARP frame data into the format expected by a token-ring or Ethernet LAN. Frame conversion is performed only when this parameter is enabled and when frames are being bridged between token-ring and Ethernet LANs.	
Parameter **Valid Values** **Default Value** **Description**	Enable AppleTalk conversion Enable, Disable Disable When enabled, this parameter instructs the translational bridge to convert a frame containing AppleTalk protocol data into the format expected by a token-ring or Ethernet LAN. Frame conversion is performed only when this parameter is enabled and when frames are being bridged between token-ring and Ethernet LANs.	
Parameter **Valid Values** **Default Value** **Description**	Enable IPX conversion Enable, Disable Disable When enabled, this parameter instructs the translational bridge to convert a Novell NetWare frame containing IPX protocol data into the format expected by a token-ring or Ethernet LAN. Frame conversion is performed only when this parameter is enabled and when frames are being bridged between token-ring and Ethernet LANs.	

Table 5-98 (Page 1 of 2). Configuration Worksheet - Address Mapping

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Map token-ring to Ethernet addresses Enable, Disable Enable When this parameter is enabled, the translational bridge will map a specified token-ring address to a specified Ethernet address when bridging frames between token-ring and Ethernet LANs. Each address pair you define must be unique within the bridged network.	
Parameter **Valid Values** **Default Value** **Description**	Convert token-ring to Ethernet broadcast address Enable, Disable Enable When this parameter is enabled, the translational bridge converts the token-ring all-stations broadcast address of X'C000 FFFF FFFF' in a frame to the Ethernet all-stations broadcast address of X'FFFF FFFF FFFF'. This parameter takes effect only when the Map token-ring to Ethernet addresses parameter is enabled. **Note:** This parameter converts only the token-ring broadcast address in frames. To convert the Ethernet all-stations broadcast address to the token-ring all-stations broadcast address, you must specify the Ethernet address and the token-ring address as a mapped address pair and *disable* this parameter. When the broadcast addresses are defined as a mapped address pair, the bridge converts the addresses in either direction.	

Table 5-98 (Page 2 of 2). Configuration Worksheet - Address Mapping

Parameter Information		Your Value
Token Ring to Ethernet Mapped Address Pair List - Parameters configured for each pair defined		
Parameter	Token ring (required address for each address pair defined)	
Valid Values	Any valid MAC address in noncanonical form	
Default Value	None	
Description	This parameter specifies the token-ring address in a pair of mapped addresses. When the translational bridge is bridging frames between token-ring and Ethernet LANs and this token-ring address appears in a frame, the bridge converts this address to the Ethernet address associated with it.	
Parameter	Ethernet (required address for each address pair defined)	
Valid Values	Any MAC address in canonical form	
Default Value	None	
Description	This parameter specifies the Ethernet address in a pair of mapped addresses. When the translational bridge is bridging frames between token-ring and Ethernet LANs and this Ethernet address appears in a frame, the bridge converts this address to the token-ring address associated with it.	
Parameter		
Valid Values	A string of up to 40 alphanumeric characters, including special characters	
Default Value	None	
Description	This parameter is a text field that can be used to describe the mapped address pair being defined.	

Table 5-99 (Page 1 of 2). Configuration Worksheet - Ethernet V2.0 Support

Parameter Information		Your Value
Parameter	Mode of translation between token ring and Ethernet	
Valid Values	One of the following options: • Translate token-ring frames to Ethernet V2.0 • Translate token-ring frames to Ethernet 802.3 • Select translation mode automatically	
Default Value	Select translation mode automatically	
Description	This parameter specifies the translation mode to be used by the 6611 when translating bridged frames from token-ring to Ethernet format. When this parameter is set to **Translate token-ring frames to Ethernet V2.0**, the 6611 expects all frames transmitted over attached Ethernet LANs to be in Ethernet Version 2.0 format. (This mode is equivalent to the *mode 1* setting on an IBM 8209 or 8229 Bridge.) When this parameter is set to **Translate token-ring frames to Ethernet 802.3**, the 6611 expects all frames transmitted over attached Ethernet LANs to be in Ethernet 802.3 format. (This mode is equivalent to the *mode 2* setting on an IBM 8209 or 8229 Bridge.) The default, **Select translation mode automatically**, allows the 6611 to determine the correct Ethernet format to use based on the format of frames previously transmitted from the destination Ethernet station.	

Table 5-99 (Page 2 of 2). Configuration Worksheet - Ethernet V2.0 Support

Parameter Information		Your Value
Parameter	Mode priority (see table note)	
Valid Values	Ethernet V2.0, Ethernet 802.3	
Default Value	Ethernet V2.0	
Description	When the 6611 is bridging frames from a token-ring LAN to an Ethernet LAN, this parameter specifies the Ethernet frame format to use for translation when the correct format cannot be determined automatically. When the Mode of translation between token ring and Ethernet parameter is set to **Select translation mode automatically**, the 6611 attempts to determine the correct Ethernet format to use based on the format of frames previously transmitted from the destination Ethernet station. The 6611 maintains this information in the filtering database for transparent bridge ports. If an entry for the destination Ethernet station is not in the filtering database, the 6611 uses the default frame format specified by this parameter.	
Parameter	Transmit multicast as both Ethernet V2.0 and Ethernet 802.3 (see table note)	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter specifies whether the 6611 is to transmit two multicast frames (one in Ethernet Version 2.0 format and one in Ethernet 802.3 format) for each frame with a group, functional, or broadcast address that is forwarded from a token-ring network.	

Note: The Mode priority parameter and the Transmit multicast as both Ethernet V2.0 and Ethernet 802.3 parameter can be configured only when the Mode of translation between token ring and Ethernet parameter is set to **Select translation mode automatically**.

Table 5-100 (Page 1 of 2). Configuration Worksheet - LLC on Ethernet V2.0

Parameter Information		Your Value
Parameter	Enable encapsulation of LLC-based protocols in Ethernet V2.0 (see table notes)	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	When the 6611 is bridging frames between a token-ring LAN and an Ethernet LAN that uses Ethernet V2.0, this parameter specifies whether the 6611 should encapsulate LLC protocol (IEEE 802.2) data units into the Ethernet V2.0 frames being forwarded. When this parameter is enabled, service access point (SAP) values in the associated list are encapsulated and forwarded in Ethernet V2.0 frames. **Note:** The Type field in an Ethernet V2.0 frame is set to X'80D5' when the frame contains an LLC-based protocol.	
SAPs Enabled for LLC on Ethernet List - Parameters configured for each SAP defined		
Parameter	SAP enabled for LLC-on-Ethernet V2.0 encapsulation (required for each SAP defined)	
Valid Values	X'00' to X'FF'	
Default Value	None	
Description	This parameter specifies the name of a SAP value, within an LLC protocol data unit, that the 6611 should encapsulate into an Ethernet V2.0 frame and forward.	

Table 5-100 (Page 2 of 2). Configuration Worksheet - LLC on Ethernet V2.0

Parameter Information		Your Value
Parameter **Valid Values** **Description**	Description of this SAP A string of up to 40 alphanumeric characters, including special characters None This parameter is a text field that can be used to describe the SAP value selected for encapsulation in an Ethernet V2.0 frame.	

Note:

- The parameters in this table can be configured if the Mode of translation between token ring and Ethernet parameter (in Table 5-99 on page 5-97) is set to either **Translate token-ring frames to Ethernet V2.0** or **Select translation mode automatically**.
- The following SAP values are included, by default, for encapsulation within Ethernet V2.0 frames:
  - X'00' - Null
  - X'04' - SNA path control
  - X'08' - SNA
  - X'F0' - NetBIOS
  - X'F4' - LAN Network Manager
  - X'FC' - Discovery

  See Appendix B on page B-1 for a description of these and other common SAP values.

Table 5-101 (Page 1 of 2). Configuration Worksheet - Transparent Bridging Parameters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Duplicate address check Forward, Filter Forward This parameter specifies whether the translational bridge supports the IEEE 802.2 Duplicate Address Check protocol for Ethernet frames. Select **Forward** to instruct the bridge to forward all frames that have identical source and destination MAC addresses. This option allows the detection of duplicate MAC addresses in the network. Select **Filter** to instruct the bridge to discard frames that have identical source and destination MAC addresses. This option reduces the amount of traffic in the network.	
Parameter **Valid Values** **Default Value** **Description**	Overflow policy Learn, Do not learn Learn This parameter specifies how the translational bridge should handle a new entry for the filtering database if the database is full. Select **Learn** (the default) to instruct the bridge to discard an old entry in the database and replace it with the new entry. Select **Do not learn** to instruct the bridge to discard the new entry, leaving the database unchanged. The Ethernet database on all adapters that support Ethernet can contain up to 4096 entries. The token-ring database on A25 and A47 adapters that support token ring can contain up to 3072 entries. On other adapters that support token ring, the token-ring database can contain up to 1024 entries.	
Parameter **Valid Values** **Default Value** **Description**	Aging time 10 to 1 000 000 seconds 300 seconds This parameter specifies the number of seconds that a dynamic entry can remain in the filtering database without the translational bridge observing any activity from that address. When the age of an entry equals the aging time, the bridge deletes the entry from the filtering database.	

Table 5-101 (Page 2 of 2). Configuration Worksheet - Transparent Bridging Parameters

Parameter Information		Your Value
Static Destination MAC Address Filters List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default Value** **Description**	Static destination MAC address (required for each filter defined) X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter specifies a destination MAC address that is placed in the filtering database to serve as an address filter. The filter is applied to frames received on ports enabled for transparent bridging. When a frame is received with a destination MAC address that matches the specified MAC address, the frame is discarded by the bridge. The address is *static* because it remains in the filtering database until you remove or change it. Each static address you define reduces the amount of space available in the filtering database for dynamic entries. This parameter affects only bridged frames on ports enabled for transparent bridging. Routed frames are not affected by this parameter.	
Parameter **Valid Values** **Default Value** **Description**	Form of MAC address Canonical, Noncanonical Canonical This parameter specifies how the 6611 should interpret the static destination MAC address defined for the filter. Addresses can be in canonical form and noncanonical form.	

Note: A maximum of 4080 static destination address filters can be defined.

Table 5-102 (Page 1 of 2). Configuration Worksheet - Spanning Tree Parameters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Bridge priority X'0000' to X'FFFF', where X'0000' is the *highest* priority value and X'FFFF' is the *lowest* priority value. X'8000' This parameter specifies the priority of the translational bridge. When this bridge is activated, its priority value is compared to the priority values of other active bridges in the network. The bridge with the highest priority becomes the root bridge of the spanning tree. When the highest priority value in the network is shared by two or more bridges, the bridges compare port MAC addresses (one port on each bridge is selected for this purpose). The bridge with the lowest value MAC address becomes the root bridge.	
Parameter **Valid Values** **Default Value** **Description**	Hello time 1 to 10 seconds 2 seconds When this translational bridge is selected as the root bridge for the network, this parameter specifies how often the bridge transmits configuration bridge protocol data units (BPDUs). The BPDUs contain information about the topology of the spanning tree and reflect changes to the topology.	

Table 5-102 (Page 2 of 2). Configuration Worksheet - Spanning Tree Parameters

Parameter Information		Your Value
Parameter	Forward delay	
Valid Values	4 to 30 seconds	
Default Value	15 seconds	
Description	When this translational bridge is selected as the root bridge for the network, the value of this parameter specifies how long ports on all bridges remain in either a *listening state* or *learning state*. When the forward delay time expires, ports in the listening state go into the learning state and ports in the learning state go into the forwarding state. State changes occur as a result of changes in the topology of the spanning tree, such as when an active bridge fails or is shut down. To keep the information in the filtering database current, the value of this parameter also is used as the value of the Aging time parameter for a short period after a topology change occurs.	
Parameter	Max age	
Valid Values	6 to 40 seconds	
Default Value	20 seconds	
Description	When this translational bridge is selected as the root bridge for the network, the value of this parameter specifies how long other active bridges are to store the topology information received configuration bridge protocol data units (BPDUs). When this information reaches its maximum age limit without being replaced, the active bridges in the network discard it and assume the root bridge or the path to the root bridge has failed. A new root bridge or path is then selected.	

Table 5-103 (Page 1 of 2). Configuration Worksheet - Port Filter Order

Parameter Information		Your Value
Parameter	Hop count filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	1	
Description	This parameter controls when the hop count filter type is to be applied on all 6611 ports that support source route bridging. The hop count filter is applied to inbound frames only.	
Parameter	Source SAP filters	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	2	
Description	This parameter controls when the source service access point (SAP) filter type is to be applied on all 6611 ports that support bridging.	
Parameter	Ethernet/SNAP type filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	3	
Description	This parameter controls when Ethernet Type or SNAP value filters are to be applied on 6611 ports that support bridging. The Ethernet Type filter can be defined on transparent bridge ports and is applied to the contents of the Type field within an Ethernet frame. The SNAP value filter can be defined on source route bridge ports.	

Table 5-103 (Page 2 of 2). Configuration Worksheet - Port Filter Order

Parameter Information		Your Value
Parameter	RI field filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	4	
Description	This parameter controls when the routing information (RI) field filter type is to be applied on all 6611 ports that support source route bridging.	
Parameter	MAC address filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	5	
Description	This parameter controls when the MAC address filter type is to be applied on all 6611 ports that support bridging.	
Parameter	Sliding window filter	
Valid Values	1 to 6, where 1 specifies that this filter type should be applied *first* on all source route bridging ports, and 6 specifies that this filter type should be applied *last*	
Default Value	6	
Description	This parameter controls when the sliding window filter type is to be applied on all 6611 ports that support bridging.	

IP Protocol

Internet Protocol (IP) is a standard protocol that defines the delivery mechanism used on the Internet. The 6611 implements the following IP routing protocols: Open Shortest Path First (OSPF), Routing Information Protocol (RIP) Versions 1 and 2, Hello, Border Gateway Protocol (BGP), and Exterior Gateway Protocol (EGP), all of which will be described in the following sections. In addition, static routes also may be configured manually.

Port Types Supported

Table 5-104. Port Types Supported for IP Routing

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	√

Restrictions

- You can define a total of 50 port and node-level IP packet filters. Each filter must have a unique filter ID.
- When IP is configured on a frame relay port with either AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by IP on the port.
- You can configure up to 8 TCP not well-known ports and 8 UDP not well-known ports in the list of prioritized ports.
- If you enable transmission group for IP, the Configuration Program automatically merges the list of prioritized ports from both serial ports. This merged list may contain up to 8 TCP not well-known ports and 8 UDP not well-known ports.

Configuration Changes ...

That Require the IP Function to Restart

- X.25 remote host parameters
  - Destination IP address for X.25
  - Virtual circuit type
  - Logical channel number
  - Remote DTE address

- SVC option parameters (for X.25 Adapters)
  - Receive packet size
  - Transmit packet size
  - Receive packet window size
  - Transmit packet window size
  - Closed user group index
  - Closed user group with outgoing access index
  - User-defined facilities
  - RPOA indices

That Require the 6611 to Restart

- IP destination per DLCI parameters (for frame relay)
  - DLCI number
  - Destination IP address

Before You Configure...

This section contains additional information to assist you in configuring the IP protocol.

Tailoring Your IP Traffic Flow

The IBM 6611 provides various means by which you will be able to tailor the flow of IP traffic between routers. There are options available for tailoring by address, port and protocol which will minimize unnecessary traffic flow and allow you to prioritize the important traffic.

IP Packet Filters: Packet filters are available at the node level to provide for tailoring of inbound IP traffic. You will be able to permit/deny IP traffic coming into the IBM 6611 by IP addresses or IP addresses and TCP/UDP ports. See "IP Packet Filters" on page 5-213 for information on how to define and configure packet filters.

Inbound Port Filters: Inbound port filters work in the same way as the IP packet filters except that they are available at the port level. You will be able to permit/deny IP traffic coming into the IBM 6611 on a specific port. The filter can be set up to filter on IP addresses or IP addresses and TCP/UDP ports.

Well-known Port Filters: Each process that wants to communicate with another process identifies itself by one or more ports. A port is a 16-bit number used by the host-to-host protocol to identify to which higher-level protocol or application program (process) it must deliver incoming messages.

Higher-level programs (such as telnet and FTP) are themselves protocols as they use the same port number in all TCP/IP implementations. Those "assigned" port numbers are called *well-known ports*. These ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA). The assigned well-known ports occupy port numbers in the range 1 to 1023. The ports with numbers in the range 1024 to 65535 are not controlled by the IANA and on most systems can be used by ordinary user-developed programs.

Well-known port filters enable you to restrict access to services provided by well-known TCP or UDP ports on the 6611. For example, if you want to prohibit certain networks from using FTP, you would use the IBM 6611 filtering function to filter on TCP ports 20,21 (FTP).

This function is available with packet filters and inbound port filters discussed above.

IP Export Filters: Export filters provide the ability to share routes which are learned by one protocol with another protocol. You will be able create filters which pass or restrict all routes or specific routes. When exporting to or from RIP or Hello, you can further qualify the filtering by specifying an interface or a specific gateway from which this route can be learned or to which it can be passed. See "IP Export Filters" on page 5-201 for information on configuring export filters.

Import Filters: When export filters are defined on multiple 6611s in your network, it may become advantageous to restrict the sources from which routes are accepted. Import filters regulate which routes the protocol learns and accepts. Import filters take effect when learning routes from other routers, and when exporting from one protocol to another.

Import filters are defined at the protocol level for the following protocols:

- BGP
- EGP
- Hello
- RIP

Import filters deny route imports on the basis of destination IP address, thus enabling you to control the source of the routes imported for each of these IP protocols. For the RIP and Hello protocols, you can also further qualify import applicability by specifying interfaces or specific gateways. For the EGP and BGP protocols, import filter applicability must be qualified with respect to the autonomous system of the EGP neighbor or EGP peer supplying the routes.

You might want to use import filters to prevent the import of routes from certain interfaces or certain routers in order to:

- Prevent the sharing of routes for security reasons
- Limit network traffic across certain links
- Control the size of the route table

Route Preference: Because there is the possibility that more than one of the protocols may provide routes to the same destination, you can indicate ahead of time which protocol (including static) is preferable. It is called the *route preference* and can be any value from 0 to 255. A preference of 0 is the most preferred. The preference of each protocol can be configured. The default values are listed in the following worksheets for the various protocols. It is not possible to have more than one route to a destination from the same protocol. Therefore, it is not possible to prefer one static route over another, for instance.

IP Priority: When configuring IP on a serial port running frame relay or PPP, you have the ability to assign priority to your traffic. You can tailor either a well-known port or a specific TCP or UDP not well-known port to have a low, medium, or high priority. This will enable important applications to have preference on your network.

Refer to the remote DLSw section of Table 5-453 on page 5-343 for information about the ports and IP priority that DLSw uses.

UDP Broadcast Forwarding: UDP broadcast forwarding is provided for client/server applications operating over multiple IP networks. These applications broadcast rather than unicast datagrams in two situations:

- A server wishes to communicate with many clients. These clients may be unknown to the server or, known to the server and broadcasting is more efficient. An example of this application is time server (RFC 868).
- A client wishes to obtain a particular type of service and the available server or servers are unknown. An example of this application is BOOTP (RFC 951).

The normal behavior for IP broadcasts is to remain on the local network. For example, an IP datagram addressed to 128.141.255.255 would not be forwarded outside the class B 128.141 network. When a 6611 port has UDP broadcast forwarding enabled, that port will monitor received IP broadcast datagrams. When an IP broadcast datagram is received with a destination UDP port corresponding to one of those configured, a separate IP broadcast is generated for each port configured in the Target Port IP Address list.

UDP Directed Broadcast: UDP directed broadcast is provided for all-host broadcast UDP messages that IP receives. When the 6611 receives a broadcast that is directed to an attached interface, IP forwards the message directly to that interface and broadcasts it. For more information, see the *Introduction and Planning Guide*.

By default, UDP directed broadcast is enabled. Directed broadcast can only be used for broadcast media such as LANs and fully-meshed frame-relay networks. In partially meshed frame-relay networks, directed broadcast is not available on point-to-point links.

Transmission Groups

The 6611 allows you to configure transmission groups for IP over serial links using PPP. A transmission group (TG) is two physical links that act as a single logical link. The TG function allows the 6611 to perform load balancing with T1 or E1 lines by redirecting IP traffic from the primary link to the alternate link when the queue depth of the primary link reaches a certain number.

A TG must be configured over two serial ports. Refer to Table 4-42 on page 4-27 for the serial port combinations that can support a TG. After you initially configure TG and IP on one serial port, the Configuration Program automatically enables both TG and IP on the other serial port. The Configuration Program also:

- Takes the lower MTU value from the serial ports and sets both Max. transmission unit parameters to that value
- Sets the Enable inbound port filters and Enable IP priority parameters on the second serial port to match the values in the first serial port
- Merges the individual lists of inbound port filters from both serial ports
- Merges the individual lists of prioritized ports from both serial ports

While TG is enabled for IP on both serial ports, the Configuration Program automatically keeps the values for the MTU, port filters, and IP priority parameters on both serial ports in synch. If you disable TG for IP on one serial port, the Configuration Program stops updating IP parameters on either serial port.

Configuration Options

When IP is configured on a frame relay port with either AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by IP on the port.

Table 5-105 summarizes the configuration options for each adapter type that supports IP. After configuring IP on specific ports, you need to enable IP routing at the node level.

For a sample network that illustrates the configuration of IP in a partially meshed frame-relay network, see Appendix A on page A-1.

Table 5-105 (Page 1 of 2). IP Configuration Options

WHEN configuring IP...	THEN optionally...
...on a token-ring port or an Ethernet port: • Enable IP on the port. • Enter the IP address. • Determine the subnet mask.	• Determine Ethernet framing for IP for Ethernet port. • Determine the maximum transmission unit. • Disable ICMP address mask requests. • Define inbound port filters for this port. • Enable UDP broadcast forwarding.
...on a serial port using PPP...	
...for basic configuration: • Enable IP on the port. • Enter the IP address. • Determine the subnet mask. • Enter the destination IP address.	• Determine the maximum transmission unit. • Disable ICMP address mask requests. • Determine whether to enable a transmission group for IP on this port. • Define inbound port filters for this port. • Set IP priority for this port. • Enable UDP broadcast forwarding.
...to enable transmission groups: • Enable transmission group on the Physical Interface. • Set the transmission group name. • Enable IP on the port. • Enter the IP address. • Determine the subnet mask. • Enter the destination IP address. • Enable transmission group for IP on this port.	• Determine the maximum transmission unit. • Disable ICMP address mask requests. • Enable filtering on this port. • Define inbound port filters. • Set IP priority for this port. • Define a list of prioritized ports. • Enable UDP broadcast forwarding.

Table 5-105 (Page 2 of 2). IP Configuration Options

WHEN configuring IP...	THEN optionally...
...on a serial port using frame relay...	
...for defining point-to-point links only: • Enable IP on the port. • Enter the IP address. • Determine the subnet mask. • Enable point-to-point only. • On the IP Point-to-Point Addresses per DLCI - Detail window, specify each IP point-to-point destination. If the LMI option on the Frame Relay window is set to **None**, you must also specify a DLCI number for each destination.	• Determine the maximum transmission unit. • Disable ICMP address mask requests. • Define IP destinations for each DLCI to provide a logical mapping between the DLCI number and the destination IP address. • Set IP priority for this port. • Define inbound port filters for this port. • Enable UDP broadcast forwarding. • Define IP destinations for each DLCI to provide a logical mapping between the DLCI number and the destination IP address.
...for defining mesh links only: • Enable IP on the port. • Enter the IP address. • Determine the subnet mask. • Enable directed broadcast. • Disable point-to-point only. • Set the assignment for discovered DLCIs to **Mesh**.	• Determine the maximum transmission unit. • Disable ICMP address mask requests. • Set IP priority for this port. • Define inbound port filters for this port. • Enable UDP broadcast forwarding. • On the Frame Relay window, enter the DLCIs to be used in the mesh. • Define IP destinations for each DLCI to provide a logical mapping between the DLCI number and the destination IP address.
...for defining point-to-point and mesh links: • On the Frame Relay window, enter the DLCIs to be used in the mesh. • Enable IP on the port. • Enter the IP address. • Determine the subnet mask. • Set the assignment for discovered DLCIs to **Point-to-point**. • On the IP Point-to-Point Addresses window, specify each the IP address of each IP point-to-point destination. Do *not* specify the DLCI number; discovered DLCIs will be assigned to the point-to-point link. • On the IP destinations per DLCI window, enter the DLCI number and the IP address to define each mesh link.	• Determine the maximum transmission unit. • Disable ICMP address mask requests. • Set IP priority for this port. • Define inbound port filters for this port. • Enable UDP broadcast forwarding.
...on an X.25 adapter: • Enable IP on the port. • Enter the IP address. • Determine the subnet mask. • Add each X.25 remote host	• Determine the maximum transmission unit. • Disable ICMP address mask requests.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform IP routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-106. IP Configuration Verification Checklist

Internet Protocol Rule	**Configuration Parameter**	√
Port-Level Parameters:		
Ensure that the Enable IP routing on this port parameter is enabled.	Enable IP routing on this port	
Ensure that there are no duplicate IP addresses in the network.	IP address	
Ensure that there are no overlapping subnet addresses in the network.	Subnet address	
When the Enable port for Transmission Group parameter is enabled for a port, the Data link protocol parameter must be set to **PPP** and the Enable transmission group for IP on this port parameter must be enabled.	Enable port for Transmission Group	
	Enable PPP data link protocol	
	Enable transmission group for IP on this port	

Sample Network Graphic

Figure 5-13 on page 5-110 shows two 6611s (6611 A and 6611 B) configured to use port-level IP packet filters. Additional samples networks that illustrate the configuration for IP in a partially meshed frame-relay network are in Appendix A on page A-1.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and RIP over PPP
  - An Ethernet port running RIP and IP
  - A token-ring port running RIP and IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and RIP over PPP
  - An Ethernet port running RIP and IP
  - A token-ring port running RIP and IP

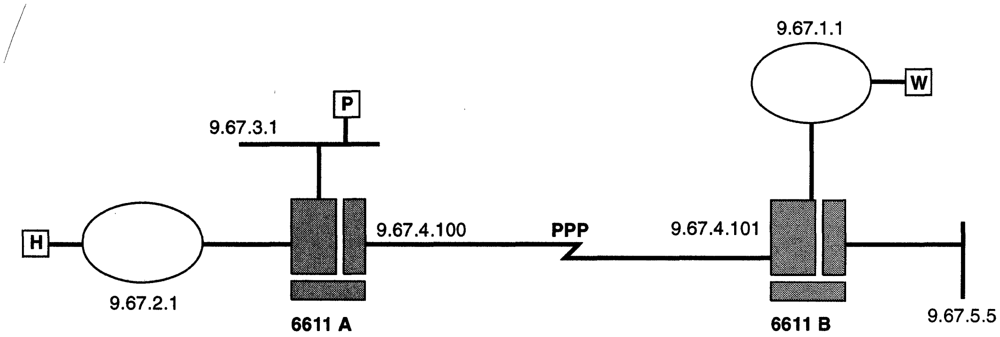


Figure 5-13. Sample Network For IP Port Filters

This sample network, which is running with the subnet mask of 255.255.255.0, shows:

- The configuration of IP port filters
- The configuration of RIP
- Serial, Ethernet, and token-ring ports

Inbound IP port filter 1 defined on the serial port (slot 1 port 2) of router 6611 A is set to prevent the workstation on Ethernet segment 9.67.5.0 from accessing the printer on Ethernet segment 9.67.3.0. Inbound IP port filter 2 defined on the serial port (slot 1 port 2) of router 6611 A is set to prevent the workstation on token-ring segment 9.67.1.0 from accessing the host on token-ring segment 9.67.2.0.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-13. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Port and Protocols Running on It

Table 5-107. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-108. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-109. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link quality monitoring protocol	Link quality monitoring protocol

Table 5-110. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.4.100	9.67.4.101
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	9.67.4.101	9.67.4.100
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Enable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-111. Serial Port - Inbound Port Filters Detail Parameters Configured

Parameter	6611 A Slot 1 Port 2 Filter 1 Value	6611 A Slot 1 Port 2 Filter 2 Value
Enable inbound port filters	Enable	Enable
IP Inbound Port Filter - Detail		
Filter ID	1	2
Filter type	Singular	Singular
Filtering mode	Deny	Deny
Filter IP address 1	9.67.5.0	9.67.1.0
Filter subnet mask 1	255.255.255.0	255.255.255.0
Filter IP address 2	NA	NA
Filter subnet mask 2	NA	NA
Protocol	None	None
Well known port filters		
Filter 1	NA	NA
Filter 2	NA	NA
Filter 3	NA	NA
Filter 4	NA	NA

Ethernet Ports and the Protocols Running on Them

Table 5-112. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	None	None

Table 5-113. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.3.1	9.67.5.5
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table 5-114. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-115. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.2.1	9.67.1.1
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-116. Node Level - RIP Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Routing Information Protocol (RIP)	Enable	Enable
Broadcast	Enable	Enable
Zero reserved fields	Enable	Enable
Route preference	100	100

Port Level Worksheets

Figure 5-14 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-14.

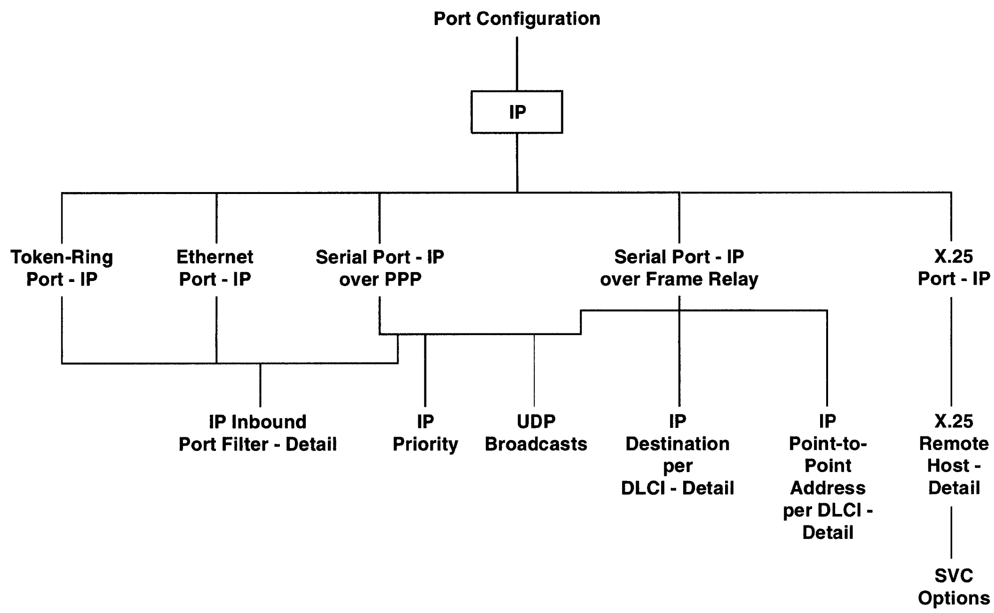


Figure 5-14. Flow of Port Level IP Help Windows

To enable adapters to transmit and receive IP packets, you need to enable IP routing at the port level. Configure IP on each adapter that will transmit and receive IP packets. Then configure any IP routing protocols (for example, OSPF, RIP, Hello, EGP, BGP), static routes, export filters, and packet filters at the node level.

Use the following tables as worksheets for your port level configurations.

- Token Ring Port - IP on page 5-114
- Ethernet Port - IP on page 5-115
- Serial Port - IP over PPP on page 5-116
- Serial Port - IP over Frame Relay on page 5-117
- IP Destination per DLCI - Detail on page 5-118
- IP Point-to-Point Addresses per DLCI on page 5-118
- X.25 Port - IP on page 5-118
- X.25 Remote Host - Detail on page 5-119
- SVC Options on page 5-120

- IP Inbound Port Filters on page 5-121
- IP Priority on page 5-123
- UDP Broadcasting on page 5-123

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-13 on page D-12 for a mapping of parameter names and their associated labels.

Table 5-117. Configuration Worksheet - Token Ring Port - IP

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable IP routing on this port Enable, Disable Disable This parameter enables or disables IP routing on a port.	
Parameter **Valid Values** **Default** **Description**	IP address (required) Addresses can be class A, class B, class C • The class A range is 1.0.0.1 through 126.255.255.254 • The class B range is 128.0.0.1 through 191.255.255.254 • The class C range is 192.0.0.1 through 223.255.255.254 None This parameter defines the IP address of this port.	
Parameter **Valid Values** **Default** **Description**	Subnet mask Value between 0.0.0.0 and 255.255.255.255. 255.255.255.255 The subnet mask must cover the network portion of the IP address.	
Parameter **Valid Values** **Default** **Description**	Maximum transmission unit • 4 MB Token ring: 256 to 4472 bytes • 16 MB Token ring: 256 to 17800 bytes • Version 2.0 Ethernet: 256 to 1500 bytes • 802.3 Ethernet: 256 to 1492 bytes • Serial (V.35/36): 256 to 2048 bytes • X.25: 256 to 4096 bytes • Token ring - 1492 • Ethernet - 1492 • Serial - 1500 • X.25 - 576 The maximum transmission unit (MTU) is the number of bytes per frame of data that can be transferred across a given physical network.	
Parameter **Valid Values** **Default** **Description**	Enable Internet Control Message Protocol (ICMP) address mask requests Enable, Disable Enable This parameter allows a network administrator to enable or disable ICMP mask requests.	
Parameter **Valid Values** **Default** **Description**	Directed broadcast Enable, Disable Disable This parameter enables or disables directed broadcast. When this parameter is set to **Enable** and IP receives an *all host broadcast* UDP message that is destined for another interface in this router, IP forwards the message to that interface.	

Table 5-118. Configuration Worksheet - Ethernet Port - IP

Parameter Information		Your Value
Parameter	Enable IP routing on this port	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables IP routing on a port.	
Parameter	IP address (required)	
Valid Values	IP addresses can be class A, class B, or class C • The class A range is 1.0.0.1 through 126.255.255.254 • The class B range is 128.0.0.1 through 191.255.255.254 • The class C range is 192.0.0.1 through 223.255.255.254	
Default	None	
Description	This parameter defines the IP address of this port.	
Parameter	Subnet mask	
Valid Values	Value between 0.0.0.0 and 255.255.255.255.	
Default	None	
Description	The subnet mask must cover the network portion of the IP address.	
Parameter	Maximum transmission unit	
Valid Values	• 4 MB Token ring: 256 to 4472 bytes • 16 MB Token ring: 256 to 17800 bytes • Version 2 Ethernet: 256 to 1500 bytes • 802.3 Ethernet: 256 to 1492 bytes • Serial (V.35/36): 256 to 2048 bytes • X.25: 256 to 4096 bytes	
Default	• Token ring - 1492 • Ethernet - 1492 • Serial - 1500 • X.25 - 576	
Description	The maximum transmission unit (MTU) is the number of bytes per frame of data that can be transferred across a given physical network.	
Parameter	Ethernet framing for IP	
Valid Values	Both, Ethernet V2.0,Ethernet 802.3 SNAP	
Default	Ethernet V2.0	
Description	This parameter determines which frame types are processed correctly by the IP protocol.	
Parameter	Enable Internet Control Message Protocol (ICMP) address mask requests	
Valid Values	Enable, Disable	
Default	Enable	
Description	This parameter allows a network administrator to enable or disable ICMP mask requests.	
Parameter	Directed broadcast	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables directed broadcast. When this parameter is set to **Enable** and IP receives an *all host broadcast* UDP message that is destined for another interface in this router, IP forwards the message to that interface.	

Table 5-119. Configuration Worksheet - Serial Port - IP over PPP

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable IP routing on this port Enable, Disable Disable This parameter enables or disables IP routing on a port.	
Parameter **Valid Values** **Default** **Description**	IP address (required) IP addresses can be class A, class B, or class C • The class A range is 1.0.0.1 through 126.255.255.254 • The class B range is 128.0.0.1 through 191.255.255.254 • The class C range is 192.0.0.1 through 223.255.255.254 None This parameter defines the IP address of this port.	
Parameter **Valid Values** **Default** **Description**	Subnet mask Value between 0.0.0.0 and 255.255.255.255. 255.255.255.255 The subnet mask must cover the network portion of the IP address.	
Parameter **Valid Values** **Default** **Description**	Destination IP address (required) A valid IP address None This parameter identifies the destination IP address on a serial link. The destination IP address is required, in addition to the other IP port parameters, when configuring IP on a serial adapter port configured to support PPP. This address must be on the same network as the IP address.	
Parameter **Valid Values** **Default** **Description**	Maximum transmission unit • 4 MB Token ring: 256 to 4472 bytes • 16 MB Token ring: 256 to 17800 bytes • Version 2.0 Ethernet: 256 to 1500 bytes • 802.3 Ethernet: 256 to 1492 bytes • Serial (V.35/36): 256 to 2048 bytes • X.25: 256 to 4096 bytes • Token ring - 1492 • Ethernet - 1492 • Serial - 1500 • X.25 - 576 The maximum transmission unit (MTU) is the number of bytes per frame of data that can be transferred across a given physical network.	
Parameter **Valid Values** **Default** **Description**	Enable Internet Control Message Protocol (ICMP) address mask requests Enable, Disable Enable This parameter allows a network administrator to enable or disable ICMP mask requests.	
Parameter **Valid Values** **Default** **Description**	Enable transmission group for IP on this port Enable, Disable Disable Use this parameter to enable this port to be a part of a transmission group used to send IP traffic over PPP.	

Table 5-120 (Page 1 of 2). Configuration Worksheet - Serial Port - IP over Frame Relay

Parameter Information		Your Value
Parameter	Enable IP routing on this port	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables IP routing on a port.	
Parameter	IP address (required)	
Valid Values	IP addresses can be class A, class B, or class C • The class A range is 1.0.0.1 through 126.255.255.254 • The class B range is 128.0.0.1 through 191.255.255.254 • The class C range is 192.0.0.1 through 223.255.255.254	
Default	None	
Description	This parameter defines the IP address of this port.	
Parameter	Subnet mask	
Valid Values	Value between 0.0.0.0 and 255.255.255.255.	
Default	255.255.255.255.	
Description	The subnet mask must cover the network portion of the IP address.	
Parameter	Maximum transmission unit	
Valid Values	• 4 MB Token ring: 256 to 4472 bytes • 16 MB Token ring: 256 to 17800 bytes • Version 2.0 Ethernet: 256 to 1500 bytes • 802.3 Ethernet: 256 to 1492 bytes • Serial (V.35/36): 256 to 2048 bytes • X.25: 256 to 4096 bytes	
Default	• Token ring - 1492 • Ethernet - 1492 • Serial - 1500 • X.25 - 576	
Description	The maximum transmission unit (MTU) is the number of bytes per frame of data that can be transferred across a given physical network.	
Parameter	Enable Internet Control Message Protocol (ICMP) address mask requests	
Valid Values	Enable, Disable	
Default	Enable	
Description	This parameter allows a network administrator to enable or disable ICMP mask requests.	
Parameter	Directed broadcast	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables directed broadcast. When this parameter is set to **Enable** and IP receives an *all host broadcast* UDP message that is destined for another interface in this router, IP forwards the message to that interface. **Note:** This parameter is not available when either of the following is true: • The Point-to-point only parameter is enabled. • **Point-to-point** is selected as the value for the Assignment for discovered DLCIs parameter.	
Parameter	Point-to-point only	
Valid Values	Enable, disable	
Default	Disable	
Description	When this parameter is enabled, this interface will *only* support point-to-point links. Broadcast or mesh connections will not be supported on this interface.	

Table 5-120 (Page 2 of 2). Configuration Worksheet - Serial Port - IP over Frame Relay

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Assignment for discovered DLCIs Mesh, Point-to-point Mesh This parameter indicates whether the DLCIs, which are discovered via the LMI options, will be assigned to the meshed network on this port or to a point-to-point link on this port.	

Table 5-121. Configuration Worksheet - IP Destination per DLCI - Detail

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	DLCI number (required) Any DLCI configured for this port (the DLCIs are displayed in the user interface) None This parameter defines the DLCI number that provides a logical connection to a router with an IP address given in the Destination IP address parameter.	
Parameter **Valid Values** **Default** **Description**	Destination IP address A valid IP address None This parameter defines the destination IP address for this DLCI connection on this serial port. The destination IP address must be on the same network as the IP address.	

Table 5-122. Configuration Worksheet - IP Point-to-Point Addresses per DLCI

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	IP point-to-point destination A valid IP address None This is the destination IP address for the DLCI connection on this serial port. This parameter may be entered multiple times on the same frame relay port, to a maximum of 90 addresses per port and 120 addresses per 6611.	
Parameter **Valid Values** **Default** **Description**	DLCI number A valid DLCI that is not specified as a DLCI for the mesh network. None This is the DLCI number for a point-to-point link that provides a logical connection to a router with an IP address.	

Table 5-123 (Page 1 of 2). Configuration Worksheet - X.25 Port - IP

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable IP routing on this port Enable, Disable Enable This parameter enables or disables IP routing on a port. When this parameter is set to **Disable**, configuration date for IP is retained.	

Table 5-123 (Page 2 of 2). Configuration Worksheet - X.25 Port - IP

Parameter Information		Your Value
Parameter	IP address (required)	
Valid Values	Addresses can be class A, class B, or class C. • The class A range is 1.0.0.1 through 126.255.255.254 • The class B range is 128.0.0.1 through 191.255.255.254 • The class C range is 192.0.0.1 through 223.255.255.254	
Default Value	None.	
Description	This parameter identifies the IP address of this port. The address selected for this port cannot be the same address as any other port.	
Parameter	Subnet mask	
Valid Values	Addresses can be class A, class B, or class C. • The class A range is 1.0.0.1 through 126.255.255.254 • The class B range is 128.0.0.1 through 191.255.255.254 • The class C range is 192.0.0.1 through 223.255.255.254	
Default Value	None	
Description	The subnet mask is a 32-bit internet address that corresponds to the physical network and the host identifier. If you answer this parameter, then you must enter a subnet mask of value between 000.000.000.000 to 255.255.255.255. The subnet mask is optional with the Ethernet, the Token-Ring Network 16/4, and the X.25 adapters. The subnet mask must cover the network portion of the IP address.	
Parameter	Maximum transmission unit	
Valid Values	• 4 MB Token ring: 256 to 4472 bytes • 16 MB Token ring: 256 to 17800 bytes • Version 2.0 Ethernet: 256 to 1500 bytes • 802.3 Ethernet: 256 to 1492 bytes • Serial (V.35/36): 256 to 2048 bytes • X.25: 256 to 4096 bytes	
Default	• Token ring - 1492 • Ethernet - 1492 • Serial - 1500 • X.25 - 576	
Description	The maximum transmission unit (MTU) is the number of bytes per frame of data that can be transferred across a given physical network.	
Parameter	Enable ICMP address mask requests	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter allows a network administrator to enable or disable ICMP address mask requests. If the router receives an ICMP address mask request and this parameter is set to **Enable**, the router will return the IP net mask of the requested network.	

Table 5-124 (Page 1 of 2). Configuration Worksheet - X.25 Remote Host - Detail

Parameter Information		Your Value
Parameter	Destination IP address for X.25 (required)	
Valid Values	A valid IP address	
Default	None	
Description	This parameter specifies the destination IP address to map to an X.25 virtual circuit. The destination IP address for X.25 must be on the same network as the IP address for this X.25 adapter.	

Table 5-124 (Page 2 of 2). Configuration Worksheet - X.25 Remote Host - Detail

Parameter Information		Your Value
Parameter	Virtual circuit type	
Valid Values	SVC, PVC	
Default Value	SVC	
Description	This parameter defines the type of virtual circuit to be associated with the Destination IP address for X.25 parameter.	
SVC Only		
Parameter	Remote DTE address (required when the Virtual circuit type parameter is set to **SVC**)	
Valid Values	1 to 15 decimal digits	
Default Value	None	
Description	This parameter defines the X.25 address of the remote DTE.	
PVC Only		
Parameter	Logical channel number	
Valid Values	The range must lie between the value of the Lowest logical channel number for a PVC parameter and the value of the equation (from these parameters) [Lowest logical channel number for a PVC + Number of logical channels for PVCs - 1]	
Default Value	The value of the Lowest logical channel number for a PVC parameter.	
Description	Use this parameter to enter the logical channel number of the PVC that will be used to communicate with the remote host.	

Table 5-125 (Page 1 of 2). Configuration Worksheet - SVC Options

Parameter Information		Your Value
Parameter	Receive packet size	
Valid Values	64, 128, 256, 512, 1024, 2048, 4096, None. The values 2048 and 4096 are allowed only if the CCITT Support parameter is set to with **1984**.	
Default Value	None	
Description	This parameter defines the desired receive packet size to be used with this virtual circuit.	
Parameter	Transmit packet size	
Valid Values	64, 128, 256, 512, 1024, 2048, 4096, None. The values 2048 and 4096 are allowed only if the CCITT support parameter is set to **1984**.	
Default Value	None	
Description	This parameter defines the desired transmit packet size to be used with this virtual circuit.	
Parameter	Receive packet window size	
Valid Values	If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31	
Default Value	None	
Description	This parameter represents the desired receive packet window size for this SVC. Answer this parameter only if you are subscribed to the Flow control parameter negotiation facility.	
Parameter	Transmit packet window size	
Valid Values	If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31	
Default Value	None	
Description	This parameter represents the desired transmit packet window size for this SVC. Answer this parameter only if you are subscribed to the Flow control parameter negotiation facility.	

Table 5-125 (Page 2 of 2). Configuration Worksheet - SVC Options

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Closed user group index 00 to 99, or 0000 to 9999 None This parameter defines the closed user group (CUG) index. The basic format of a CUG is 2 decimal digits. The extended format of a CUG is 4 decimal digits and is allowed only when the CCITT support parameter is set to **1984**.	
Parameter **Valid Values** **Default Value** **Description**	CUG with outgoing access index 00 through 99, or 0000 through 9999. None This parameter defines the index of the CUG with outgoing access. The basic format of a CUG is 2 decimal digits. The extended format of a CUG is 4 decimal digits and is allowed only when the CCITT support parameter is set to **1984**.	
Parameter **Valid Values** **Default Value** **Description**	User-defined facilities 0 to 16 hexadecimal digits None This parameter defines the optional user-defined facilities to be used in the call request packet. Facilities other than the listed parameters can be included in the call request packets by coding them in this parameter.	
Parameter **Valid Values** **Default Value** **Description**	RPOA indices Up to 10 indexes, each index being 4 decimal digits (up to 40 characters can be entered). None This parameter defines the data network identification code or codes identifying the requested Recognized Private Operating Agency (RPOA) transit network.	

Table 5-126 (Page 1 of 2). Configuration Worksheet - IP Inbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable Inbound Port Filters Enable, Disable Disable This parameter enables or disables all IP filters that are defined for this port.	
Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	IP filter ID (required for each filter defined) 1 to 50 None This parameter specifies the ID of a port level IP filter (an IP filter that is applied to inbound IP traffic received on a specific 6611 adapter port).	
Parameter **Valid Values** **Default** **Description**	Filter type Singular, Dual Singular This parameter specifies the type of filter for a specific IP filter ID.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter specifies whether the traffic for a specific IP filter ID is to be permitted through the IBM 6611 or is to be discarded.	

Table 5-126 (Page 2 of 2). Configuration Worksheet - IP Inbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Filter IP address 1 (required for each filter defined) A valid IP address None This parameter specifies the address of the host, subnetwork, or network for a specific IP filter ID.	
Parameter **Valid Values** **Default** **Description**	Filter IP address 2 A valid IP address None This parameter specifies the address of the host, subnetwork, or network for a specific IP filter ID.	
Parameter **Valid Values** **Default** **Description**	Filter subnet mask 1 0.0.0.0 to 255.255.255.255 255.255.255.255 This parameter specifies the mask for a specific IP filter ID. The mask, with the Filter IP address 1 parameter, defines the range of IP addresses to be filtered.	
Parameter **Valid Values** **Default** **Description**	Filter subnet mask 2 0.0.0.0 to 255.255.255.255 255.255.255.255 This parameter specifies the mask for a specific IP filter ID. The mask, with the Filter IP address 2 parameter, defines the range of IP addresses to be filtered.	
Well-known Port Filter - Parameters configured for each well-known port filter defined		
Parameter **Valid Values** **Default** **Description**	Protocol None, TCP or UDP None This parameter specifies an IP protocol (TCP or UDP) well-known port. The IP filter is applied to that port.	
Parameter **Valid Values** **Default** **Description**	Filter 1 1 to 1023 None This parameter specifies the first selected TCP or UDP well-known port associated with this filter ID.	
Parameter **Valid Values** **Default** **Description**	Filter 2 1 to 1023 None This parameter specifies the second selected TCP/UDP well-known port associated with this filter ID.	
Parameter **Valid Values** **Default** **Description**	Filter 3 1 to 1023 None This parameter specifies the third selected TCP or UDP well-known port associated with this filter ID.	
Parameter **Valid Values** **Default** **Description**	Filter 4 1 to 1023 None This parameter specifies the fourth selected TCP or UDP well-known port associated with this filter ID.	

Note: A maximum of 50 port level IP filters can be configured for each port.

Table 5-127. Configuration Worksheet - IP Priority

Parameter Information		Your Value
Parameter	Enable IP priority	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables IP priority for a physical port.	
Parameter	Default priority for IP	
Valid Values	Low, medium, high	
Default	Medium	
Description	This parameter specifies the default priority. IP traffic is transmitted at the default priority setting.	
Prioritized Ports List - Parameters configured for each prioritized port defined		
Parameter	IP port number (required for each prioritized port defined)	
Valid Values	0 to 65 535	
Default	None	
Description	This parameter specifies a TCP or UDP port to which you assign a priority.	
Parameter	Port type	
Valid Values	TCP, UDP	
Default	TCP	
Description	This parameter specifies the protocol for the logical port specified in the IP port number parameter.	
Parameter	Priority	
Valid Values	Low, medium, high	
Default	Medium	
Description	This parameter defines the priority for the TCP or UDP port specified in the IP port number parameter.	

Table 5-128. Configuration Worksheet - UDP Broadcasting

Parameter Information		Your Value
Parameter	Enable UDP broadcast forwarding	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables and disables the forwarding of UDP packets from this port.	
Parameter	UDP port	
Valid Values	0 to 65 535	
Default	None	
Description	This parameter identifies a UDP port for which broadcast forwarding is enabled.	
Parameter	Target UDP port IP address	
Valid Values	A valid IP address	
Default	None	
Description	This parameter identifies the local IP address of a 6611 port to which UDP broadcasts will be forwarded.	

Node Level Worksheets

To enable the 6611 to route IP packets across the network, you need to enable IP routing at the node level. Use the following table as a worksheet for your node level configuration.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-13 on page D-12 for a mapping of parameter names and their associated labels.

Table 5-129. Configuration Worksheet - IP Routing

Parameter Information		**Your Value**
Parameter	Connection decay interval	
Valid Values	1 to 20 minutes	
Default	10 minutes	
Description	This parameter defines how long an inactive Address Resolution Protocol (ARP) entry will remain in the Internet Protocol (IP) ARP table before it is deleted.	

IP Border Gateway Protocol (BGP)

BGP is an inter-autonomous system routing protocol for exchanging network reachability information.

A BGP router exchanges information about the networks that it can reach. That information is used to construct a graph representing the topology of all autonomous systems using BGP to share network reachability, which facilitates detection and elimination of problems, such as routing loops.

BGP uses TCP to establish a connection between two BGP neighbors (in this case, the 6611 and another router using BGP). After the TCP connection has been established, the BGP neighbors exchange their full routing tables. After the initial exchange of routing tables, the BGP neighbors exchange only changes to the routing tables. For each network that can be reached via the BGP neighbor, the routing table indicates the complete autonomous system path to the network.

BGP uses a policy-based algorithm to determine the best path to an autonomous system. The routing policies used by the algorithm are based partly on the information you specify during configuration of the router.

Restrictions

When routes are exported from or to BGP, it is necessary to define the autonomous system number to or from which the routes are being exported.

For example, to configure an autonomous system boundary router running OSPF in the local autonomous system and using BGP to attach to autonomous system 1002, it would be necessary to:

- Export from BGP 1002 to OSPFASE
- Export from OSPF and OSPFASE to BGP 1002

The correct autonomous system number must be specified for the export to be successful.

See "Sample Network Graphic" on page 5-127 for an example of a BGP export.

Configuration Changes...

That Require the BGP Function to Restart

None

That Require the 6611 to Restart

None

Configuration Options

Using the Configuration Program, you will:

1. **Specify the global default parameters.**

   You will specify, on the BGP window, the parameter values to be applied to the 6611. These parameter values establish the global default values for each BGP group that you define.

2. **Specify the BGP group and BGP neighbor parameters.**

On the BGP Group Detail window, you will define each BGP group. For each BGP group, you will specify the BGP neighbors in the group. At least one BGP neighbor (configured or unconfigured) must be specified per BGP group. The BGP group values establish the default values for the BGP neighbors in the group.

3. **Specify the BGP import filter parameters.**

   On the BGP Import Detail window, you will specify the BGP import filter parameters for each autonomous system from which routes are to be imported. Import filters regulate which routes are accepted when routes are exported to BGP.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform BGP routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-130 (Page 1 of 2). BGP Configuration Verification Checklist

BGP Rule	**Configuration Parameter**	√
Node-Level Parameters:		
Enable the Enable Border Gateway Protocol (BGP) parameter.	Enable Border Gateway Protocol (BGP)	
Set the BGP group type parameter to **External**, **Internal**, or **IGP** if you want to route BGP. When this parameter is set to **Test**, BGP is not routed.	BGP group type	
When the BGP group type parameter is set to **Internal** or **IGP**, the 6611s listed in the BGP Neighbors list must have the same value for the autonomous node number parameter.	BGP group type	
	Autonomous node number	
When two BGP neighbors are in the same autonomous node and they are routing IP using OSPF, set the Group type parameter to **IGP**.	Autonomous node number	
When two BGP neighbors are in the same autonomous node and they are *not* routing IP using OSPF, set the Group type parameter to **Internal**.	Enable OSPF	
	BGP group type	
When two BGP neighbors are in different autonomous nodes, set the Group type parameter to **External**.	Autonomous node number	
	BGP group type	
When the BGP group type parameter is set to **External** or **Internal**, the IP addresses of the BGP neighbors must be in the same subnet.	BGP group type	
	IP address	
For every BGP group defined, set the Neighbor type parameter of at least one configured BGP neighbor or at least one unconfigured BGP neighbor to **All**.	BGP group name	
	BGP neighbor IP address	
	Neighbor type	
When a BGP group has a value configured for the Interface IP address parameter, the subnet portion of the BGP neighbor IP address parameter must match the subnet portion of Interface IP address parameter for the group. The exception to this rule is when the BGP group is an IGP group; in this case, the neighbor does not have to be connected to an attached interface and the subnet portion of the IP address may be different.	BGP group name	
	Interface IP address	
	BGP neighbor IP address	

Table 5-130 (Page 2 of 2). BGP Configuration Verification Checklist

BGP Rule	**Configuration Parameter**	√
When a configured neighbor has a value configured for the Interface IP address parameter, the subnet portion of the Next hop destination parameter must match the subnet portion of the Interface IP address parameter for the configured neighbor.	Interface IP address	
	Next hop destination	
When a configured neighbor does not have a value configured for the Interface IP address parameter, the subnet portion of the Next hop destination parameter must match the subnet portion of the Interface IP address parameter of the BGP group.	Interface IP address	
	Next hop destination	
	Interface IP address	
When a BGP group does not have a value configured for the Interface IP address parameter, the subnet portion of the Next hop destination parameter must match the subnet portion of the IP address of a port that attaches this 6611 to the WAN.	Interface IP address	
	Next hop destination	
	IP address	
Port-Level Parameters:		
For the ports that connect each 6611 to the WAN: • Enable the Enable IP routing on this port parameter. • Configure the IP address parameter.	Enable IP routing on this port	
	IP address	

Sample Network Graphic

Figure 5-15 on page 5-128 shows two 6611s (6611 C and 6611 D) configured as autonomous system boundary routers that use BGP to communicate. Both autonomous systems are running OSPF as their Interior Gateway Protocol.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - An Ethernet port running OSPF
  - A token-ring port running OSPF
- 6611 B, which has the following port types and protocols running:
  - An Ethernet port running OSPF
  - Two token-ring ports running OSPF
- 6611 C, which has the following port types and protocols running:
  - A serial port running BGP and OSPF over PPP
  - Two Ethernet ports running OSPF
- 6611 D, which has the following port types and protocols running:
  - A serial port running BGP and OSPF over PPP
  - Two token-ring ports running OSPF

The following information is shown in Figure 5-15 on page 5-128:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*
- Segment numbers

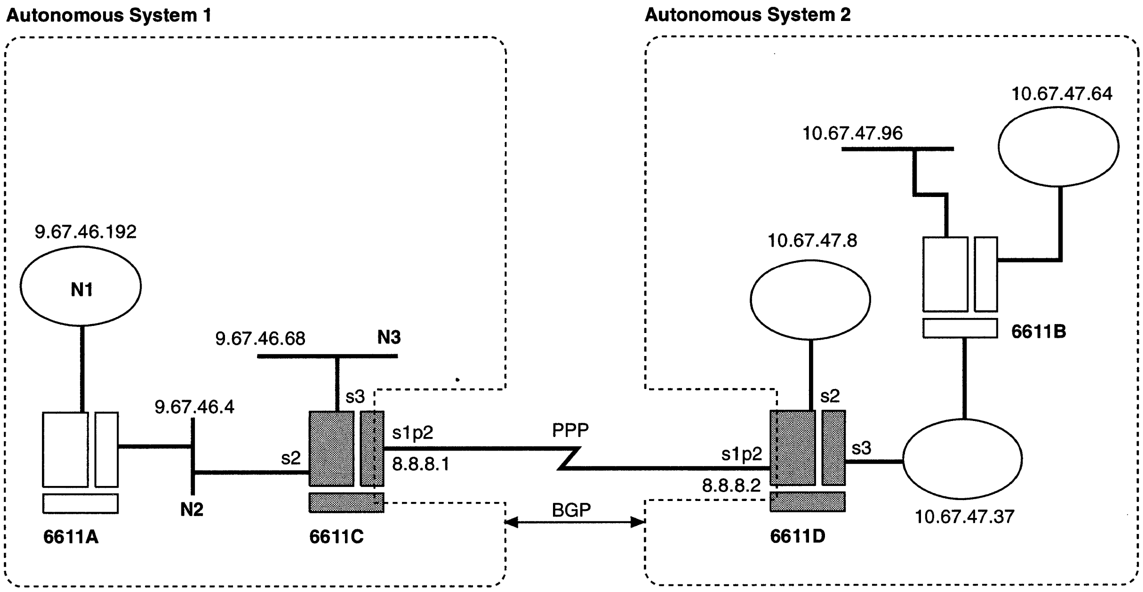


Figure 5-15. Sample Network Using BGP over a PPP Connection

Figure 5-15 shows:

- The configuration of BGP
- The configuration of OSPF
- Route exports between BGP and OSPF

Autonomous system 1 is running with the subnet mask of 255.255.255.192. Autonomous system 2 is running with the subnet mask of 255.255.255.224. The PPP link between routers 6611 C and 6611 D is running with the subnet mask of 255.255.255.252.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-15. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Port and Protocols Running on It

Table 5-131. Serial Port Parameters Configured

Parameter	6611 C Slot 1 Port 2 Value	6611 D Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-132. Serial Port - Physical Interface Parameters Configured

Parameter	6611 C Slot 1 Port 2 Value	6611 D Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56000	56000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-133. Serial Port - PPP Parameters Configured

Parameter	6611 C Slot 1 Port 2 Value	6611 D Slot 1 Port 2 Value
Enable Point-to-Point protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-134. Serial Port - IP over PPP Parameters Configured

Parameter	6611 C Slot 1 Port 2 Value	6611 D Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.252	255.255.255.252
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Ports and the Protocols Running on Them

Table 5-135. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 C Slot 2 Value	6611 C Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	None	None
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	None	None

Table 5-136. Ethernet Port - IP Parameters Configured

Parameter	6611 C Slot 2 Value	6611 C Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.4	9.67.46.68
Subnet mask	255.255.255.192	255.255.255.192
Max. transmission unit (octets)	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table 5-137. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 D Slot 2 Value	6611 D Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-138. Token-Ring Port - IP Parameters Configured

Parameter	6611 D Slot 2 Value	6611 D Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	10.67.47.8	10.67.47.37
Subnet mask	255.255.255.224	255.255.255.224
Max. transmission unit (octets)	2000	2000
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-139. Node Level - OSPF Parameters Configured

Parameter	6611 C Value	6611 D Value
Enable OSPF	Enable	Enable
Router ID	9.67.46.68	10.67.47.37

Table 5-140. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 C Value	6611 D Value
Area ID	0.0.0.0	0.0.0.0
Area type	NA	NA
Stub cost	NA	NA
Authentication type	Simple	Simple

Table 5-141. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 C Value 1	6611 C Value 2	6611 D Value 1	6611 D Value 2
Interface IP address	9.67.46.4	9.67.46.68	10.67.47.8	10.67.47.37
Interface type	Broadcast	Broadcast	Broadcast	Broadcast
Authorization key	Raleigh	Raleigh	Raleigh	Raleigh
Retransmit interval	5	5	5	5
Router priority	1	1	1	1
Interface transit delay	1	1	1	1
Cost	default	default	default	default
Router dead interval	40	40	40	40
Poll interval	NA	NA	NA	NA
Hello interval	10	10	10	10

Border Protocol (EGP/BGP) Parameters Configured

Table 5-142. Node Level - Border Protocols Parameters Configured

Parameter	6611 C Value	6611 D Value
EGP	Disable	Disable
BGP	Enable	Enable
Generate default route	Enable	Enable
Local autonomous system number	1001	1002

Table 5-143. Node Level - BGP Parameters Configured

Parameter	6611 C Value	6611 D Value
Enable Border Gateway Protocol (BGP)	Enable	Enable
Default preference	200	200
Default metric	1	1
Import filters	Disable	Disable

Table 5-144. Node Level - BGP Groups Parameters Configured

Parameter	6611 C Value	6611 D Value
Autonomous system number	1002	1001
BGP group type	External	External
BGP group name	ASN1002	ASN1001
Metric out	1	1
Next hop destination	None	None
Interface IP address	8.8.8.2	8.8.8.1
Generate default route	Enable	Enable
Passive	Disable	Disable
Default network in	Disable	Disable
Default network out	Disable	Disable
Preference	150	150
Hold time	180	180

Table 5-145. Node Level - Configured Neighbor Parameters Configured

Parameter	6611 C Value	6611 D Value
BGP neighbor IP address	8.8.8.2	8.8.8.1
BGP neighbor name	6611 D	6611 C
Metric out	1	1
Next hop destination	None	None
Interface IP address	8.8.8.2	8.8.8.1
Generate default route	Enable	Enable
Passive	Disable	Disable
Default network in	Disable	Disable
Default network out	Disable	Disable
Preference	150	150
Hold time	180	180

Table 5-146. Node Level - Export Filter Parameters Configured

Parameter	**6611 C Filter 1 Value**	**6611 C Filter 2 Value**	**6611 C Filter 3 Value**	**6611 C Filter 4 Value**	**6611 C Filter 5 Value**	**6611 D Filter 1 Value**	**6611 D Filter 2 Value**	**6611 D Filter 3 Value**	**6611 D Filter 4 Value**	**6611 D Filter 5 Value**
From protocol										
From protocol	EGP/BGP Default	Direct	BGP	OSPF	OSPFASE	EGP/BGP Default	Direct	BGP	OSPF	OSPFASE
AS number	NA	NA	1002	NA	NA	NA	NA	1001	NA	NA
Origin	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
AS path specification	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
To protocol										
To protocol	OSPFASE	BGP	OSPFASE	BGP	BGP	OSPFASE	BGP	OSPFASE	BGP	BGP
AS number	NA	1002	NA	1002	1002	NA	1001	NA	1001	1001
Tag	1	NA	1	NA	NA	1	NA	1	NA	NA
Type	2	NA	2	NA	NA	2	NA	2	NA	NA
Routes to be exported										
Route(s) to be exported	All	All	All	All	All	All	All	All	All	All
Restrict export	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable
Metric	1	1	1	1	1	1	1	1	1	1
Specific route	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Mask	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

Node Level Worksheets

Figure 5-16 on page 5-134 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-16 on page 5-134.

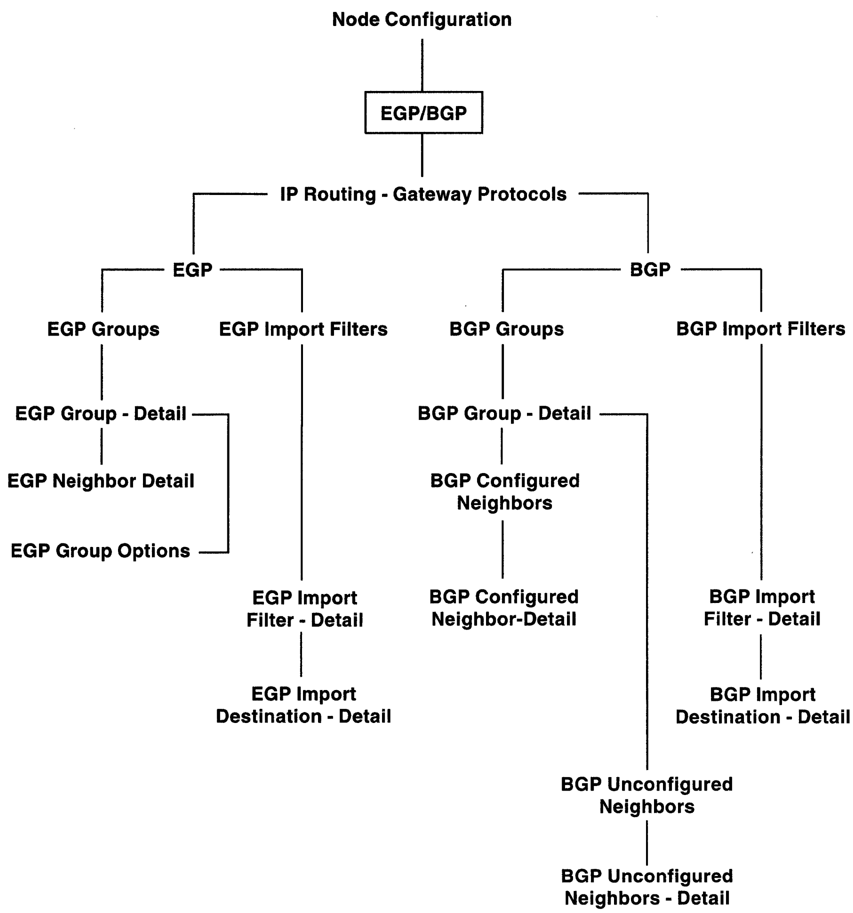


Figure 5-16. Flow of Node Level BGP Windows

To enable the adapter to transmit and receive BGP packets, you need to enable IP routing at the port level. Configure IP on each adapter that will transmit and receive IP packets. See "IP Protocol" on page 5-103 for more information. Then configure BGP at the node level.

Use the following tables as worksheets for your node level configurations.

- IP Routing - Gateway Protocols on page 5-135
- BGP on page 5-135
- BGP Group - Detail on page 5-135
- BGP Configured Neighbor - Detail on page 5-137
- BGP Unconfigured Neighbor - Detail on page 5-138
- BGP Import Filters on page 5-138

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-5 on page D-7 for a mapping of parameter names and their associated labels.

Table 5-147. Configuration Worksheet - IP Routing - Gateway Protocols

Parameter Information	Your Value
Parameter Generate default route **Valid Values** Enable, Disable **Default** Disable **Description** When set to **Enable**, this parameter generates a default route pointer to this 6611. This route can be exported to other protocols using the protocol default.	
Parameter Local autonomous system number **Valid Values** 1 to 65534 **Default** None **Description** This parameter defines the autonomous system number (ASN) for this 6611.	

Table 5-148. Configuration Worksheet - BGP

Parameter Information	Your Value
Parameter Enable Border Gateway Protocol (BGP) **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables BGP.	
Parameter Default preference **Valid Values** 0 to 255 (with the lowest value being the most preferred) **Default Value** None **Description** This parameter defines the preference value that BGP assigns to all routes learned by the IBM 6611 (unless a preference is assigned to a particular BGP group, BGP configured neighbor, or BGP import).	
Parameter Default metric **Valid Values** 0 to 65535 **Default Value** None **Description** This parameter specifies the default metric used by BGP when propagating the routes learned from other protocols (for example, OSPF).	

Table 5-149 (Page 1 of 2). Configuration Worksheet - BGP Group - Detail

Parameter Information	Your Value
Parameter Autonomous system number (required for each BGP group defined) **Valid Values** 1 to 65534 **Default Value** None **Description** The neighbors in the BGP group must reside in an autonomous system. This parameter specifies the autonomous system number of the neighboring autonomous system.	
Parameter BGP group type **Valid Values** External, Test, Internal, IGP **Default Value** External **Description** This parameter specifies whether this group is external, test, internal, or an Interior Gateway Protocol (IGP).	
Parameter BGP group name **Valid Values** Any alphanumeric from 1 to 16 characters in length **Default Value** None **Description** This parameter specifies a user-defined name for a BGP group.	

Table 5-149 (Page 2 of 2). Configuration Worksheet - BGP Group - Detail

Parameter Information	Your Value
Parameter Metric out **Valid Values** 0 to 65 535 **Default Value** None **Description** This parameter specifies the default metric given by the 6611 to all routes propagated to neighbors in this BGP group.	
Parameter Next hop destination **Valid Values** Any IP address defined for this IBM 6611 in which the host portion of the address is non-zero **Default Value** None **Description** This parameter specifies the IP address of the border router to be used as the next hop to the networks listed in the IBM 6611 updates to this BGP group. Next hop destination must be on the same network as the interface IP address.	
Parameter Interface IP address **Valid Values** An IP address defined for this IBM 6611 **Default Value** None **Description** This parameter specifies the IP address, of the interface on the IBM 6611, to use when connecting to neighbors in this BGP group.	
Parameter Generate default route **Valid Values** Enable, Disable **Default Value** Enable **Description** When set to **Disable**, this parameter specifies that the internal default route will *not* be used for routing information learned from this BGP group. When set to **Enable**, this parameter specifies that BGP will use the setting of the Generate default route parameter on the IP Routing - Gateway Protocols window.	
Parameter Passive **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter specifies that active opens to this BGP group should not be attempted.	
Parameter Default network in **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter controls whether the default network (0.0.0.0) can be imported in updates exchanged with this BGP group.	
Parameter Default network out **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter controls whether the default network (0.0.0.0) can be exported in updates exchanged with this BGP configured neighbor.	
Parameter Preference **Valid Values** 0 to 255 (with the lowest value being the most preferred) **Default Value** None **Description** This parameter specifies the preference value for routes that are learned from any BGP configured or unconfigured neighbor in this BGP group.	
Parameter Hold time **Valid Values** 20 to 65 535 **Default Value** None **Description** This parameter specifies the maximum number of seconds that can elapse between the receipt of successive keepalive, update, or notification messages before the connection will be closed.	

Table 5-150 (Page 1 of 2). Configuration Worksheet - BGP Configured Neighbor - Detail

Parameter Information		Your Value
Parameter	BGP neighbor IP address (required for each BGP neighbor defined)	
Valid Values	A valid IP address. The host portion of the address must be non-zero.	
Default Value	None	
Description	This parameter specifies the IP address of a BGP configured neighbor.	
Parameter	BGP neighbor name	
Valid Values	Any alphanumeric from 1 to 16 characters in length	
Default Value	None	
Description	This parameter defines the origin of the path information you specified for the Autonomous system path specification parameter.	
Parameter	Metric out	
Valid Values	0 to 65535	
Default Value	None	
Description	This parameter specifies the default metric given by the IBM 6611 to all routes propagated to this BGP neighbor. This parameter is ignored for Interior Gateway Protocol (IGP) neighbors.	
Parameter	Next hop destination	
Valid Values	Any IP address defined for this IBM 6611 in which the host portion of the address is non-zero	
Default Value	None	
Description	This parameter specifies the IP address of the border router to be used as the next hop to the networks listed in the IBM 6611 updates to this BGP configured neighbor. Next hop destination must be on the same network as the Interface IP address.	
Parameter	Interface IP address	
Valid Values	An IP address configured for this IBM 6611	
Default Value	None	
Description	This parameter specifies the IP address of an interface on the IBM 6611 over which you want to connect to this BGP configured neighbor.	
Parameter	Generate default route	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	When set to **Disable**, this parameter specifies that the internal default route will *not* be used for routing information learned from this BGP group. When set to **Enable**, this parameter specifies that BGP will use the setting of the Generate default route parameter on the IP Routing - Gateway Protocols window.	
Parameter	Passive	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter specifies that active opens to this BGP configured neighbor should not be attempted.	
Parameter	Default network in	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter controls whether the default network (0.0.0.0) can be imported in updates exchanged with this BGP configured neighbor.	
Parameter	Default network out	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter controls whether the default network (0.0.0.0) can be exported in updates exchanged with this BGP configured neighbor.	

Table 5-150 (Page 2 of 2). Configuration Worksheet - BGP Configured Neighbor - Detail

Parameter Information	Your Value
Parameter Preference **Valid Values** 0 to 255 (with the lowest value being the most preferred) **Default Value** None **Description** This parameter specifies the preference value for routes that are learned from this BGP configured neighbor.	
Parameter Hold time **Valid Values** 20 to 65535 **Default Value** None **Description** This parameter specifies the maximum number of seconds that can elapse between receipt of successive keepalive, update, or notification messages before the connection will be closed.	

Table 5-151. Configuration Worksheet - BGP Unconfigured Neighbor - Detail

Parameter Information	Your Value
Parameter Neighbor type **Valid Values** All, Host, Network **Default Value** All **Description** This parameter specifies an unconfigured neighbor to which the IBM 6611 will allow a BGP connection.	
Parameter BGP neighbor name **Valid Values** Any alphanumeric from 1 to 16 digits in length **Default Value** None **Description** This parameter defines the origin of the path information you specified for the Autonomous system path specification parameter.	
Parameter IP address **Valid Values** Host, Network **Default Value** None **Description** This parameter specifies the IP address of a BGP unconfigured neighbor.	
Parameter Mask **Valid Values** Any mask as specified by its dotted-decimal notation **Default Value** None **Description** This parameter specifies the mask that identifies the selected network unconfigured neighbors to which this IBM 6611 can communicate.	

Table 5-152 (Page 1 of 3). Configuration Worksheet - BGP Import Filters

Parameter Information	Your Value
Parameter Enable BGP import filters **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter specifies whether BGP imports are enabled or disabled for the IBM 6611.	
BGP Imports List - Parameters configured for each BGP import defined	
Parameter BGP import name (required for each BGP import filter defined) **Valid Values** Any alphanumeric from 1 to 16 digits in length **Default Value** None **Description** The List of BGP Destinations option allows you to build a list of BGP destinations you want matched to the BGP routes imported for an autonomous system number or autonomous system path.	

Table 5-152 (Page 2 of 3). Configuration Worksheet - BGP Import Filters

Parameter Information	Your Value
Parameter Import route filters **Valid Values** AS number, AS path **Default Value** AS number **Description** This parameter specifies the autonomous system to which the import specifications for this destination apply.	
Parameter Autonomous system number (required for each BGP import) filter defined) **Valid Values** 1 to 65534 **Default Value** None **Description** This parameter specifies the autonomous system to which the import specifications for this destination apply.	
Parameter Autonomous system path specification (required conditionally) **Valid Values** From 1 to 80 integers and notational shorthand symbols as detailed in the description of this parameter **Default Value** None **Description** This parameter is used to identify one or more autonomous system paths to which you wish to apply import route filters.	
Parameter AS path origin (required conditionally) **Valid Values** IGP, EGP, Incomplete, Any **Default Value** Any **Description** This parameter defines the origin of the path information you specified for the Autonomous system pathe specification parameter. In other words, the autonomous system path origin indicates how a particular route was injected into BGP (for example, by the EGP, and IGP, or some other means).	
Parameter Restrict imports **Valid Values** Enable, Disable **Default Value** Disable **Description** When this parameter is set to **Enable**, all routes associated with the BGP import name and either the Autonomous system number parameter or Autonomous system path specification parameter will *not* be imported.	
Parameter Preference **Valid Values** 0 to 255 (with the lowest value being the most preferred) **Default Value** None **Description** This parameter defines the default preference that is assigned to all BGP routes that are imported.	
BGP Destinations List - Parameters configured for each BGP destination defined	
Parameter Destination address **Valid Values** Specific, All, Default **Default Value** Specific **Description** This parameter specifies whether to accept imports from a specific address, from all addresses, or from a default address.	
Parameter Destination IP address (required for each BGP import filter defined) **Valid Values** A valid IP address **Default Value** None **Description** This parameter specifies the destination that should be filtered.	
Parameter Destination mask **Valid Values** A valid IP address mask **Default Value** 255.255.255.255 **Description** This parameter defines the mask that will be applied to the Destination parameter for defining a range of IP addresses to be imported.	

Table 5-152 (Page 3 of 3). Configuration Worksheet - BGP Import Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Restrict routes Enable, Disable Disable Enabling this parameter restricts the routes that are specified by the Destination and Destination mask parameters from being learned by BGP.	
Parameter **Valid Values** **Default Value** **Description**	Preference 0 to 255 None This parameter defines the preference to be attached to BGP routes that are imported.	

IP Exterior Gateway Protocol (EGP)

EGP is used for communication between routers in different autonomous systems. The basic categories of communication between EGP routers are these EGP messages:

- Neighbor acquisition
- Routing update
- Neighbor reachability

Neighbor acquisition messages are used to establish communication between two routers.

Routing update messages are used to communicate among routers. EGP neighbors that agree to communicate may exchange information about the routes to all of the networks within their autonomous system. The neighbors do not exchange information about subnetworks.

Neighbor reachability messages are used to verify that an EGP neighbor still exists and is willing to communicate. EGP neighbors exchange these messages periodically.

Restrictions

When routes are exported from or to EGP, it is necessary to define the autonomous system number to or from which the routes are being exported.

For example, to configure an autonomous system boundary router running OSPF in the local autonomous system and using EGP to attach to autonomous system 1002, it would be necessary to:

- Export from EGP 1002 to OSPFASE
- Export from OSPF and OSPFASE to EGP 1002.

The correct autonomous system number must be specified for the export to be successful. See "Sample Network Graphic" on page 5-142 for an example of an EGP export.

Configuration Changes...

That Require the EGP Function to Restart

None

That Require the 6611 to Restart

None

Configuration Options

Using the Configuration Program, you will:

1. **Specify the global default parameters.**

   You will specify, on the EGP window, the parameter values to be applied to the 6611. These parameter values establish the global default values for each EGP group that you define.

2. **Specify the EGP group and EGP neighbor parameters.**

On the EGP Group Detail window, you will define each EGP group. For each EGP group, you will optionally specify the EGP neighbors in the group. The EGP group values establish the default values for the EGP neighbors in the group.

3. **Specify the EGP import filter parameters.**

   On the EGP Import Detail window, you will specify the EGP import filter parameters for each autonomous system from which routes are to be imported. Import filters regulate which routes are accepted when routes are exported to EGP.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform EGP routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-153. EGP Configuration Verification Checklist

EGP Rule	**Configuration Parameter**	√
Node-Level Parameters:		
Ensure that the Enable EGP parameter is enabled.	Enable EGP	
When an EGP group is defined, the value of the Neighbor autonomous system number parameter on this 6611 must match the value of the Local autonomous system number for each defined neighbor in that group.	Neighbor autonomous system number	
	EGP neighbor IP address	
	Local autonomous system number	
To establish an EGP connection: • IP must be enabled at the port level on both 6611s • The values of the EGP neighbor IP address parameter must correspond to directly-connected neighbors	Enable EGP	
	EGP neighbor IP address	
	IP address	
	Enable IP routing on this port	
The following parameters should have the same value on both ends on an EGP connection: • Minimum hello interval • Minimum polling interval	Minimum hello interval	
	Minimum polling interval	

Sample Network Graphic

Figure 5-17 on page 5-143 shows two 6611s (6611 C and 6611 D) configured as autonomous system boundary routers that use EGP to communicate and exchange reachability information. Both autonomous systems are running OSPF as their Interior Gateway Protocol.

This network includes:

- 6611 A, which has the following port types and protocols running:

- An Ethernet port running OSPF
- A token-ring port running OSPF

- 6611 B, which has the following port types and protocols running:
  - An Ethernet port running OSPF
  - Two token-ring ports running OSPF
- 6611 C, which has the following port types and protocols running:
  - A serial port running PPP, EGP, and OSPF
  - Two Ethernet ports running OSPF
- 6611 D, which has the following port types and protocols running:
  - A serial port running PPP, EGP, and OSPF
  - Two token-ring ports running OSPF

The following information is shown in Figure 5-17:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*
- Segment numbers

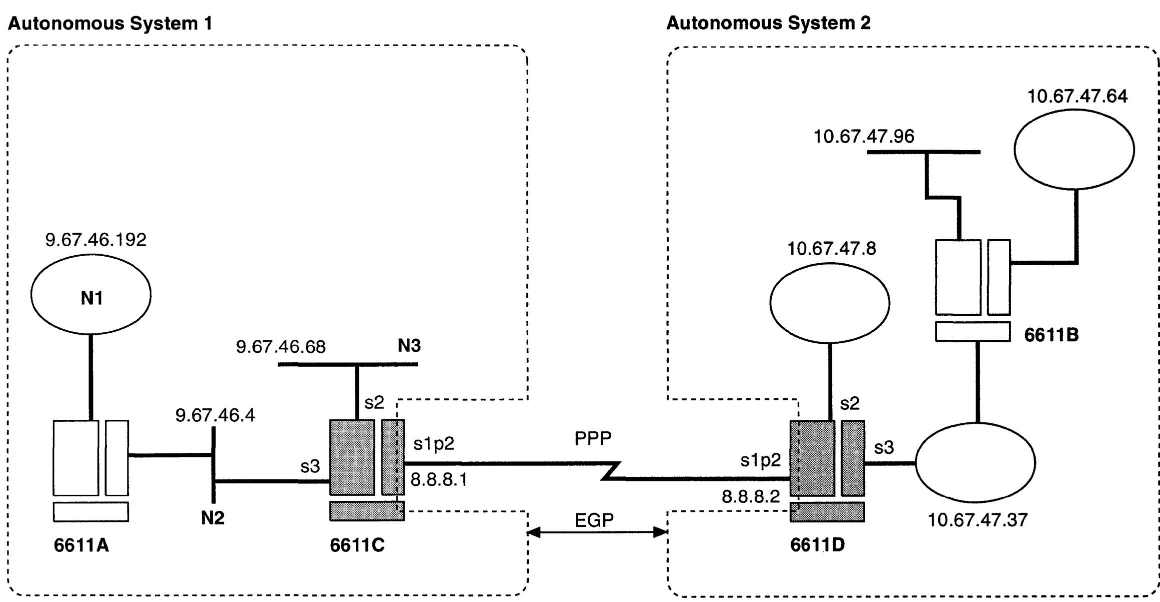


Figure 5-17. Sample Network Using EGP over a PPP Connection

Figure 5-17 shows:

- The configuration of PPP
- The configuration of EGP
- Route exports between EGP and OSPF

Autonomous system 1 is running with the subnet mask of 255.255.255.192. Autonomous system 2 is running with the subnet mask of 255.255.255.224. The PPP link between routers 6611 C and 6611 D is running with the subnet mask of 255.255.255.252.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-17 on page 5-143. The following tables list the parameters for the configuration of the 6611s in the sample network.

Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 5-154. Serial Port Parameters Configured

Parameter	**6611 C Slot 1 Port 2 Value**	**6611 D Slot 1 Port 2 Value**
Data link protocol	PPP	PPP

Table 5-155. Serial Port - Physical Interface Parameters Configured

Parameter	**6611 C Slot 1 Port 2 Value**	**6611 D Slot 1 Port 2 Value**
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56000	56000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-156. Serial Port - PPP Parameters Configured

Parameter	**6611 C Slot 1 Port 2 Value**	**6611 D Slot 1 Port 2 Value**
Enable Point-to-Point protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-157. Serial Port - IP over PPP Parameters Configured

Parameter	6611 C Slot 1 Port 2 Value	6611 D Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.252	255.255.255.252
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Ports and the Protocols Running on Them

Table 5-158. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 C Slot 2 Value	6611 C Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	None	None
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	None	None

Table 5-159. Ethernet Port - IP Parameters Configured

Parameter	6611 C Slot 2 Value	6611 C Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.4	9.67.46.68
Subnet mask	255.255.255.192	255.255.255.192
Max. transmission unit (octets)	1492	1492
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table 5-160. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 D Slot 2 Value	6611 D Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-161. Token-Ring Port - IP Parameters Configured

Parameter	6611 D Slot 2 Value	6611 D Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	10.67.47.8	10.67.47.37
Subnet mask	255.255.255.224	255.255.255.224
Max. transmission unit (octets)	2000	2000
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-162. Node Level - OSPF Parameters Configured

Parameter	6611 C Value	6611 D Value
Enable OSPF	Enable	Enable
Router ID	9.67.46.4	10.67.47.8

Table 5-163. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 C Value	6611 D Value
Area ID	0.0.0.0	0.0.0.0
Area type	NA	NA
Stub cost	NA	NA
Authentication type	Simple	Simple

Table 5-164. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 C Value 1	6611 C Value 2	6611 D Value 1	6611 D Value 2
Interface IP address	9.67.46.4	9.67.46.68	10.67.47.8	10.67.47.37
Interface type	Broadcast	Broadcast	Broadcast	Broadcast
Authorization key	Raleigh	Raleigh	Raleigh	Raleigh
Retransmit interval	5	5	5	5
Router priority	1	1	1	1
Interface transit delay	1	1	1	1
Cost	10	10	25	25
Router dead interval	40	40	40	40
Poll interval	NA	NA	NA	NA
Hello interval	10	10	10	10

Border Protocol (EGP/BGP) Parameters Configured

Table 5-165. Node Level - Border Protocols Parameters Configured

Parameter	6611 C Value	6611 D Value
EGP	Enable	Enable
BGP	Disable	Disable
Generate default route	Enable	Enable
Local autonomous system number	1001	1002

Table 5-166. Node Level - EGP Parameters Configured

Parameter	6611 C Value	6611 D Value
Enable Exterior Gateway Protocol (EGP)	Enable	Enable
Preference	200	200
Default metric	1	1
Import filters	Disable	Disable

Table 5-167. Node Level - EGP Groups Parameters Configured

Parameter	6611 C Value	6611 D Value
EGP group name	ASN1002	ASN1001
Neighbor ASN	1002	1001
Maximum active neighbors	None	None
EGP Neighbor Detail		
EGP neighbor IP address	8.8.8.2	8.8.8.1
Generate default routes from this neighbor	Enable	Enable
Import default routes	Disable	Disable
Export default routes	Disable	Disable
Minimum hello interval	30	30
Minimum polling interval	120	120
Default metric	1	1

Table 5-168. Node Level - Export Filter Parameters Configured

Parameter	**6611 C Filter 1 Value**	**6611 C Filter 2 Value**	**6611 C Filter 3 Value**	**6611 C Filter 4 Value**	**6611 C Filter 5 Value**	**6611 D Filter 1 Value**	**6611 D Filter 2 Value**	**6611 D Filter 3 Value**	**6611 D Filter 4 Value**	**6611 D Filter 5 Value**
From protocol										
From protocol	EGP/BGP Default	Direct	EGP	OSPF	OSPFASE	EGP/BGP Default	Direct	EGP	OSPF	OSPFASE
AS number	NA	NA	1002	NA	NA	NA	NA	1001	NA	NA
Origin	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
AS path specification	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
To protocol										
To protocol	OSPFASE	EGP	OSPFASE	EGP	EGP	OSPFASE	EGP	OSPFASE	EGP	EGP
AS number	NA	1002	NA	1002	1002	NA	1001	NA	1001	1001
Tag	1	NA	1	NA	NA	1	NA	1	NA	NA
Type	2	NA	2	NA	NA	2	NA	2	NA	NA
Routes to be exported										
Route(s) to be exported	All	All	All	All	All	All	All	All	All	All
Restrict export	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable
Metric	1	1	1	1	1	1	1	1	1	1
Specific route	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Mask	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

Node Level Worksheets

Figure 5-18 on page 5-149 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-18 on page 5-149.

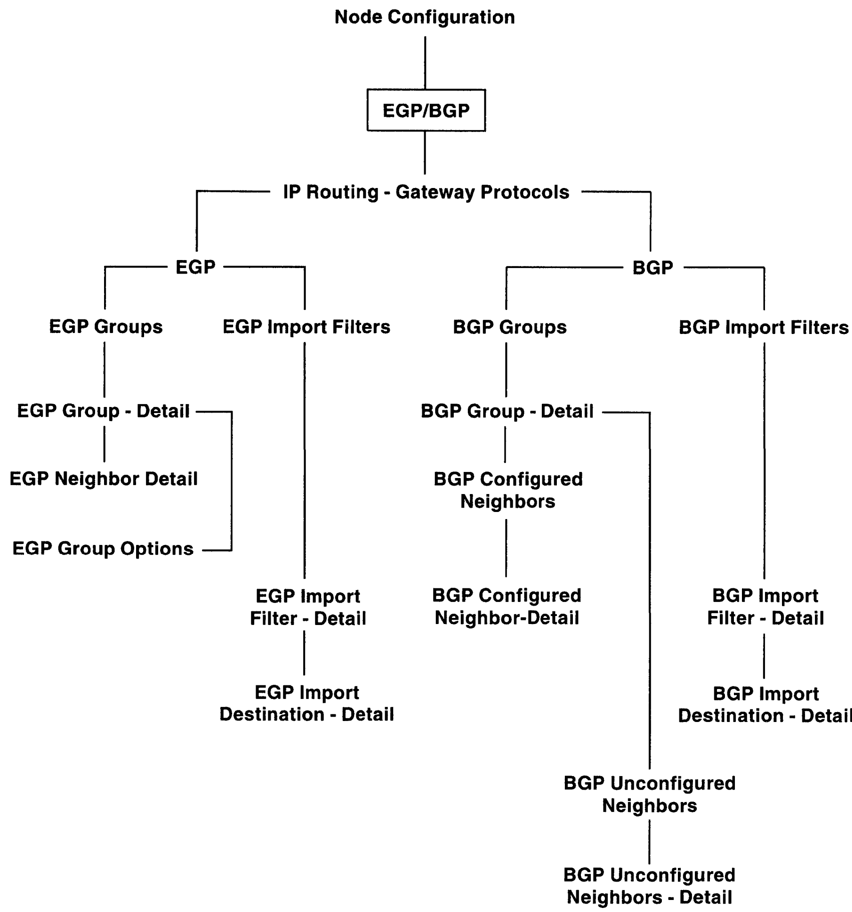


Figure 5-18. Flow of Node Level EGP Help Windows

To enable the adapter to transmit and receive EGP packets, you need to enable IP routing at the port level. Configure IP on each adapter that will transmit and receive IP packets. See "IP Protocol" on page 5-103 for more information. Then configure EGP at the node level.

Use the following tables as worksheets for your node level configurations.

- IP Routing - Gateway Protocols on page 5-150
- EGP on page 5-150
- EGP Group - Detail on page 5-150
- EGP Group Options on page 5-151
- EGP Import Filters on page 5-152

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-10 on page D-11 for a mapping of parameter names and their associated labels.

Table 5-169. Configuration Worksheet - IP Routing - Gateway Protocols

Parameter Information		Your Value
Parameter	Generate default route	
Valid Values	Enable, Disable	
Default	Disable	
Description	When set to **Enable**, this parameter generates a default route pointer to this 6611. This route can be exported to other protocols using the protocol default.	
Parameter	Local autonomous system number	
Valid Values	1 to 65534	
Default	None	
Description	This parameter defines the autonomous system number for this 6611.	

Table 5-170. Configuration Worksheet - EGP

Parameter Information		Your Value
Parameter	Enable Exterior Gateway Protocol (EGP)	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the Exterior Gateway Protocol (EGP).	
Parameter	Preference	
Valid Values	0 to 255, 0 being most preferred	
Default Value	200	
Description	This parameter defines the preference value for routes learned by EGP.	
Parameter	Default metric	
Valid Values	0 to 255	
Default Value	1	
Description	This parameter specifies the default metric used when sending out EGP updates.	

Table 5-171 (Page 1 of 2). Configuration Worksheet - EGP Group - Detail

Parameter Information		Your Value
EGP Group List - Parameters configured for each EGP group defined		
Parameter	EGP group name (required for each EGP group defined)	
Valid Values	Any alphanumeric character	
Default Value	The default neighbor group	
Description	This parameter is the user-defined name that is used as an identifier for each EGP neighbor group.	
Parameter	Neighbor autonomous system number	
Valid Values	1 to 65534 an empty string after blanks have been removed	
Default Value	None	
Description	This parameter specifies the autonomous system number of the EGP neighbor group being defined.	
Parameter	Maximum active neighbors	
Valid Values	1 to the maximum number of neighbors (arbitrarily set to 4096 as the maximum number of neighbors)	
Default Value	None	
Description	This parameter sets the maximum number of EGP neighbors in this group kept active at one time.	
EGP Neighbor List - Parameters configured for each EGP neighbor defined		

Table 5-171 (Page 2 of 2). Configuration Worksheet - EGP Group - Detail

Parameter Information	Your Value
Parameter EGP neighbor IP address (required for each EGP neighbor defined) **Valid Values** IP address **Default Value** None **Description** This parameter defines the IP address of a remote 6611 that is defined as an EGP neighbor within this EGP group. This address must be on a directly attached network.	
Parameter Generate default routes from this neighbor **Valid Values** Enable, Disable **Default Value** Enable **Description** This parameter generates default routes from this neighbor.	
Parameter Import default route **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter tells EGP whether or not to import the default route (0.0.0.0) when seen in advertisements from other routers.	
Parameter Export default route **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter tells EGP whether or not to export the default route (0.0.0.0) when making advertisements to other 6611s.	
Parameter Minimum hello interval **Valid Values** 30 to 900 seconds **Default Value** 30 seconds **Description** This parameter defines the minimum time between sending Hello messages to the EGP neighbor defined in this group.	
Parameter Minimum polling interval **Valid Values** 120 to 3600 seconds **Default Value** 120 seconds **Description** This parameter defines the minimum time period elapsed between separate router polls taken of the EGP neighbors in this group; the polls collect routing update information.	
Parameter Default metric **Valid Values** 0 to 255 **Default Value** 1 **Description** This parameter defines the metric for routes sent to the EGP neighbor.	

Table 5-172 (Page 1 of 2). Configuration Worksheet - EGP Group Options

Parameter Information	Your Value
Parameter Preference **Valid Values** 0 to 255, 0 being the most preferred **Default Value** 200 **Description** This parameter defines the preference value for routes learned by an EGP neighbor defined for this EGP group.	
Parameter Default metric **Valid Values** 0 to 255 **Default Value** 1 **Description** This parameter defines the metric for routes sent to the EGP neighbor.	

Table 5-172 (Page 2 of 2). Configuration Worksheet - EGP Group Options

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Generate default from this neighbor group Enable, Disable Enable This parameter is enabled by default. The default is generated from the neighbor group.	
Parameter **Valid Values** **Default Value** **Description**	Import default route Enable, Disable Disable This parameter instructs EGP whether or not to import the default route (0.0.0.0) presented in advertisements from other routers.	
Parameter **Valid Values** **Default Value** **Description**	Export default route Enable, Disable Disable This parameter instructs EGP whether or not to export the default route (0.0.0.0) when presenting advertisements to other routers.	
Parameter **Valid Values** **Default Value** **Description**	Minimum hello interval 30 to 900 seconds The value of the previous Minimum Hello interval parameter This parameter defines the minimum time period elapsed between the sending of Hello packets to this EGP neighbor.	
Parameter **Valid Values** **Default Value** **Description**	Minimum polling interval 120 to 3600 seconds The value of the previous Minimum polling interval parameter This parameter defines the minimum time period elapsed between separate polls taken by this router for this EGP neighbor; polls collect routing update information.	
Parameter **Valid Values** **Default Value** **Description**	Next hop IP address or domain name IP address or domain name None This parameter defines the IP address or domain name of an 6611 on an attached network.	

Table 5-173 (Page 1 of 2). Configuration Worksheet - EGP Import Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable EGP import filters Enable, Disable Disable This parameter enables or disables EGP imports.	
EGP Import Filter List - Parameters configured for each import filter defined		
Parameter **Valid Values** **Default Value** **Description**	Autonomous system number (required for each EGP import filter defined) 1 to 65535 None This parameter specifies the autonomous system to which the import specifications apply.	
Parameter **Valid Values** **Default Value** **Description**	Restrict Enable, Disable Disable This parameter defines the default value for the next Restrict parameter.	

Table 5-173 (Page 2 of 2). Configuration Worksheet - EGP Import Filters

Parameter Information	Your Value
Parameter Preference **Valid Values** 0 to 255 (0 being the most preferred) **Default Value** 200 **Description** This parameter defines the default preference attached to all EGP imported routes.	
EGP Import Destination List - Parameters configured for each destination defined	
Parameter Destination address **Valid Values** Specific, All, Default **Default Value** Specific **Description** This parameter specifies whether to accept imports from a specific address, from all addresses, or from a default address.	
Parameter Destination IP address (required for each EGP import filter defined) **Valid Values** Any IP address **Default Value** None **Description** This parameter defines the IP address of the destination that matches the destination in the EGP imported route.	
Parameter Destination mask **Valid Values** A valid IP address mask **Default Value** 255.255.255.255 **Description** This parameter defines the mask applied to the IP address to define a range of imported IP addresses.	
Parameter Restrict routes **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter determines if the routes defined in the EGP import Destination and Destination mask parameters are restricted from the local route table.	
Parameter Preference **Valid Values** 0 to 255 (0 being most preferred) **Default Value** 200 **Description** This parameter defines the preference attached to EGP imported routes.	

IP Hello Protocol

The Hello protocol is an IP Interior Gateway Protocol. Hello, like RIP, broadcasts its routing information. Instead of using a hop count routing metric like RIP, the Hello protocol uses a network delay routing metric to represent the round-trip delay to the destination network. The metric assigned to the 6611 by the Hello protocol can be a value of 0 to 30000 milliseconds. When 30000 milliseconds is assigned, the destination is considered unattainable. At each router, the Hello protocol algorithm calculates delays for destinations and selects the router with the shortest delay for the pathway.

By default, Hello is disabled. When Hello is enabled, it is sent and received on all IP interfaces.

Restrictions

None

Configuration Changes ...

That Require the Hello Function to Restart

None

That Require the 6611 to Restart

None

Configuration Options

Using the Configuration Program, you will:

1. **Enable Hello and specify global default parameters.**
2. **Optionally specify Hello interface settings.**

   Configure and define each interface on the 6611 to send and receive Hello messages, as required for that interface. These parameters control only outbound traffic on that interface.
3. **Optionally configure Hello source routers.**

   If one or more interfaces of the 6611 are connected to non-broadcast networks (for example, frame relay networks), Hello cannot broadcast response messages on those interfaces. In this case, it is necessary to specifically define the Hello routers to which Hello response messages should be sent.
4. **Optionally configure Hello trusted routers.**

   A trusted router is one whose Hello routes are more reliable than those from other routers on a network. Once a trusted router is defined, Hello messages from all other routers are ignored.
5. **Optionally define Hello import filters.**

   Routes can be exported to Hello from a number of sources including OSPF, OSPFASE, EGP, BGP, and Direct. Import filters regulate which routes are accepted when routes are exported to Hello.

Sample Network Graphic

Figure 5-19 shows two 6611s (6611 A and 6611 B) configured to use Hello to communicate.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and Hello over PPP
  - 2 Ethernet ports running Hello and IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and Hello over PPP
  - 2 token-ring ports running Hello and IP

The following information is shown in Figure 5-19:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

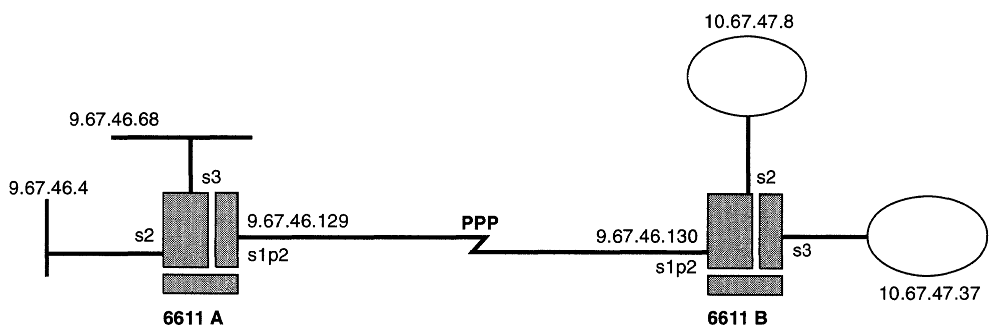


Figure 5-19. Sample Network Using Hello over a PPP Connection

This example shows:

- The configuration of Hello
- Serial, Ethernet, and token-ring ports

The Ethernet segments attached to router 6611 A are running with the subnet mask of 255.255.255.192. The token-ring segments attached to router 6611 B are running with the subnet mask of 255.255.255.224. The PPP link between routers 6611 A and 6611 B is running with the subnet mask of 255.255.255.252.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-19. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Port and Protocols Running on It

Table 5-174. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-175. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56000	56000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-176. Serial Port - PPP Parameters Configured - Port Level

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link quality monitoring protocol	Link quality monitoring protocol

Table 5-177. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.129	9.67.46.130
Subnet mask	255.255.255.252	255.255.255.252
Destination IP address	9.67.46.130	9.67.46.129
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Ports and the Protocols Running on Them

Table 5-178. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 A Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	None	None

Table 5-179. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 A Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.4	9.67.46.68
Subnet mask	255.255.255.192	255.255.255.192
Max. transmission unit (octets)	1492	1492
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table 5-180. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 2 Value	6611 B Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-181. Token-Ring Port - IP Parameters Configured

Parameter	6611 B Slot 2 Value	6611 B Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	10.67.47.8	10.67.47.37
Subnet mask	255.255.255.224	255.255.255.224
Max. transmission unit (octets)	2000	2000
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-182. Node Level - Hello Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Hello protocol	Enable	Enable
Broadcast	Enable	Enable
Route preference	90	90

Table 5-183. Node Level - 6611 A Hello Interface Parameters Configured

Parameter	6611 A Value 1	6611 A Value 2	6611 A Value 3
IP address of local interface	9.67.46.4	9.67.46.68	9.67.46.130
Listen for Hello updates	Enable	Enable	Enable
Send Hello updates	Enable	Enable	Enable

Table 5-184. Node Level - 6611 B Hello Interface Parameters Configured

Parameter	6611 B Value 1	6611 B Value 2	6611 B Value 3
IP address of local interface	9.67.46.129	10.67.47.8	10.67.47.37
Listen for Hello updates	Enable	Enable	Enable
Send Hello updates	Enable	Enable	Enable

Node Level Worksheets

Figure 5-20 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-20.

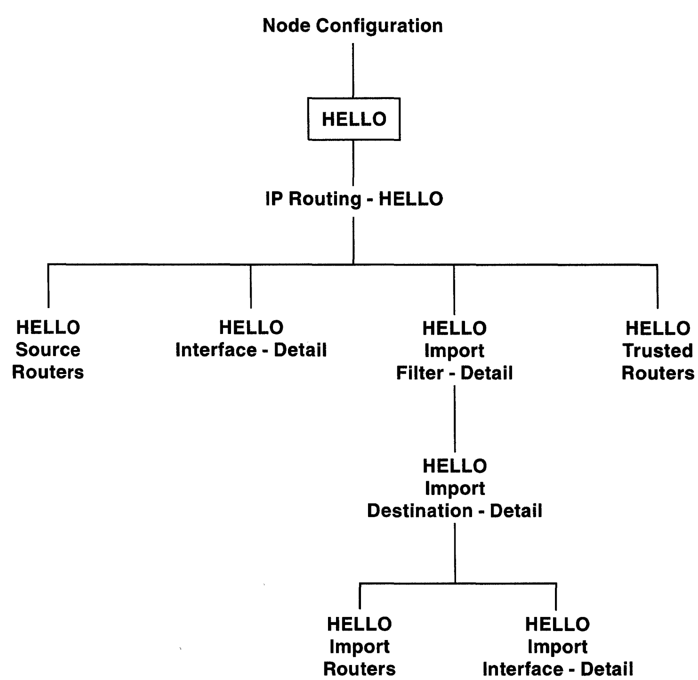


Figure 5-20. Flow of Node Level Hello Help Windows

To enable the adapter to transmit and receive Hello messages, you need to enable IP routing at the port level. Configure IP on each adapter that will transmit and receive IP messages. See “IP Protocol” on page 5-103 for more information. Then configure Hello at the node level.

Use the following tables as worksheets for your node level configurations.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-12 on page D-12 for a mapping of parameter names and their associated labels.

Table 5-185. Configuration Worksheet - IP Routing - Hello

Parameter Information		Your Value
Parameter	Enable Hello protocol	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the Hello protocol on defined IP interfaces.	
Parameter	Broadcast	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	If this parameter is enabled, the Hello messages are broadcast on all Hello-enabled interfaces. If this parameter is disabled (default), the Hello messages are sent exclusively to gateways listed in the source gateways parameter (IP Address of source router).	
Parameter	Route preference	
Valid Values	0 to 255 (0 being the most preferred value)	
Default	90	
Description	This parameter defines the preference value for routes learned by Hello.	

Table 5-186. Configuration Worksheet - Hello Source Routers

Parameter Information		Your Value
Hello Source Router List - Parameter configured for each source router defined		
Parameter	IP address of source router (required for each source router defined)	
Valid Values	IP address or domain name of source router	
Default Value	None	
Description	This parameter specifies the routers to which hello messages are sent. This address must be on a directly attached network.	

Table 5-187. Configuration Worksheet - Hello Trusted Routers

Parameter Information		Your Value
Hello Trusted Router List - Parameter configured for each trusted router defined		
Parameter	IP address of trusted router (required for each trusted router defined)	
Valid Values	A valid IP address or domain name	
Default Value	None	
Description	This parameter specifies a list of routers with valid advertised routes. This address must be on a directly attached network.	

Table 5-188. Configuration Worksheet - Hello Interface - Detail

Parameter Information		Your Value
Hello Interface Settings List - Parameters configured for each interface defined		
Parameter	IP address of local interface	
Valid Values	A valid IP address (For serial links, the IP address will be that of the destination router)	
Default Value	The IP address selected from the list	
Description	This parameter displays in read-only format the IP address of an interface on this 6611.	
Parameter	Listen for Hello updates	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables the acceptance of Hello messages on this interface.	
Parameter	Send Hello updates	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables the sending of Hello messages on the interface.	

Table 5-189 (Page 1 of 2). Configuration Worksheet - Hello Import Filters - Detail

Parameter Information		Your Value
Hello Import Filter List - Parameter configured for each import filter defined		
Parameter	Name of import filter (required for each Hello import filter defined)	
Valid Values	Any alphanumeric string up to 16 characters in length	
Default Value	None	
Description	This parameter is used to internally map a name to each import filter.	
Hello Import Destination List - Parameters configured for each import destination defined		
Parameter	Destination address	
Valid Values	Specific, All, Default	
Default Value	Specific	
Description	This parameter specifies whether the filter operates on a specific destination address, all destination addresses, or default destination addresses.	
Parameter	Destination IP address (required for each Hello import filter defined)	
Valid Values	A valid IP address	
Default Value	None	
Description	This parameter defines the IP address of a destination imported from a received Hello update.	

Table 5-189 (Page 2 of 2). Configuration Worksheet - Hello Import Filters - Detail

Parameter Information	Your Value
Parameter Preference **Valid Values** 0 to 255 (with the lowest value being the most preferred) **Default Value** None **Description** This parameter defines the default preference attached to all Hello routes that are imported with the set of addresses specified by the Destination and Destination Mask parameters.	
Parameter Destination mask **Valid Values** A valid IP mask address **Default Value** 255.255.255.255 **Description** This parameter defines the mask applied to the IP address. This, in turn, defines a range of imported IP addresses.	
Parameter Restrict from routing table **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter determines if the routes defined via the Destination and Destination mask parameters are either restricted or not restricted from being added to the local route table. The default (Disable), ensures that the routes are not restricted.	
Parameter Filter routes from **Valid Values** All sources, Interfaces, Remote routers **Default Value** All sources **Description** This parameter determines whether route imports are applied to local IP interfaces or remote routers.	

Table 5-190. Configuration Worksheet - Hello Import Routers

Parameter Information	Your Value
Hello Import Router List - Parameter configured for each import router defined	
Parameter IP address of remote router (required for each Hello import router defined) **Valid Values** An IP address **Default Value** None **Description** Use this parameter to define an IP address of a remote router used to receive Hello updates. This address must be on a directly attached network.	

Table 5-191. Configuration Worksheet - Hello Import Interface - Detail

Parameter Information	Your Value
Hello Import Interface List - Parameter configured for each import interface defined	
Parameter IP address of local interface (required for each Hello import interface defined) **Valid Values** IP address of local interface **Default Value** None **Description** Use this parameter to define an IP address of any local interface configured for IP.	

IP Open Shortest Path First (OSPF)

OSPF is an Interior Gateway Protocol. It enables users to overcome:

- Some of the limitations of RIP
- The restriction that a route may not define a path through more than 15 routers.

By enabling a network administrator to divide the autonomous system into smaller portions called *areas*, OSPF reduces the size of the *link-state* database each router maintains. This database includes information that describes the status and cost of the links between OSPF routers in an area. By defining areas that consist of small groups of networks, you can also significantly reduce the amount of OSPF traffic passing over individual links.

All OSPF networks contain a backbone area, which is assigned an area identifier of 0.0.0.0. The backbone area is responsible for distributing routing information to the areas attached to it. Normally an OSPF backbone should be contiguous, with all backbone routers attached to one another. If this is not be possible because of network topology, virtual links should be defined to restore backbone continuity.

OSPF routers use messages to establish communication and exchange routing database information. The services of IP are used for delivery.

By default, OSPF is disabled. When OSPF is fully configured and enabled, it is sent and received on all IP interfaces configured to run OSPF.

Restrictions

- Virtual links are defined in the backbone area only. When you define virtual links, the Virtual neighbor ID parameter must have the same value as the Router ID parameter of the destination router to which the virtual link attaches.
- When routes are exported to OSPFASE, it is necessary to specify the Type parameter to define how the metric of the exported route is interpreted. When the Type parameter is set to 2, the metric is interpreted as an OSPF cost greater than that of any OSPF internal routes. When the Type parameter is set to 1, the metric is interpreted as a regular OSPF cost. In order to insure that internal routes are preferred over external routes, type 2 use is recommended.

Configuration Changes...

That Require the OSPF Function to Restart

- Any OSPF changes
- Any EGP changes
- Any BGP changes
- Any RIP changes
- Any Hello changes
- Any static route changes

When one of the above parameters is modified, OSPF will exit nondisruptively, restart and then reacquire route information.

That Require the 6611 to Restart

None

Configuration Options

Using the Configuration Program, you will:

1. **Enable OSPF and define a router identifier for the 6611.**

   The router identifier can be the IP address of any interface on the 6611. It should be stable and must be up when OSPF starts.

2. **Assign an area identifier to the 6611.**

   The backbone must use area identifier 0.0.0.0; other areas conventionally use an identifier that reflects the network or subnetwork number of the area.

   Each area must be defined as transit or stub. Most areas are defined as transit (the backbone *must* be transit); stub areas will be attached to only one other area, which will be the OSPF backbone.

   Choose an authentication scheme to be used for all OSPF message exchanges within the area. All routers within an area must be configured with the same authentication type.

3. **Define each OSPF interface on the 6611 by specifying its IP address and additional parameters.**

   For the following parameters, it is important to assign the same value to all router interfaces in the network:

   - Authorization key (define only if the Authorization type parameter is set to **Simple**)
   - Hello interval
   - Router dead interval

   If the router interface is connected to a non-broadcast network, it is necessary to configure the IP addresses of neighbor routers on the network.

4. **Optionally configure network ranges.**

   Network ranges are defined for area border routers only. They represent the network ranges that are contained within the area and which will be summarized in summary link advertisements to other areas attached to the area border router.

5. **Optionally configure virtual links.**

   Virtual links are used to maintain and ensure that the OSPF backbone remains continuous. A virtual link is a type of point-to-point interface that connects two area border routers that are separated by a non-backbone transit area. Because area border routers are part of the OSPF backbone, the virtual link connects the backbone.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform OSPF routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-192. OSPF Configuration Verification Checklist

OSPF Rule	**Configuration Parameter**	√
The Enable OSPF parameter must be enabled.	Enable OSPF	
All 6611s in the same OSPF area must have the same values for the following parameters: • Area ID • Authorization key • Router dead interval • Hello interval	Area ID	
	Authorization key	
	Router dead interval	
	Hello interval	
The Interface IP address parameter of 6611 A must be included as an IP address of neighbor 6611 on other 6611s with which 6611 A wants to communicate.	Interface IP address	
	IP address of neighbor 6611	
If 6611 A and 6611 B are virtual neighbors, 6611 A's Router ID must be a member of 6611 B's Virtual Neighbor ID list, and vice-versa.	Router ID	
	Virtual neighbor ID	
If 6611 B's Router ID is not included in 6611 A's Virtual Neighbor ID list, verify that this is correct for your configuration. If correct, view 6611 A's list of Virtual Neighbor ID's and verify that: 1. the correct 6611s are displayed in the list 2. that 6611 A's Router ID is defined in 6611 B's Virtual Neighbor ID list.	Router ID	
	Virtual neighbor ID	

Sample Network Graphic One - OSPF Multiarea

Figure 5-21 on page 5-165 shows five 6611s (6611 A, 6611 B, 6611 C, 6611 D, and 6611 E) in a multiarea OSPF configuration that enables IP routing between token-ring and Ethernet subnetworks over a frame relay backbone.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and OSPF over frame relay
  - An Ethernet port running IP and OSPF
  - A token-ring port running IP and OSPF
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and OSPF over frame relay
  - A token-ring port running IP and OSPF
- 6611 D, which has the following port types and protocols running:
  - An Ethernet port running IP and OSPF
  - A token-ring port running IP and OSPF
- 6611 E, which has the following port types and protocols running:
  - 2 token-ring ports running IP and OSPF
  - An Ethernet port running IP and OSPF

The following information is shown in Figure 5-21 on page 5-165:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

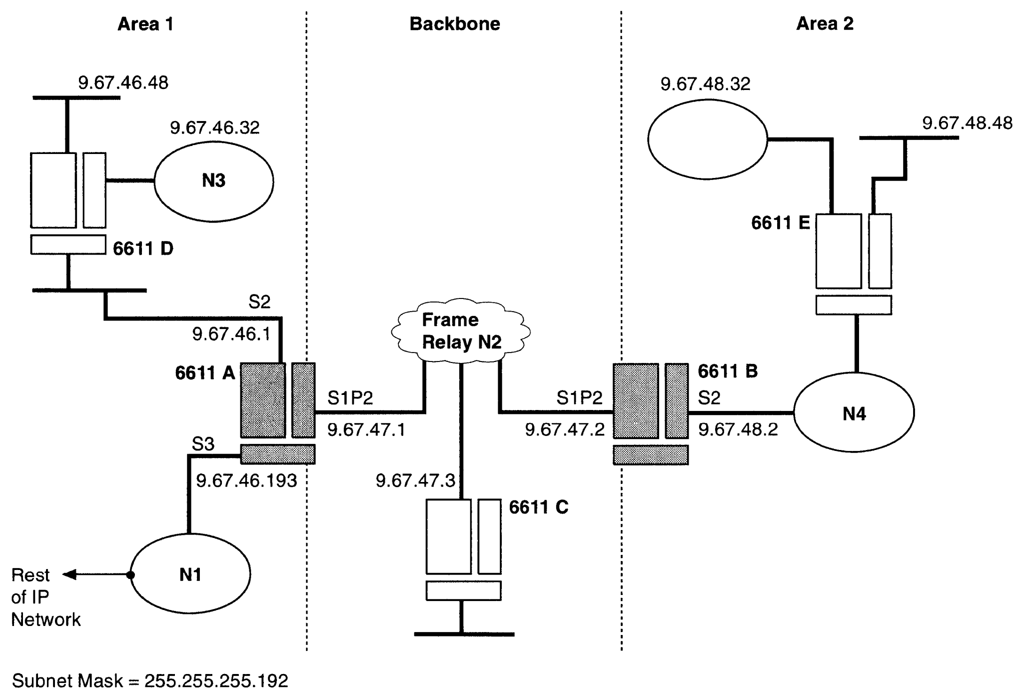


Figure 5-21. Sample Network of an OSPF Multiarea Configuration

This sample network, which is running with a subnet mask of 255.255.255.192, shows:

- The configuration of OSPF with multiple areas
- The use of OSPF stub areas

The configuration consists of five routers. Routers 6611 A, 6611 B, and 6611 C are attached to a frame relay backbone network. Routers 6611 D and 6611 E route traffic from token-ring and Ethernet subnetworks to the primary routers, 6611 A and 6611 B.

All routers run OSPF. Routers 6611 A, 6611 B, and 6611 C are attached to the OSPF backbone, OSPF area 0.0.0.0. Router 6611 A is an area border router that attaches the backbone to area 9.67.46.0; Router 6611 B is an area border router that attaches the backbone to area 9.67.48.0.

All the networks in the configuration are subnetworks of the 9.0.0.0 network.

Summary of All Configured Parameters in Sample One

Use this section as a reference for Figure 5-21. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 5-193. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	Frame Relay	Frame Relay

Table 5-194. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	55855	55855
Data encoding	NRZ	NRZ
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table 5-195. Serial Port - Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Frame Relay on this port	Enable	Enable
Polling interval	10	10
Full inquiry interval	6	6
LMI option	ANSI T1.617 Annex D	ANSI T1.617 Annex D
Use InARP to resolve remote protocol addresses	Enable	Enable
DLCIs assigned to this port	None	None

Table 5-196. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.47.1	9.67.47.2
Subnet mask	255.255.255.192	255.255.255.192
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Disable	Disable
Point-to-point only	Disable	Disable
Assignment for discovered DLCIs	Mesh	Mesh
IP Priority	Disable	Disable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Port and Protocols Running on It

Table 5-197. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	None
Enable additional multicast addresses	Disable
Multicast MAC address	None

Table 5-198. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value
Enable IP routing on this port	Enable
IP address	9.67.46.1
Subnet mask	255.255.255.192
Max. transmission unit (octets)	1500
Ethernet framing for IP	Ethernet V2.0
Enable ICMP address mask requests	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Token-Ring Ports and Protocols Running on Them

Table 5-199. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mpbs
Broadcast type	Non-local	Non-local

Table 5-200. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.193	9.67.48.2
Subnet mask	255.255.255.192	255.255.255.192
Max. transmission unit (octets)	2000	2000
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured - Backbone Area (0.0.0.0)

Table 5-201. Node Level - OSPF Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable OSPF	Enable	Enable
Router ID	9.67.47.1	9.67.47.2

Table 5-202. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 A Value 1	6611 B Value 2
Area ID	0.0.0.0	0.0.0.0
Area type	NA	NA
Stub cost	NA	NA
Authentication type	Simple	Simple

Table 5-203. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 A Value 1	6611 B Value 1
Interface IP address	9.67.47.1	9.67.47.2
Interface type	Non-broadcast	Non-broadcast
Authorization key	Raleigh	Raleigh
Retransmit interval	5	5
Router priority	1	1
Interface transit delay	1	1
Cost	65	65
Router dead interval	40	40
Poll interval	120	120
Hello interval	10	10

Table 5-204. Node Level - OSPF Neighbor Detail Parameters Configured

Parameter	6611 A Value 1	6611 A Value 2	6611 B Value 1	6611 B Value 2
IP address of neighbor router	9.67.47.2	9.67.47.3	9.67.47.1	9.67.47.3
Eligible to become designated router	Enable	Enable	Enable	Enable

Table 5-205. Node Level - Network Ranges Parameters Configured

Parameter	6611 A Value 1	6611 A Value 2	6611 B Value 1	6611 B Value 2
Advertise network range	Enable	Enable	Enable	Enable
Network number	9.67.47.0	9.67.46.0	9.67.47.0	9.67.48.0
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Node-Level Parameters Configured - Area 1 (9.67.46.0)

Table 5-206. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 A Value 2
Area ID	9.67.46.0
Area type	Stub
Stub cost	1
Authentication type	Simple

Table 5-207. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 A Value 1	6611 A Value 2
Interface IP address	9.67.46.1	9.67.46.193
Interface type	Broadcast	Broadcast
Authorization key	Raleigh	Raleigh
Retransmit interval	5	5
Router priority	1	1
Interface transit delay	1	1
Cost	10	25
Router dead interval	40	40
Poll interval	NA	NA
Hello interval	10	10

Table 5-208. Node Level - Network Ranges Parameters Configured

Parameter	6611 A Value 1	6611 A Value 2	6611 B Value 1	6611 B Value 2
Network number	9.67.47.0	9.67.46.0	9.67.47.0	9.67.48.0
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Node-Level Parameters Configured - Area 2 (9.67.48.0)

Table 5-209. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 B Value 2
Area ID	9.67.48.0
Area type	Stub
Stub cost	1
Authentication type	Simple

Table 5-210. Node Level - OSPF Interface Detail Parameters Configured

Parameter	**6611 B Value 2**
Interface IP address	9.67.48.2
Interface type	Broadcast
Authorization key	Raleigh
Retransmit interval	5
Router priority	1
Interface transit delay	1
Cost	25
Router dead interval	40
Poll interval	NA
Hello interval	10

Table 5-211. Node Level - Network Ranges Parameters Configured

Parameter	**6611 A Value 1**	**6611 A Value 2**	**6611 B Value 1**	**6611 B Value 2**
Network number	9.67.47.0	9.67.46.0	9.67.47.0	9.67.48.0
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Sample Network Graphic Two - Virtual Links

Figure 5-22 on page 5-171 illustrates three routers in an OSPF network. In this example, Area 0 is the backbone area (0.0.0.0). Router 6611 C in Area 2 needs to receive routing information from the backbone area (Area 0), but is not directly connected to it. To enable Router 6611 C to receive this information, virtual links are defined between Area 0 and Area 2.

This sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and OSPF over PPP
  - A token-ring port running IP and OSPF
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and OSPF over frame relay
  - A token-ring port running IP and OSPF
- 6611 C, which has the following port types and protocols running:
  - A serial port running IP and OSPF over frame relay
  - A token-ring port running IP and OSPF

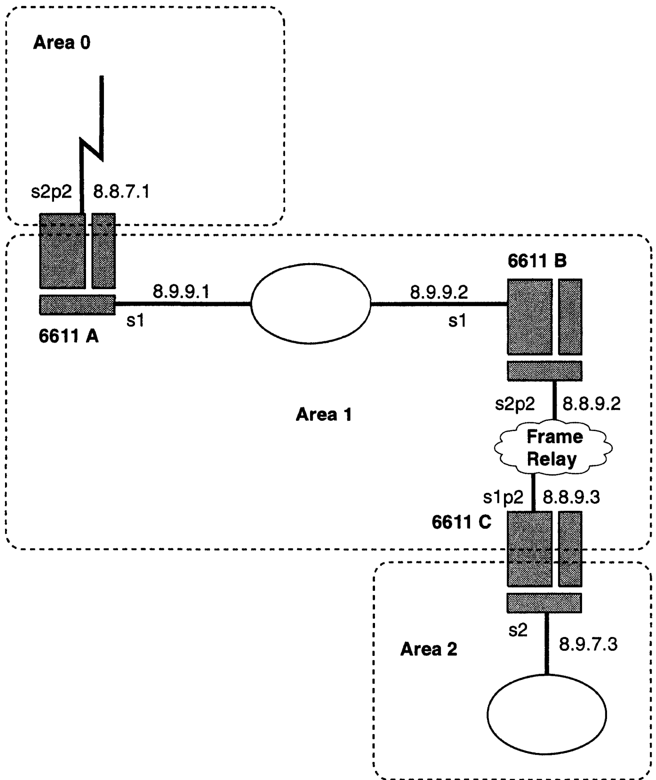


Figure 5-22. Sample Network for OSPF with Virtual Links Defined

The sample network, which is running with a subnet mask of 255.255.255.0, shows:

- The configuration of OSPF
- The configuration of virtual links to connect a noncontiguous segment to the OSPF backbone area

For the purposes of this example, the configured parameters are grouped by OSPF area. To recreate this configuration, you would configure each router rather than each area.

Summary of All Customized Parameters in Sample Two

Use this section as a reference for Figure 5-22. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Area 0 - Serial Port and Protocols Running on It

Table 5-212. Serial Port Parameters Configured

Parameter	6611 A Value Slot 2 Port 2
Data link protocol	PPP

Table 5-213. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Port 2 Value	6611 B Slot 2 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-214. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 2 Port 2 Value	6611 B Slot 2 Port 2 Value
Enable Point-to-Point protocol (PPP) On this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring protocol	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-215. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 2 Port 2 Value
Enable IP routing on this port	Enable
IP address	8.8.7.1
Subnet mask	255.255.255.0
Destination IP address	8.8.7.2
Max. transmission unit (octets)	1500
Enable ICMP address mask requests	Enable
Enable transmission group for IP on this port	Disable
Inbound Port Filters	Disable
IP Priority	Disable
UDP Broadcasts	Disable

Area 1 - Serial Ports and Protocols Running on Them

Table 5-216. Serial Port Parameters Configured

Parameter	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Data link protocol	Frame Relay	Frame Relay

Table 5-217. Serial Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Cylink serial number	None	None
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for Transmission Group	Disable	Disable
Transmission Group name	None	None

Table 5-218. Serial Port - Frame-Relay Parameters Configured

Parameter	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Enable Frame Relay on this port	Enable	Enable
Polling interval	10	10
Full inquiry interval	6	6
LMI option	None	None
Use InARP to resolve remote protocol addresses	Enable	Enable
DLCIs assigned to this port	50	50

Table 5-219. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.9.2	8.8.9.3
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Disable	Disable
Point-to-point only	Enable	Enable
Assignment for discovered DLCIs	NA	NA
IP Priority	Disable	Disable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Area 1 - Token-Ring Ports and Protocols Running on Them

Table 5-220. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Value	6611 B Slot 1 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-221. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 1 Value	6611 B Slot 1 Value
Enable IP routing on this port	Enable	Enable
IP address	8.9.9.1	8.9.9.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Area 2 - Token-Ring Port and Protocols Running on It

Table 5-222. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 C Slot 2 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	NA
MAC address format	NA
Token ring data rate	4 Mbps
Broadcast type	Non-local

Table 5-223. Token-Ring Port - IP Parameters Configured

Parameter	6611 C Slot 2 Value
Enable IP routing on this port	Enable
IP address	8.9.7.3
Subnet mask	255.255.255.0
Max. transmission unit (octets)	1492
Enable ICMP address mask request	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Area 0 - Node-Level Parameters Configured

Table 5-224. Node Level - OSPF Parameters Configured

Parameter	6611 A Value	6611 C Value
Enable OSPF	Enable	Enable
Router ID	8.8.7.1	8.9.7.3

Table 5-225. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 A Value	6611 C Value
Area ID	0.0.0.0	0.0.0.0
Area type	NA	NA
Stub cost	NA	NA
Authentication type	None	None

Table 5-226. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 A Value
Interface IP address	8.8.7.2
Interface type	Point-to-point
Authorization key	NA
Retransmit interval	5
Router priority	1
Interface transit delay	1
Cost	65
Router dead interval	40
Poll interval	120
Hello interval	10

Table 5-227. Node Level - Virtual Link Detail Parameters Configured

Parameter	6611 A Value	6611 C Value
Virtual link ID	Area2	Area2
Retransmit interval	5	5
Virtual neighbor ID	8.9.7.3	8.8.7.1
Interface transit delay	1	1
Transit area ID	0.0.0.1	0.0.0.1
Router dead interval	60	60
Authorization key	NA	NA
Hello interval	10	10

Area 1 - Node-Level Parameters Configured

Table 5-228. Node Level - OSPF Parameters Configured

Parameter	6611 A Value	6611 B Value 1	6611 B Value 2	6611 C Value
Enable OSPF	Enable	Enable	Enable	Enable
Router ID	8.8.7.1	8.8.9.2	8.8.9.2	8.9.7.3

Table 5-229. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 A Value	6611 B Value 1	6611 B Value 2	6611 C Value
Area ID	0.0.0.1	0.0.0.1	0.0.0.1	0.0.0.1
Area type	Transit	Transit	Transit	Transit
Stub cost	NA	NA	NA	NA
Authentication type	None	None	None	None

Table 5-230. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 A Value	6611 B Value 1	6611 B Value 2	6611 C Value
Interface IP address	8.9.9.1	8.9.9.2	8.8.9.2	8.8.9.3
Interface type	Broadcast	Broadcast	Non-broadcast	Non-broadcast
Authorization key	NA	NA	NA	NA
Retransmit interval	5	5	5	5
Router priority	1	1	1	1
Interface transit delay	1	1	1	1
Cost	25	25	65	65
Router dead interval	40	40	40	40
Poll interval	120	120	120	120
Hello interval	10	10	10	10

Table 5-231. Node Level - OSPF Neighbor Detail Parameters Configured

Parameter	6611 B Value	6611 C Value
IP address of neighbor router	8.8.9.3	8.8.9.2
Eligible to become designated router	Enable	Enable

Area 2 - Node-Level Parameters Configured

Table 5-232. Node Level - OSPF Parameters Configured

Parameter	6611 C Value
Enable OSPF	Enable
Router ID	8.9.7.3

Table 5-233. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 C Value
Area ID	0.0.0.2
Area type	Transit
Stub cost	NA
Authentication type	None

Table 5-234. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 C Value
Interface IP address	8.9.7.3
Interface type	Broadcast
Authorization key	NA
Retransmit interval	5
Router priority	1
Interface transit delay	1
Cost	25
Router dead interval	60
Poll interval	120
Hello interval	10

Node Level Worksheets

Figure 5-23 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-23.

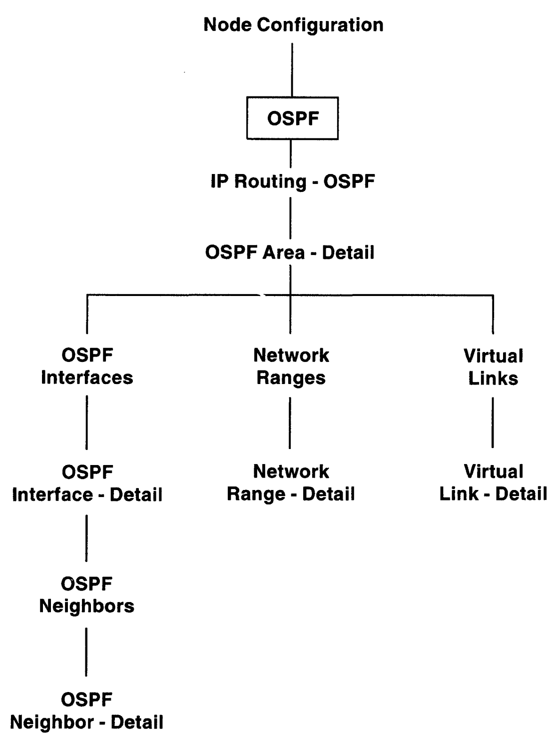


Figure 5-23. Flow of Node Level OSPF Help Windows

To enable the adapter to transmit and receive OSPF packets, you need to enable IP routing at the port level. Configure IP on each adapter that will transmit and receive IP packets (see "IP Protocol" on page 5-103 for more information), then configure OSPF at the node level.

Use the following tables as worksheets for your node level configurations.

- IP Routing - OSPF on page 5-178
- OSPF Interface - Detail on page 5-179
- OSPF Neighbor - Detail on page 5-180
- OSPF Network Ranges on page 5-181
- Virtual Link - Detail on page 5-181

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-17 on page D-15 for a mapping of parameter names and their associated labels.

Table 5-235 (Page 1 of 2). Configuration Worksheet - IP Routing - OSPF

Parameter Information		Your Value
Parameter	Enable OSPF	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables and disables Open Shortest Path First (OSPF).	
Parameter	ASE Route Preference	
Valid Values	0 to 255 with 0 being most preferred.	
Default Value	150	
Description	This parameter defines what the preference will be for Autonomous System External (ASE) routes learned by OSPF. This value is used in determining which route to use when multiple routes exist to the same destination. In such instances, the route with the lowest preference value will be used.	
Parameter	Router ID (required)	
Valid Values	An IP address configured for this 6611	
Default Value	None	
Description	This defined router ID is used by OSPF to uniquely identify the 6611.	
OSPF Area List - Parameters configured for each area defined		
Parameter	Area ID	
Valid Values	0.0.0.0 and 255.255.255.255	
Default Value	0.0.0.0	
Description	Use this parameter to specify the area ID. An area is a group of connected networks, hosts, and specific router interfaces. The backbone area ID must use 0.0.0.0; other areas conventionally use an identifier that reflects the network or subnetwork number of the area.	
Parameter	Area type	
Valid Values	Transit, Stub	
Default Value	Transit	
Description	An area can be a transit area or a stub area (also known as a *nontransit area*). A transit area is an area that is attached to more than one other area and, therefore, can be used for transit traffic (between areas). A stub area will be attached to only one other area, which will be the OSPF backbone.	

Table 5-235 (Page 2 of 2). Configuration Worksheet - IP Routing - OSPF

Parameter Information		Your Value
Parameter	Stub cost	
Valid Values	1 to 65535	
Default Value	None	
Description	This value defines the cost (see hop count) OSPF associates with the default route to its area border router. The cost is used to determine the shortest path for the import default route to its area border router.	
Parameter	Authentication type	
Valid Values	None, Simple	
Default Value	None	
Description	The authentication type for an area defines whether the OSPF protocol packets are authenticated. If the authentication is simple (simple password authentication is used), then a password must be defined for each interface in this area.	

Table 5-236 (Page 1 of 2). Configuration Worksheet - OSPF Interface - Detail

Parameter Information		Your Value
OSPF Interface List - Parameters configured for each interface defined		
Parameter	Interface IP address (required for each OSPF interface defined)	
Valid Values	All configured IP addresses for the 6611 (For serial links, the IP address will be that of the destination router.)	
Default Value	The IP address selected in the list.	
Description	This parameter presents a read-only list of the configured IP addresses of the 6611. (For serial links the destination IP address will be provided in the list).	
Parameter	Interface type	
Valid Values	Broadcast, Non-broadcast	
Default Value	Broadcast	
Description	This parameter specifies the interface as broadcast or non-broadcast media.	
Parameter	Authorization key	
Valid Values	Any 8 characters	
Default Value	None	
Description	This parameter defines the authorization key for this interface.	
Parameter	Retransmit interval	
Valid Values	1 to 3600 seconds	
Default Value	5 seconds	
Description	This parameter defines the frequency of retransmitting link-state update packets, link-state request packets, and database description packets.	
Parameter	Router priority	
Valid Values	0 to 255	
Default Value	1	
Description	This value is used for broadcast and non-broadcast multiaccess networks to elect the designated router.	
Parameter	Interface transit delay	
Valid Values	1 to 3600 seconds	
Default Value	1 second	
Description	Each link-state advertisement has a finite lifetime that is equal to the constant Maximum age parameter. As each link-state advertisement is sent to the particular interfaces, it is aged by this configured delay. The minimum delay is 1 second.	

Table 5-236 (Page 2 of 2). Configuration Worksheet - OSPF Interface - Detail

Parameter Information		Your Value
Parameter	Cost	
Valid Values	1 to 65 535	
Default Value	10**8/interface speed (4M TR = 25, 16M TR = 6, EN = 10, T1 = 65, X.25=1744)	
Description	This parameter defines the cost that OSPF associates with the interface.	
Parameter	Router dead interval	
Valid Values	1 to 65 535 seconds	
Default Value	40 seconds	
Description	When an OSPF Hello message from a neighboring router is not received within the number of seconds allocated in the Router dead interval parameter, the neighbor is declared to be down. This value must be the same as the value of the neighbor or virtual neighbor router's Router dead interval parameter.	
Parameter	Poll interval	
Valid Values	1 to 255 seconds	
Default Value	120 seconds	
Description	This parameter sets the interval in which OSPF packets are sent to a neighbor that is inactive (that is, Hello packets have not been sent by the neighbor during the amount of time allocated by the Router dead interval parameter).	
Parameter	Hello interval	
Valid Values	1 to 255 seconds	
Default Value	10 seconds	
Description	This parameter defines the frequency of sending OSPF Hello packets. This value must be the same as the neighbor or virtual neighbor router's Hello interval.	

Table 5-237. Configuration Worksheet - OSPF Neighbor - Detail

Parameter Information		Your Value
OSPF Neighbor List - Parameters configured for each neighbor defined		
Parameter	IP address of neighbor router (required for each OSPF neighbor defined)	
Valid Values	A valid IP address	
Default Value	None	
Description	This parameter defines the IP address of an OSPF neighbor router on a non-broadcast multiaccess network. This address must be on a directly attached network.	
Parameter	Eligible to become designated router	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables a specific neighbor router, declaring it either eligible (Enable) or ineligible (Disable) to become the designated router. This specific router is defined in the IP address of neighbor router parameter.	

Table 5-238. Configuration Worksheet - OSPF Network Ranges

Parameter Information		Your Value
Network Range - Parameters configured for each network range defined		
Parameter **Valid Values** **Default Value** **Description**	Advertise network range Enable, Disable Enable This parameter defines the status of the network range. When this parameter is enabled, a summary link advertisement will be built and advertised into the other areas. When disabled, a summary link advertisement will not be built. When a summary link advertisement is not built, the existence of those networks included in the network range will be hidden from other areas.	
Parameter **Valid Values** **Default Value** **Description**	Network number (required for each network range defined) A valid IP network address None This parameter specifies the network number for the area border router.	
Parameter **Valid Values** **Default Value** **Description**	Network mask (required for each network range defined) A valid IP network mask 255.255.255.0 This parameter defines the network mask with respect to the network range.	

Table 5-239 (Page 1 of 2). Configuration Worksheet - Virtual Link - Detail

Parameter Information		Your Value
Virtual Link - Parameters configured for each virtual link defined		
Parameter **Valid Values** **Default Value** **Description**	Virtual link name (required for each virtual link defined) Any alphanumeric string 1 to 16 characters in length (the blank string is not valid) None This parameter uniquely identifies this virtual link in the list control.	
Parameter **Valid Values** **Default Value** **Description**	Retransmit interval 1 to 3600 seconds 5 seconds This parameter defines the frequency of retransmitting link-state update packets, link-state request packets, and database description packets.	
Parameter **Valid Values** **Default Value** **Description**	Virtual neighbor ID (required for each virtual link defined) A valid class A, B or C IP address. None This parameter defines the router ID of the virtual neighbor.	
Parameter **Valid Values** **Default Value** **Description**	Interface transit delay 1 to 3600 seconds 1 second Each link-state advertisement has a finite lifetime that is equal to the constant Maximum age parameter. As each link-state advertisement is sent to the particular interfaces, it is aged by this configured delay. The minimum delay is 1 second.	
Parameter **Valid Values** **Default Value** **Description**	Transit area ID (required for each virtual link defined) 0.0.0.1 to 255.255.255.255 None The transit area ID must be one of this area border router's adjacent configured transit areas.	

Table 5-239 (Page 2 of 2). Configuration Worksheet - Virtual Link - Detail

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Router dead interval 1 to 65 535 seconds 60 seconds When an OSPF Hello message from a neighboring router is not received within the number of seconds allocated in the Router dead interval parameter, the neighbor is declared to be down. This value must be the same as the neighbor or virtual neighbor router's router dead interval.	
Parameter **Valid Values** **Default Value** **Description**	Authorization key Any 8 characters None This parameter determines if OSPF protocol packets are authenticated.	
Parameter **Valid Values** **Default Value** **Description**	Hello interval 1 to 255 seconds 10 seconds This parameter defines the frequency of sending OSPF Hello packets. This value must be the same as the neighbor or virtual neighbor router's Hello interval.	

IP Routing Information Protocol (RIP)

RIP is a routing protocol that uses the User Datagram Protocol (UDP) to exchange routing information between routers. RIP uses a metric called a hop count to measure the distance of each RIP route. The hop count is an integer from 0 to 16. A hop count of zero indicates that the destination network is directly attached to the 6611. A hop count of 16 means that the destination network cannot be reached from an 6611. Therefore, a RIP internet cannot have valid routes longer than 15 hops.

The operation of RIP involves the broadcasting of routing information every 30 seconds on each interface that is configured to send RIP information. Other routers in the network that also are running RIP read the broadcasts containing the RIP information and update their route tables according to the information received. This allows for alternate route recovery if links become unavailable.

The MPNP Version 1 Release 2 includes a partial implementation of RIP Version 2 (based on RFC 1388). This implementation supports advertisement of subnets, advertisement of an alternate next hop, and support of multicasting. Subnet mask information makes RIP more useful in a variety of environments and allows the use of variable subnet masks on the network. Support for next hop addresses allows for optimization of routes in an environment which uses multiple routing protocols. Multicast addressing enables network administrators to ensure that the receivers of multicast messages are RIP Version 2 compatible routers.

By default, RIP is disabled. The optional RIP parameters allow the network administrator to tailor IP interfaces on which RIP information should be sent and from which it should be received. The Route metric and Preference parameters control how the RIP routes are used.

Restrictions

When RIP is running with no exports defined to it, there are always two implied exports active: Direct-to-RIP and RIP-to-RIP. If specific exports are defined in the 6611 system configuration, these implied exports are disabled and must be explicitly added into the export routes list.

If Static-to-RIP is exported, therefore, you must also add exports for Direct-to-RIP and RIP-to-RIP. See "Sample Network Graphic" on page 5-184 for an example of RIP exports.

Configuration Changes

That Require the RIP Function to Restart

None

That Require the 6611 to Restart

None

Configuration Options

Using the Configuration Program, you will:

1. **Enable RIP at the node level and and specify global parameters.**
2. **Optionally specify RIP interface settings.**

   Configure and define each interface on the 6611 to send and receive RIP packets, as required for that interface. These parameters control only outbound traffic on that interface.
3. **Optionally configure RIP source routers.**

   If one or more interfaces of the 6611 are connected to non-broadcast networks (for example, frame relay networks), RIP cannot broadcast response packets on those interfaces. In this case, it is necessary to specifically define the RIP routers to which RIP response packets should be sent.
4. **Optionally configure RIP trusted routers.**

   A trusted router is one whose RIP routes are more reliable than those from other routers on a network. After a trusted router is defined, RIP responses from all other routers are ignored.
5. **Optionally define RIP import filters.**

   Routes can be exported to RIP from a number of sources including OSPF, OSPASE, EGP, BGP, and Direct. Import filters regulate which routes are accepted when routes are exported to RIP.

Sample Network Graphic

Figure 5-24 on page 5-185 shows two 6611s (6611 A and 6611 B) configured with RIP to route IP from token-ring and Ethernet subnetworks over an X.25 backbone network.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - An X.25 Adapter running IP and RIP
  - An Ethernet port running IP and RIP
  - A token-ring port running RIP and IP
- 6611 B, which has the following port types and protocols running:
  - An X.25 Adapter running IP and RIP
  - A token-ring port running IP and RIP
- 6611 C, which has the following port types and protocols running:
  - 2 Ethernet ports running IP and RIP
  - A token-ring port running IP and RIP
- 6611 D, which has the following port types and protocols running:
  - An Ethernet port running IP and RIP
  - 2 token-ring ports running IP and RIP

The following information is shown in Figure 5-24 on page 5-185:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

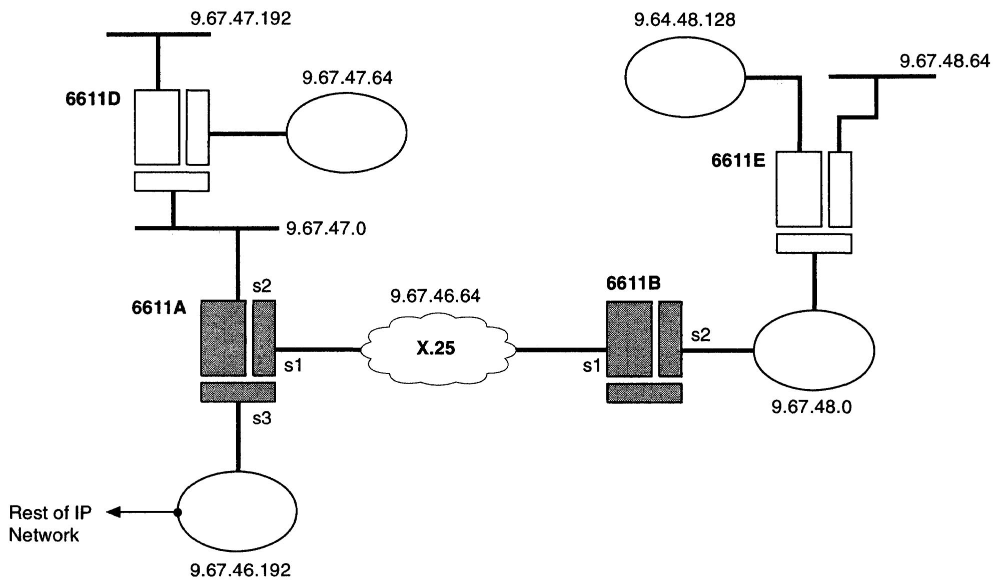


Figure 5-24. Sample X.25 Network Using RIP

This sample network shows:

- The configuration of IP over X.25
- The configuration of RIP
- The use of static routes
- The export of static routes to RIP

All the networks in the configuration are subnetworks on the 9.0.0.0 network with a subnet mask of 255.255.255.192.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-24. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

X.25 Ports and Protocols Running on Them

Table 5-240. X.25 Port Parameters Configured

Parameter	6611 A Slot 1 Value	6611 B Slot 1 Value
Enable X.25 interface on this port	Enable	Enable
Type of line	DTE	DTE
Locally administered MAC address	None	None

Table 5-241. X.25 Port - Subscription Mapping Parameters Configured

Parameter	6611 A Slot 1 Value	6611 B Slot 1 Value
Local DTE address	201002600	201002700
Country code ID	None	None
Network identifier	Other private	Other private
Lowest logical channel number for outgoing SVCs	251	251
Number of logical channels for outgoing SVCs	0	0
Lowest logical channel number for two-way SVCs	10	10
Number of logical channels for two-way SVCs	1	1
Lowest logical channel number for incoming SVCs	1	1
Number of logical channels for incoming SVCs	0	0
Lowest logical channel number for PVCs	1	1
Number of logical channels for PVCs	1	1

Table 5-242. X.25 Port - SVC Options Parameters Configured

Parameter	6611 A Slot 1 Value	6611 B Slot 1 Value
SVC defaults		
Receive packet size	128	128
Transmit packet size	128	128
Receive packet window	7	7
Transmit packet window	7	7
SVC parameters		
Include calling address in call request packets	include	include
Calling address in incoming call packets	*	*
Allow incoming calls	Enable	Enable
Allow outgoing calls	Enable	Enable

Table 5-243. X.25 Port - Facilities Control Parameters Configured

Parameter	6611 A Slot 1 Value	6611 B Slot 1 Value
Packet size negotiation facility	Disable	Disable
Packet window size negotiation facility	Disable	Disable
Packet size and packet window size negotiation	Negotiate	Negotiate
Reverse charging facility	Disable	Disable
Allow reverse charging	Allow	Allow
Closed User Group (CUG) Selection Facility parameters		
Basic format	Disable	Disable
Extended format	Disable	Disable
CUG with OA selection facility - basic format	Disable	Disable
CUG with OA selection facility - extended format	Disable	Disable
Closed user group	1	1

Table 5-244. X.25 Port - IP Parameters Configured

Parameter	6611 A Slot 1 Value	6611 B Slot 1 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.65	9.67.46.66
Subnet mask	255.255.255.192	255.255.255.192
Max. transmission unit (octets)	576	576
Enable ICMP address mask requests	Enable	Enable

Table 5-245. X.25 Port - X.25 Remote Host Detail Parameters Configured

Parameter	6611 A Slot 1 Value	6611 B Slot 1 Value
Destination IP address for X.25	9.67.46.66	9.67.46.65
Virtual circuit type	SVC	SVC
Remote DTE address	201002700	201002600
Logical channel number	NA	NA

Ethernet Port and Protocols Running on It

Table 5-246. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	None
Enable additional multicast addresses	Disable
Multicast MAC address	None

Table 5-247. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value
Enable IP routing on this port	Enable
IP address	9.67.47.1
Subnet mask	255.255.255.192
Max. transmission unit (octets)	1492
Ethernet framing for IP	Ethernet V2.0
Enable ICMP address mask requests	Enable
Directed broadcast	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Token-Ring Ports and Protocols Running on Them

Table 5-248. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-249. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.193	9.67.48.2
Subnet mask	255.255.255.192	255.255.255.192
Max. transmission unit (octets)	2000	2000
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-250. Node Level - RIP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 2 Value
Enable Routing Information Protocol (RIP)	Enable	Enable
Broadcast	Disable	Disable
Zero reserved fields	Enable	Enable
Route preference	100	100

Table 5-251. Node Level - RIP Source Routers Configured

Parameter	6611 A Value	6611 A Value	6611 A Value	6611 B Value	6611 B Value
IP address of source router	9.67.46.66	9.67.46.236	9.67.47.4	9.67.46.65	9.67.48.5

Table 5-252. Node Level - Static Route Detail Parameters Configured

Parameter	6611 A Value	6611 A Value	6611 A Value	6611 A Value
Destination IP address	Specific	Specific	Specific	Specific
Destination address	9.67.38.0	9.67.38.64	9.67.38.128	9.67.38.192
Destination mask	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192
Next hop router number 1	9.67.46.195	9.67.46.195	9.67.46.195	9.67.46.195
Next hop router number 2	None	None	None	None
Next hop router number 3	None	None	None	None
Preference	50	50	50	50
Retain route in master table	Disable	Disable	Disable	Disable

Table 5-253. Node Level - Export Filter Parameters Configured

Parameter	6611 A Filter 1 Value
From protocol	
From protocol	Static
AS number	NA
Origin	NA
AS path specification	NA
To protocol	
To protocol	RIP
AS number	NA
Tag	NA
Type	NA
Routes to be exported	
Route(s) to be exported	All
Restrict export	Disable
Metric	1
Specific route	NA
Mask	NA

Table 5-254. Node Level - IP Routing - IP over X.25 Parameter Configured

Parameter	6611 A Value	6611 B Value
Connection decay interval	10	10

Node Level Worksheets

Figure 5-25 on page 5-190 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-25 on page 5-190.

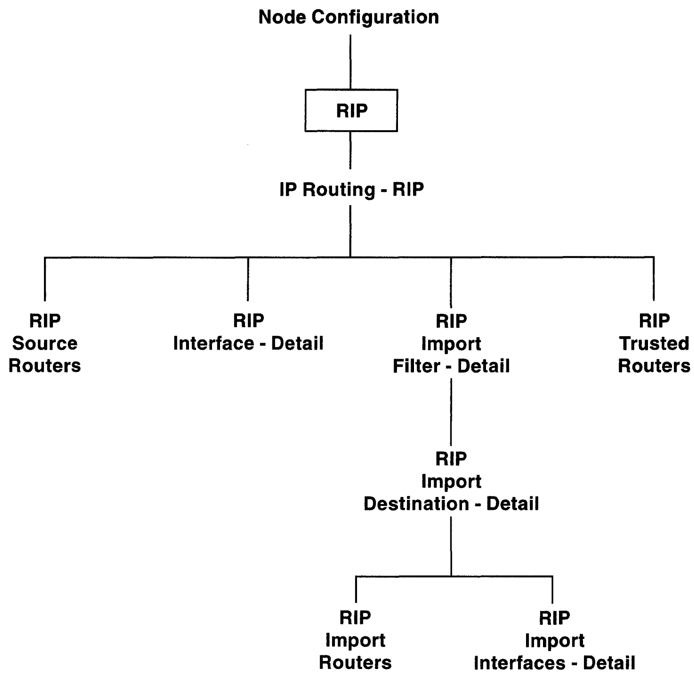


Figure 5-25. Flow of Node Level RIP Help Windows

To enable the adapter to transmit and receive RIP packets, you need to enable IP routing at the port level. Configure IP on each adapter that will transmit and receive IP packets. See "IP Protocol" on page 5-103 for more information. Then configure RIP at the node level.

Use the following tables as worksheets for your port level configurations.

- IP Routing - RIP on page 5-190
- RIP Source Routers on page 5-191
- RIP Trusted Routers on page 5-191
- RIP Interface - Detail on page 5-191
- RIP Import Filter - Detail on page 5-192
- RIP Import Destination - Detail on page 5-193
- RIP Import Routers on page 5-193
- RIP Import Interfaces - Detail on page 5-194

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-18 on page D-16 for a mapping of parameter names and their associated labels.

Table 5-255 (Page 1 of 2). Configuration Worksheet - IP Routing - RIP

Parameter Information		Your Value
Parameter	Enable Routing Information Protocol (RIP)	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the use of the Routing Information Protocol (RIP) on the defined interfaces.	

Table 5-255 (Page 2 of 2). Configuration Worksheet - IP Routing - RIP

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Broadcast Enable, Disable Enable When enabled, this parameter ensures that RIP packets are broadcast on all RIP enabled interfaces. When this parameter is disabled, the RIP packets are sent to routers defined in the source routers list in the IP address of source router parameter.	
Parameter **Valid Values** **Default Value** **Description**	Zero reserved fields Enable, Disable Enable When enabled, this parameter ensures that RIP verifies that the unused fields in RIP packets are zero. When this parameter is disabled, the zeroing of reserved fields is suppressed.	
Parameter **Valid Values** **Default Value** **Description**	Route preference 0 to 255 (0 being most preferred) 100 This parameter identifies the preference value for routes learned by RIP.	

Table 5-256. Configuration Worksheet - RIP Source Routers

Parameter Information		Your Value
RIP Source Router List - Parameters configured for each source router configured		
Parameter **Valid Values** **Default Value** **Description**	IP address of source router A valid IP address None This parameter specifies that the routers on this list are sent RIP messages. This address must be on a directly attached network.	

Table 5-257. Configuration Worksheet - RIP Trusted Routers

Parameter Information		Your Value
RIP Trusted Router List - Parameters configured for each trusted router configured		
Parameter **Valid Values** **Default Value** **Description**	IP address of trusted router A valid IP address None This parameter specifies routers from which advertised routes will be "trusted" or learned and used for IP datagram routing. This address must be on a directly attached network.	

Table 5-258 (Page 1 of 2). Configuration Worksheet - RIP Interface - Detail

Parameter Information		Your Value
RIP Interface Settings List - Parameters configured for each interface defined		
Parameter **Valid Values** **Default** **Description**	Local IP interface Specific, All Specific This parameter specifies whether to send and receive RIP packets on a specific interface or on all interfaces configured for RIP.	

Table 5-258 (Page 2 of 2). Configuration Worksheet - RIP Interface - Detail

Parameter Information		Your Value
Parameter	IP address of local interface (required for each RIP interface defined)	
Valid Values	An IP address	
Default Value	An IP address selected from the list	
Description	This parameter displays, in read-only format, the Internet Protocol (IP) address of an interface on this router that was selected from a list displayed by the program.	
Parameter	Version	
Valid Values	Version 1, Version 2	
Default Value	Version 1	
Description	This parameter specifies the RIP version as either version 1 or version 2.	
Parameter	Broadcast mode	
Valid Values	Broadcast or Multicast	
Default Value	Broadcast	
Description	This parameter specifies the broadcast mode RIP Version 2 uses. Multicasting should be selected in order to reduce unnecessary load on those hosts which are not listening to RIP Version 2 packets. This would prevent RIP Version 1 systems from receiving RIP Version 2 updates. The default value of Broadcast would send the RIP Version 2 packets to all.	
Parameter	Metric in	
Valid Values	1 to 16	
Default Value	1	
Description	The default value of 1 represents the normal situation in which a value of 1 is added to the route metric when a new route is learned over this interface. By overriding this default metric, a network administrator can assign a higher value to the metric and thereby control the selection of routes by making this RIP route less attractive.	
Parameter	Metric out	
Valid Values	0 to 16	
Default Value	0	
Description	The default value of 0 represents the normal situation in which a value of 0 is added to the route metric when a route is announced over this interface. By overriding this default metric, a network administrator can assign a higher value to the outgoing RIP route metric to make the route less attractive.	
Parameter	Listen for RIP updates	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter determines if RIP messages are accepted on the interface.	
Parameter	Send RIP updates	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter determines if RIP messages are sent on the interface.	

Table 5-259. Configuration Worksheet - RIP Import Filter - Detail

Parameter Information		Your Value
RIP Import List - Parameters configured for each import filter defined		
Parameter	Name of import filter (required for each RIP import filter defined)	
Valid Values	Any alphanumeric string up to 16 characters	
Default	None	
Description	This parameter defines a name for each RIP import filter.	

Table 5-260. Configuration Worksheet - RIP Import Destination - Detail

Parameter Information	Your Value
RIP Import Destination List - Parameters configured for each import filter destination defined	
Parameter Destination address **Valid Values** Specific, All, Default **Default** Specific **Description** This parameter specifies whether the filter operates on a specific destination address, all destination addresses, or default destination addresses.	
Parameter Destination IP address (required for each RIP import destination defined) **Valid Values** A valid IP address **Default** None **Description** This parameter specifies the destination IP address for this RIP import filter.	
Parameter Preference **Valid Values** 0 to 255 **Default** 100 **Description** This parameter defines the route preference attached to the defined RIP import filter.	
Parameter Destination mask **Valid Values** A valid subnet mask **Default** 255.255.255.255 **Description** The mask defined in this parameter is applied to the IP address that determines the range of IP addresses import filters.	
Parameter Restrict from routing table **Valid Values** Enable, Disable **Default** Disable **Description** Enabling this parameter restricts routes defined through the Destination and Destination mask parameters from being added to the routing table.	
Parameter Filter routers from **Valid Values** All sources, Remote router, Interface **Default** All sources **Description** This parameter determines whether route imports are applied to routes learned from all sources, particular local IP interfaces, or particular remote routers.	

Table 5-261. Configuration Worksheet - RIP Import Routers

Parameter Information	Your Value
RIP Import Router List - Parameters configured for each import router defined	
Parameter IP address of remote router (required for each RIP import router defined) **Valid Values** A valid IP address **Default** None **Description** This parameter defines the IP address of a remote router used to receive RIP updates. This address must be on a directly attached network.	

Table 5-262. Configuration Worksheet - RIP Import Interfaces - Detail

Parameter Information		Your Value
RIP Import Interface List - Parameters configured for each import interface defined		
Parameter	IP address of local interface (required for each RIP import interface defined)	
Valid Values	A valid IP address	
Default	None	
Description	This parameter defines the IP address of a local interface configured for IP.	

IP Static Routes

The purpose of defining static routes is to define a communication path between networks that the network administrators believe to be commonly used and operational.

A static route is defined by a pair of IP addresses. One address is the address of a router on a network that is attached to this 6611. Sometimes this address is referred to as the *next hop*. The 6611 allows you to define three next hop routers. When more than one next hop router is defined, the route is an equal cost multipath route. This means that traffic will be distributed across multiple paths (next hops 1-3). When a path is unavailable (because the associated interface has gone down), the traffic will be distributed across the other defined paths. When the associated interface of a next hop does not go down, there is no way of determining that a path has gone away, therefore, the other paths will not be used to pick up the traffic from the failing path. When the next hop is no longer available and the associated interface is still up, there is no way for the 6611 to determine that the path is unavailable (for example, the next hop router has gone down), therefore, the traffic will still be distributed across all defined paths. This is an inherent limitation of static routes and the only solution is to fix the problem or re-configure the static route omitting the unavailable next hop. The other IP address in the pair is the destination address of the route. This address identifies either a network or host. A network address can be easily recognized because the host value is zero.

After a static route is defined, it is automatically added to the route table of the 6611.

Restrictions

The 6611 maintains only one route to a destination per protocol per autonomous system. When there are multiple protocols with routes to the same destination, the route provided by the protocol with the lowest route preference is selected. If the route preferences are equal, then the route with the lowest autonomous system number is selected. If the autonomous systems are equal, then the route with the lowest numeric next-hop gateway is selected.

Configuration Changes

That Require the IP Function to Restart

None

That Require the 6611 to Restart

None

Configuration Options

Using the Configuration Program, you will:

- **Enable Static Routes at the node level.**
- **Specify the following parameters for each static route defined.:**
  - Destination IP address
  - Destination address
  - Next hop router number 1 (IP address)

- Preference

Sample Network Graphic

Figure 5-26 shows two 6611s (6611 A and 6611 B) with static routes configured.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP over PPP
  - A token-ring port running IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP over PPP
  - A token-ring ports running IP

The following information is shown in Figure 5-26:

- IP addresses
- Slot and port numbers, abbreviated *sx* p*y*

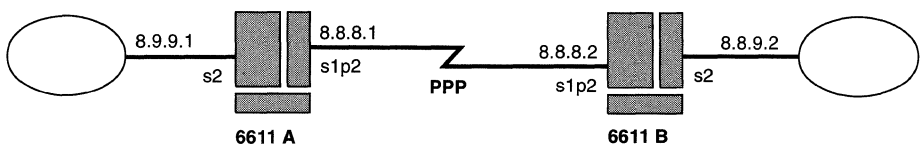


Figure 5-26. Sample Network for Static Routes

This sample network, which is running with the subnet mask of 255.255.255.0, shows the configuration for:

- Static routes
- Serial and token-ring ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-26. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Port and Protocols Running On It

Table 5-263. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-264. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-265. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-266. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	NA	NA
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Port and Protocols Running On It

Table 5-267. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-268. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.9.9.1	8.8.9.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-269. Node Level - Static Routes Parameters Configured

Parameter	6611 A Value	6611 B Value
Destination IP address	Specific	Specific
Destination address	8.8.9.0	8.9.9.0
Destination mask	255.255.255.0	255.255.255.0
Next hop router #1	8.8.8.2	8.8.8.1
Next hop router #2	None	None
Next hop router #3	None	None
Preference	50	50
Retain route in master table	Disable	Disable

Node Level Worksheets

Figure 5-27 on page 5-199 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-27 on page 5-199.

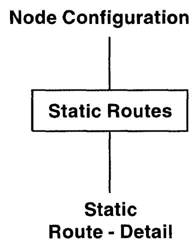


Figure 5-27. Flow of Node Level Static Routes Help Windows

Use the following table as a worksheet for your node level configurations.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter.

Table 5-270 (Page 1 of 2). Configuration Worksheet - Static Route - Detail

Parameter Information	**Your Value**
IP Static Routes List - Parameters configured for each static route defined	
Parameter Destination IP address **Valid Values** Specific, Default **Default Value** Specific **Description** This parameter determines how the 6611 learns the IP address of the destination for the static route.	
Parameter Destination address (required) **Valid Values** Any valid IP address **Default Value** None **Description** This parameter defines the destination, either a network or a host, for this static route. When this parameter specifies a host address abd tge Destination mask paramter is *not* set to **255.255.255.255.** (default), the value of this parameter must be 0.	
Parameter Destination mask **Valid Values** 0.0.0.0 to 255.255.255.255 **Default Value** 255.255.255.255 **Description** This parameter defines the destination network (host part all zeros) or a destination host for this static route.	
Parameter Next hop router number 1 (IP address) (required) **Valid Values** An IP address **Default Value** None **Description** This parameter defines the IP address of a 6611 on an attached network that is the next hop (next destination router) for packets received at this 6611. This address must be on a directly attached network. This field is an exception to the restriction of loopback addresses (IP addresses which begins with 127 in the first octet). The IP address of 127.0.0.1 is valid here.	
Parameter Next hop router number 2 (IP address) **Valid Values** An IP address **Default Value** None **Description** This parameter defines the IP address of a 6611 on an attached network that is the next hop (next destination router) for packets received at this 6611. This address must be on a directly attached network. This field is an exception to the restriction of loopback addresses (IP addresses which begins with 127 in the first octet). The IP address of 127.0.0.1 is valid here.	

Table 5-270 (Page 2 of 2). Configuration Worksheet - Static Route - Detail

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Next hop router number 3 (IP address) An IP address None This parameter defines the IP address of a 6611 on an attached network that is the next hop (next destination router) for packets received at this 6611. This address must be on a directly attached network. This field is an exception to the restriction of loopback addresses (IP addresses which begins with 127 in the first octet). The IP address of 127.0.0.1 is valid here.	
Parameter **Valid Values** **Default Value** **Description**	Preference 0 to 255 50 This parameter defines the route preference for this static route.	
Parameter **Valid Values** **Default Value** **Description**	Retain route in master table Enable, Disable Disable By enabling this parameter, you ensure that the static route is retained in the system master routing table when the routing process is shut down.	

IP Export Filters

When combinations of routing protocols are used on the 6611, it is necessary to use export filters to pass routes learned by one protocol to another. For example, you would enable export filters to:

- Export a static route to any protocol
- Pass route information between an OSPF backbone and RIP subnetworks
- Pass route information between interior and exterior gateway protocols
- Export a default route, generated by EGP or BGP, to an interior gateway protocol at an autonomous system boundary router

Exporting To and From RIP

See "Sample Network Graphic" on page 5-184 for an example.

Exporting To and From OSPF

Any routes that are exported to OSPF are imported as OSPF autonomous system external routes (OSPFASE) and advertised into the OSPF network using autonomous system external link state advertisements.

When routes are exported to OSPFASE, it is necessary to specify the Type parameter to determine how the metric of the exported route is interpreted. When the Type parameter is set to 2, the metric is interpreted as an OSPF cost greater than that of any OSPF internal routes. When the Type parameter is set to 1, the metric is interpreted as a regular OSPF cost. To ensure OSPF internal routes are preferred over external routes, type 2 use is recommended.

Exporting from OSPF is relatively straightforward. It may be necessary to export both OSPF and OSPFASE when, for example, static routes have been exported to other routers in the network. This is because these routes are advertised as OSPFASE routes throughout the entire autonomous system utilizing OSPF as an Interior Gateway Protocol (IGP).

Exporting To and From EGP

When routes are exported to or from EGP, it is necessary to define the autonomous system number to or from which the routes are being exported.

For example, to configure an autonomous system boundary router running OSPF in the local autonomous system and using EGP to attach to AS 1002, it would be necessary to:

- Export from EGP 1002 to OSPFASE
- Export from OSPF and OSPFASE to EGP 1002

The correct autonomous system number must be specified for the export to be successful.

When EGP is being used without exports, the direct-to-EGP export is implied. However, if any exports are specified explicitly, the direct-to-EGP export must be specified explicitly.

See "Sample Network Graphic" on page 5-142 for an example of an EGP export.

Exporting To and From BGP

The rules for exporting to and from BGP are similar to those for EGP. AS_Path provides additional options for exporting from BGP. Export from AS_Path allows you to specify the type of route to export to an Interior Gateway Protocol. Options of ANY, IGP, EGP, and Incomplete are available. When BGP is being used without exports, the direct-to-BGP export is implied. However, if any exports are specified explicitly, the direct-to-BGP export must be specified explicitly.

See "Sample Network Graphic" on page 5-127 for an example of an BGP export.

Exporting Default

When you export routes, default refers to the default that is generated by EGP or BGP if the Generate default routes parameter is enabled.

Export default cannot be used to export an inter-autonomous system default route without EGP or BGP being configured. To export an inter-autonomous system route without configuring EGP or BGP, export static route (0.0.0.0) to the Interior Gateway Protocol within the AS.

Default should be exported to the Interior Gateway Protocol (RIP or OSPFASE) that is running within the AS. It will become advertised only when EGP communications are established with a neighbor that is configured to generate a default route.

See "Sample Network Graphic" on page 5-127 and "Sample Network Graphic" on page 5-142 for examples of default exports.

Exporting Direct

Direct refers to routes that are established through locally attached interfaces. Enable exporting of direct routes when you want the 6611 to share the information about direct routes. For example, if you wanted routers in your OSPF network to advertise networks that are attached to interfaces running RIP, you would export RIP and Direct to OSPF and OSPFASE.

Understanding Import Filters

When export filters are defined on multiple 6611s in your network, it may become advantageous to restrict the sources from which routes are accepted. Import filters regulate which routes the protocol learns/accepts. Import filters take effect both when learning routes from other routers and when exporting from one protocol to another.

Import filters are defined for the following protocols:

- BGP
- EGP
- Hello
- RIP

Import filters deny route imports on the basis of destination IP address, thus enabling you to control the source of the routes imported for each of these IP protocols. For the RIP and Hello protocols, you can also further qualify import applicability by specifying interfaces or specific gateways. For the EGP and BGP protocols, import filter applicability must be qualified with respect to the Autonomous System (AS) of the EGP neighbor or EGP peer supplying the routes.

You might want to use import filters to prevent the import of routes from certain interfaces or certain routers in order to:

- Prevent the sharing of routes for security reasons
- Limit network traffic across certain links
- Control the size of the route table

Restrictions

None

Configuration Changes ...

That Require the Export Filters Function to Restart

None

That Require the 6611 to Restart

None

Sample Network Graphic

Figure 5-28 on page 5-204 shows three 6611s (6611 A, 6611 B, and 6611 C). 6611 A is running OSPF; 6611 B is running OSPF on the serial interface and RIP on the Ethernet interface; 6611 C is running RIP.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and OSPF over frame relay
  - A token-ring port running IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and OSPF over frame relay
  - An Ethernet port running IP and RIP
- 6611 C, which has the following port types and protocols running:
  - An Ethernet port running IP and RIP
  - A token-ring port running IP

The following information is shown in Figure 5-28 on page 5-204:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

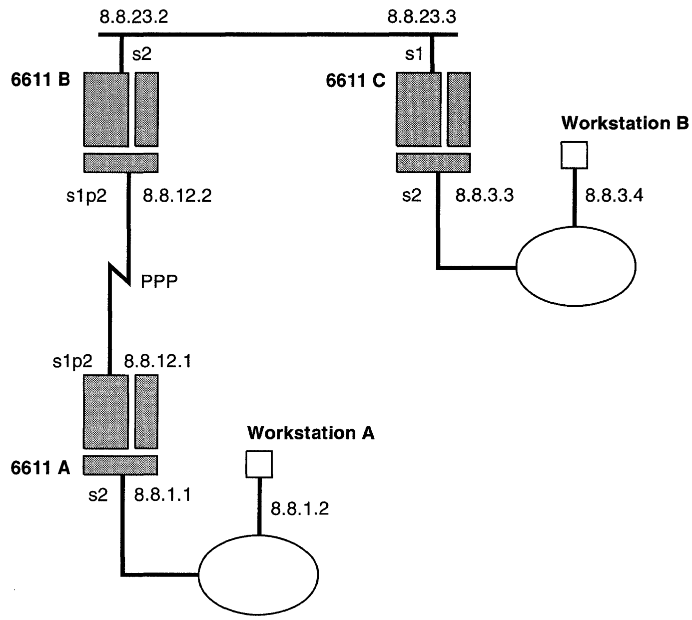


Figure 5-28. Sample Network Using Export Filters

The sample network running IP with a subnet mask of 255.255.255.0 shows:

- The configuration of RIP
- The configuration of OSPF
- Export filters between RIP and OSPF

Export filters are configured on router 6611 to enable workstation A, which is attached to a token-ring segment running OSPF, to communicate with workstation B, which is attached to a token-ring segment running RIP.

Summary of All Configured Parameters in Sample

Use this section as a reference for Figure 5-28. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 5-271. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-272. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-273. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-274. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.12.1	8.8.12.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.12.2	8.8.12.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and Protocols Running on Them

Table 5-275. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 C Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-276. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 C Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.1.1	8.8.3.3
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Ports and Protocols Running on Them

Table 5-277. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 2 Value	6611 C Slot 1 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	None	None
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	None	None

Table 5-278. Ethernet Port - IP Parameters Configured

Parameter	6611 B Slot 2 Value	6611 C Slot 1 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.23.2	8.8.23.3
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-279. Node Level - OSPF Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable OSPF	Enable	Enable
Router ID	8.8.1.1	8.8.12.2

Table 5-280. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 A Value	6611 B Value
Area ID	0.0.0.0	0.0.0.0
Area type	NA	NA
Stub cost	NA	NA
Authentication type	None	None

Table 5-281. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 A Value 1	6611 A Value 2	6611 B Value
Interface IP address	8.8.1.1	8.8.12.2	8.8.12.1
Interface type	Broadcast	Point-to-point	Point-to-point
Authorization key	NA	NA	NA
Retransmit interval	5	5	5
Router priority	1	1	1
Interface transit delay	1	1	1
Cost	25	65	65
Router dead interval	40	40	40
Poll interval	NA	NA	NA
Hello interval	10	10	10

Table 5-282. Node Level - RIP Parameters Configured

Parameter	6611 B Value	6611 C Value
Enable Routing Information Protocol (RIP)	Enable	Enable
Broadcast	Enable	Enable
Zero reserved fields	Enable	Enable
Route preference	100	100

Table 5-283. Node Level - RIP Interface Detail Parameters Configured

Parameter	6611 B Value
Local IP address interface	Specific
IP address of local interface	8.8.12.1
RIP interface settings	
Version	Version 2
Broadcast mode	Broadcast
Metric in	1
Metric out	0
Listen for RIP updates	Disable
Send RIP updates	Disable

Table 5-284. Node Level - Export Filter Parameters Configured

Parameter	6611 B Filter 1 Value	6611 B Filter 2 Value	6611 B Filter 3 Value	6611 B Filter 4 Value
From protocol				
From protocol	RIP	OSPF	OSPFASE	DIRECT
AS number	NA	NA	NA	NA
Origin	NA	NA	NA	NA
AS path specification	NA	NA	NA	NA
To protocol				
To protocol	OSPFASE	RIP	RIP	OSPFASE
AS number	NA	NA	NA	NA
Tag	1	NA	NA	1
Type	1	NA	NA	1
Routes to be exported				
Route(s) to be exported	All	All	All	All
Restrict export	Disable	Disable	Disable	Disable
Metric	1	1	1	1
Specific Route	NA	NA	NA	NA
Mask	NA	NA	NA	NA

Node Level Worksheet

Figure 5-29 on page 5-209 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-29 on page 5-209.

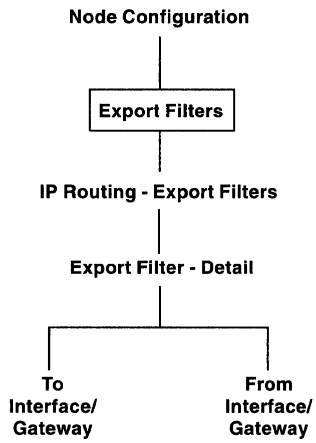


Figure 5-29. Flow of Node Level Export Filters Help Windows

Use the following table as a worksheet for your node level configurations.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-11 on page D-11 for a mapping of parameter names and their associated labels.

Table 5-285 (Page 1 of 3). Configuration Worksheet - Export Filter - Detail

Parameter Information	Your Value
Export Filter List - Parameters configured for each filter configured	
From protocol	
Parameter From protocol **Valid Values** RIP, OSPF, OSPFASE, Static, Direct, EGP, BGP, EGP/BGP Default, AS PATH and Hello **Default Value** None **Description** This parameter specifies the protocol to export from (source); the export source protocol. **Note**: You can export only one protocol to another protocol.	
Parameter AS number **Valid Values** 1 to 65536 **Default Value** None **Description** This parameter specifies that routes from this autonomous system learned by EGP or BGP should be exported to the To protocol parameter.	

Table 5-285 (Page 2 of 3). Configuration Worksheet - Export Filter - Detail

<table>
<tr><th colspan="2">Parameter Information</th><th>Your Value</th></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Origin
IGP, EGP, Incomplete, Any
Any
This parameter defines the origin of the path information you specified for the Autonomous system path specification parameter. In other words, the autonomous system path origin indicates how a particular route was injected into Border Gateway Protocol. This could have occurred by means of the Exterior Gateway Protocol (EGP), an Interior Gateway Protocol (IGP), or some other means.
• If IGP is selected, BGP will import destinations that were learned by BGP from an IGP, such as OSPF.
• If EGP is selected, BGP will import destinations that were learned by BGP from EGP.
• If Incomplete is selected, BGP will import destinations that were learned by BGP by some other means (for example, from static route information).
• If Any is selected, BGP will import destinations that were learned by BGP from any of the above three origins.</td><td></td></tr>
<tr><td>Parameter
Valid Values

Default Value
Description</td><td>Autonomous system path specification
From 1 to 80 integers and notational shorthand symbols as detailed in the description of this parameter.
None
This parameter is used to identify one or more autonomous system paths.</td><td></td></tr>
<tr><td colspan="3">To protocol</td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>To protocol
RIP, OSPFASE, EGP, BGP and Hello
None
This parameter specifies the protocol to export to; the target protocol.
Note: You can export only one protocol to another protocol.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>AS number
1 to 65536
None
This parameter specifies the autonomous system number to add to the exported route.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Tag
1 to 65534
None
This parameter is a user defined tag associated with a route to be considered for export. If no tag value is specified, routes with any tag are considered. This parameter becomes an option if you selected OSPFASE as the value for the To protocol.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Type
1, 2
1
When routes are exported to OSPFASE it is necessary to specify additional parameters to define how the external route will be advertised into the OSPF network. One of these parameters deals with the costs associated with OSPF external routes. If the Type field value is set to 1, the external routes will compete equally with the internal ones. If this value is set to 2, the external routes will have an extra penalty so that the internal routes are preferred.</td><td></td></tr>
</table>

Table 5-285 (Page 3 of 3). Configuration Worksheet - Export Filter - Detail

Parameter Information	Your Value
Routes to be exported	
Parameter Route(s) to be exported **Valid Values** Specific, All, Default (0.0.0.0) **Default Value** Specific **Description** Use this parameter to define whether the filter operates on a specific export destination address, all export destination addresses, or default (0.0.0.0) export destination.	
Parameter Restrict export **Valid Values** Enable, Disable **Default Value** Disable **Description** Enabling this parameter restricts the associated route(s) from being exported.	
Parameter Metric **Valid Values** Valid metrics for applicable protocols: RIP - 1 to 16 Hello - 100 to 30000 EGP - 0 to 255 OSPFASE - 0 to 65535 BGP - 0 to 65535 **Default Values** None - only when conditions below apply. **Description** A metric is the cost associated with using a link or network. This parameter defines the metric to be used for this exported route on the To protocol network. This parameter is required except when the following conditions apply: From protocol = RIP and To protocol = RIP From protocol = Hello and To protocol = Hello From protocol = Direct From protocol = BGP	
Parameter Specific route **Valid Values** A valid IP address **Default Value** None **Description** This parameter specifies a specific route that you have chosen to export from the From protocol.	
Parameter Mask **Valid Values** A valid IP host address mask **Default Value** 255.255.255.255 **Description** This parameter specifies the mask applied to the IP address defined in the Specific route parameter.	

Table 5-286 (Page 1 of 2). Configuration Worksheet - From Interface/Gateway

Parameter Information	Your Value
Parameter Filter routes from **Valid Values** All sources, Remote router, Interface **Default** None **Description** This parameter specifies whether you will be filtering RIP or Hello routes learned from all sources, a specific remote router, or a specific interface.	

Table 5-286 (Page 2 of 2). Configuration Worksheet - From Interface/Gateway

Parameter Information		Your Value
Parameter	IP address of local interface	
Valid Values	A valid IP address	
Default	None	
Description	This parameter specifies the local interface on this router to export from (source); the export source interface. Use the IP address of the destination if this is a PPP link.	
Parameter	IP address of remote router	
Valid Values	A valid IP address	
Default	None	
Description	This parameter specifies the IP address of a remote router to export from (source); the export source router.	

Table 5-287. Configuration Worksheet - To Interface/Gateway

Parameter Information		Your Value
Parameter	Filter routes to	
Valid Values	All sources, Remote router, Interface	
Default	None	
Description	This parameter specifies whether you will be filtering RIP or Hello routes to be passed to all sources, a specific remote router, or a specific interface.	
Parameter	IP address of local interface	
Valid Values	A valid IP address	
Default	None	
Description	This parameter specifies the local interface on this router to export to (target); the target interface. If this is a PPP link, use the IP address of the destination router.	
Parameter	IP address of remote router	
Valid Values	A valid IP address	
Default	None	
Description	This parameter specifies the IP address of a remote router to export to (target); the export target router.	

IP Packet Filters

The 6611 enables you to configure IP filters at the node level and at the adapter port level. IP filters configured at the node level are applied to inbound IP traffic that is received on any 6611 adapter port that is configured for IP and supports IP filters. IP filters configured at the adapter port level are applied only to inbound IP traffic that is received on that port. See "Well-known Port Filters" on page 5-104 for more information on port level filters.

Filters are applied to datagrams which are received on 6611 ports from the physical network. They are not applied as IP datagrams and are routed internally by the 6611.

You can define filters that are *singular* or *dual*. Singular filters operate on a specific host address, an entire subnetwork, an entire network, all traffic, or combinations thereof. Singular filters apply to both the source and destination IP addresses. Dual filters control the flow of traffic between two specific entities: hosts, networks, subnetworks, or combinations of the three. Dual filters operate on the address and filter mask to specify the entities from which traffic will be filtered.

Defining IP Filters

The filter ID uniquely defines the filter and determines when it is applied. Each port and node level filter must have a unique filter ID. You should choose the filter ID according to the sequence in which you want the incoming traffic to be filtered. A filter with a lower ID is applied before a filter with a higher ID.

Each IP filter is specified by an IP address and a user-defined filter mask. The address and filter mask combination can be used to indicate a network, a subnet, a host, or a combination. Like a subnet address mask, a *filter mask* is a series of bits in which 1s indicate a bit position that is significant for applying the filter. IP applies the filter mask to the source or destination IP address in an incoming IP datagram. Then, IP compares that result to the result of the filter mask applied to the filter IP address. If the two results do not match, the IP datagram is passed to the next filter. If the results match, one of the following events will occur and no further filters will be applied:

- The datagram is discarded if the filter is set to **Deny**
- The datagram is forwarded if the filter is set to **Permit**

Restrictions

- You can define a total of 50 port (see "IP Protocol" on page 5-103 for information) and node level IP packet filters. Each filter must have a unique filter ID. Node level filter numbers are assigned to each interface and may not be used again at the interface level.
- The following adapters will apply IP filters:
  - 6611 Ethernet Adapter
  - 6611-A25 1-Port Ethernet Adapter
  - 6611-A47 1-Port Ethernet Adapter
  - 6611-A47 2-Port Ethernet Adapter
  - 6611 Model 120 Ethernet Adapter
  - 6611 Token-Ring Network 16/4 Adapter
  - 6611-A25 1-Port Token-Ring Network 16/4 Adapter
  - 6611-A25 2-Port Token-Ring Network 16/4 Adapter

- 6611-A47 1-Port Token-Ring Network 16/4 Adapter
- 6611-A47 2-Port Token-Ring Network 16/4 Adapter
- 6611 Model 120 Token-Ring Network 16/4 Adapter
- 6611 2-Port EIA 422/449 Serial Adapter
- 6611-A25 2-Port Multi-Interface Serial Adapter
- 6611-A47 2-Port Multi-Interface Serial Adapter
- 6611-A25 4-Port Multi-Interface Serial Adapter
- 6611-A47 4-Port Multi-Interface Serial Adapter
- 6611 Model 120 2-Port EIA 422/449 Serial Adapter
- 6611 2-Port V.35/V.36 Compatible Serial Adapter
- 6611 Model 120 2-Port V.35/V.36 Compatible Serial Adapter
- 6611-A25 Multi-Interface Serial/Token-Ring Combination Adapter
- 6611-A47 Multi-Interface Serial/Token-Ring Combination Adapter
- 6611-A25 Multi-Interface Serial/Ethernet Combination Adapter
- 6611-A47 Multi-Interface Serial/Ethernet Combination Adapter

The 6611 X.25 Adapter does *not* apply IP filters to inbound IP traffic. However, if the IP traffic is received at the 6611 through one of the eight adapters that support IP filters, the traffic is filtered before it is passed to the 6611 X.25 Adapter.

Configuration Changes...

That Require the IP Function to Restart

None

That Require the 6611 to Restart

None

Configuration Options

Using the Configuration Program, you will:

- **Enable Packet Filters at the node level.**
- **Specify the following parameters for each singular or dual filter:**
  - IP filter ID
  - Filter type
  - Permit/deny traffic
  - IP filter address 1
  - Protocol

Sample Network Graphic

Figure 5-30 on page 5-215 shows two 6611s (6611 A and 6611 B) configured to use node-level IP packet filters.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and RIP over PPP
  - An Ethernet port running RIP and IP
  - A token-ring port running RIP and IP
- 6611 B, which has the following port types and protocols running:

– A serial port running IP and RIP over PPP
– An Ethernet port running RIP and IP
– A token-ring port running RIP and IP

The following information is shown in Figure 5-30:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*

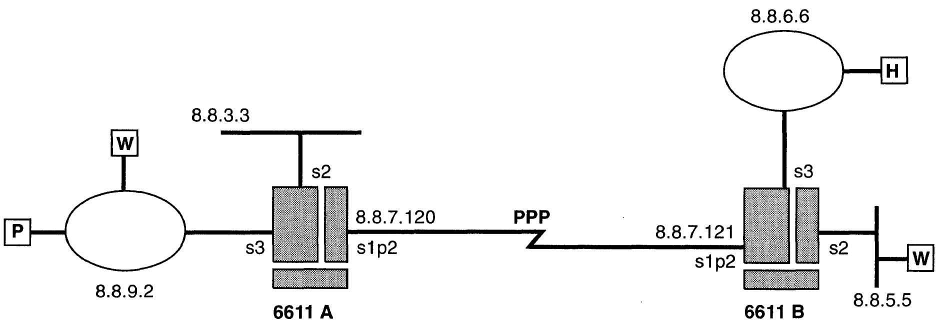


Figure 5-30. Sample Network For IP Packet Filters

This sample network, which is running with a subnet mask of 255.255.255.0, shows:

- The configuration of packet filters at the node level
- The configuration of RIP
- Serial, Ethernet, and token-ring ports

The packet filter defined on router 6611 A (filter 1) is set to prevent the host on token-ring segment 8.8.6.0 from accessing the printer on token-ring segment 8.8.9.0. The packet filter defined on router 6611 B (filter 1) is set to prevent the workstation on token-ring segment 8.8.9.0 from accessing the host on token-ring segment 8.8.6.0.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-30. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Port and Protocols Running on It

Table 5-288. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-289. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-290. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point protocol (PPP) On this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-291. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.7.120	8.8.7.121
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.7.121	8.8.7.120
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Ports and the Protocols Running on Them

Table 5-292. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	None	None
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	None	None

Table 5-293. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.3	8.8.5.5
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table 5-294. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-295. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.9.2	8.8.6.6
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Node-Level Parameters Configured

Table 5-296. Node Level - RIP Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Routing Information Protocol (RIP)	Enable	Enable
Broadcast	Enable	Enable
Zero reserved fields	Enable	Enable
Route preference	100	100

Table 5-297. Node Level - Packet Filter Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable IP packet filters	Enable	Enable
Packet Filter Detail		
Filter ID	1	1
Filter type	Singular	Singular
Filtering mode	Deny	Deny
Filter IP address 1	8.8.6.0	8.8.9.0
Filter subnet mask 1	255.255.255.0	255.255.255.0
Filter IP address 2	NA	NA
Filter subnet mask 2	NA	NA
Protocol	None	None
Well-known port filters		
Filter 1	NA	NA
Filter 2	NA	NA
Filter 3	NA	NA
Filter 4	NA	NA

Node Level Worksheet

Figure 5-31 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-31.

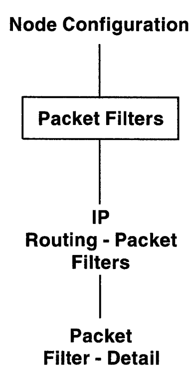


Figure 5-31. Flow of Node Level Packet Filters Help Windows

Use the following table as a worksheet for your node level configurations.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter.

Table 5-298 (Page 1 of 2). Configuration Worksheet - IP Routing - Packet Filters

Parameter Information		Your Value
Parameter	Enable IP packet filters	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables all defined IP filters.	
IP Filter List - Parameters configured for each filter defined		
Parameter	Filter ID (required)	
Valid Values	1 to 50	
Default Value	The next unused ID value	
Description	This parameter specifies the ID of a node-level IP filter (an IP filter that is applied to inbound IP traffic received on any of the IBM 6611's adapter ports).	
Parameter	Filter type	
Valid Values	Singular, Dual	
Default Value	Singular	
Description	This parameter specifies the type of filter for a specific IP filter ID.	
Parameter	Filtering mode	
Valid Values	Permit, Deny	
Default Value	Permit	
Description	This parameter specifies whether the traffic for a specific IP filter ID is to be permitted through the IBM 6611 or is to be discarded.	
Parameter	Filter IP address 1 (required)	
Valid Values	A valid IP address	
Default Value	None	
Description	This parameter specifies the address of the host, subnetwork, or network for a specific IP filter ID.	
Parameter	Filter subnet mask 1	
Valid Values	0.0.0.0 to 255.255.255.255	
Default Value	255.255.255.255	
Description	This parameter specifies the mask for a specific IP filter ID. This mask, with the value given in the Filter IP Address 1 parameter, defines the range of IP addresses to be filtered.	
Parameter	Filter IP address 2	
Valid Values	A valid IP address	
Default Value	None	
Description	This parameter specifies the destination address of the host, subnetwork, or network for a specific IP filter ID.	
Parameter	Filter subnet mask 2	
Valid Values	0.0.0.0 to 255.255.255.255	
Default Value	255.255.255.255	
Description	This parameter specifies the mask for an IP filter ID. The filter subnet mask, with the value of the Filter IP address 2 parameter, defines the range of IP addresses to be filtered.	
Parameter	Protocol	
Valid Values	None, TCP, or UDP	
Default Value	None	
Description	This parameter specifies the IP protocol (TCP/UDP) well-known ports. The filter is applied to that well-known port.	

Table 5-298 (Page 2 of 2). Configuration Worksheet - IP Routing - Packet Filters

Parameter Information	Your Value
Well-known Port Filters	
Parameter Filter 1 **Valid Values** 1 to 1023 **Default Value** None **Description** This parameter specifies the first selected TCP/UDP well-known port associated with this filter ID.	
Parameter Filter 2 **Valid Values** 1 to 1023 **Default Value** None **Description** This parameter specifies the second selected TCP/UDP well-known port associated with this filter ID.	
Parameter Filter 3 **Valid Values** 1 to 1023 **Default Value** None **Description** This parameter specifies the third selected TCP/UDP well-known port associated with this filter ID.	
Parameter Filter 4 **Valid Values** 1 to 1023 **Default Value** None **Description** This parameter specifies the fourth selected TCP/UDP well-known port associated with this filter ID.	

Note: A maximum of 50 node level IP filters can be configured for this 6611.

AppleTalk

AppleTalk is a network protocol developed by Apple** Computer, Inc. The protocol interconnects network devices, which may be a mixture of Apple and non-Apple products. The 6611 supports AppleTalk Phase 2, which extends the capabilities of the AppleTalk protocol to handle more complex networks and internets. AppleTalk Phase 2 increases the number of AppleTalk nodes that can be associated with a network and allows nodes within the same network to belong to different AppleTalk zones.

Port Types Supported

Table 5-299. Port Types Supported for AppleTalk Routing

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	
	IEEE 802.3	LLC	
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	

Restrictions

- If an AppleTalk network is attached to more than one seed router, the same network number range and local zone list must be defined on each seed router port. When changing the network number range or local zone list on the seed router ports, ensure that the configuration changes are applied at the same time on each seed router by using the Configuration Program's scheduled configuration function to control the timing of the changes. See "Specifying a Scheduled Configuration" on page 6-7 for information about using this function.
- If the network number range or a zone name associated with a seed router port is changed, all nonseed routers for which that port is the seed must be restarted in order to acquire the change. See "AppleTalk Ports" on page 5-223 for a description of seed and nonseed router ports.
- When AppleTalk is configured on a serial adapter port using frame relay, you must explicitly define the data link connection identifiers (DLCIs) that will be used by AppleTalk and *all other* protocols running on the same port. In addition, InARP must be enabled on the port.

  First, configure the frame relay protocol by enabling InARP and defining a list of DLCIs assigned to the serial port. Then as you define individual protocols on the port, specify which DLCIs are available for use by each protocol.
- When the AppleTalk protocol is being used in a frame-relay network that is partially meshed (frame-relay connections do not exist between each pair of routers in the network), the following restrictions apply:

- The Enable split horizon for routing table updates parameter must be disabled on each 6611 frame-relay port that provides a connection between AppleTalk routers that are not otherwise connected. Connections are defined using one or more DLCIs.
- All AppleTalk router ports in the frame-relay network must be configured as seed-router ports.
- All seed-router port node IDs must be unique (as specified by the Starting value for node ID acquisition parameter).
- AppleTalk Echo Requests cannot be sent from or received by a frame-relay port on a router in a partially-meshed frame-relay network. However, Echo Requests originating from and destined for other nodes can traverse the frame-relay network and will be forwarded by the router.

Configuration Changes...

That Require the AppleTalk Function to Restart on the Affected Port Only (Except for Frame Relay Ports)

When a new configuration is sent to the 6611 with changes to the following parameters, the AppleTalk function on the affected port is disabled and then enabled again with the changes within a short period of time (approximately 10 seconds, except where otherwise noted). Consequently, the changes have no impact on other 6611 functions and cause only minimal disruption to AppleTalk routing.

- Enable AppleTalk on this port
- Network number range
- Default zone name[1]
- Starting value for node ID acquisition
- Additional zone name[1]
- Enable security filter for resource names
- Enable security filter for zone names
- Enable network number range filter
- Network number range (for network number range filter)
- Optimize NBP Broadcast Request processing
- Generate DDP checksum
- Hop weight
- Enable split horizon for routing table updates
- Control routing information received on this port[1]
- Network number range (of selected network)
- Accept all zone information acquired from selected network[1]
- Allowable zone name (for selected network)[1]
- Enable network number range filter (for selected network)

[1] When this parameter is changed, the affected port is disabled for a period of 5 minutes. Disabling the port causes all routers in the internet to age out the affected port in their routing tables and to subsequently acquire the new information about the port.

That Require the 6611 to Restart

- Port type (seed or nonseed)
- All other AppleTalk configuration parameters on frame relay ports

Before You Configure...

This section contains additional information to assist you in configuring the AppleTalk Phase 2 protocol.

Network Number Ranges

AppleTalk Phase 2 expands the number of nodes that can be concurrently active on a single AppleTalk network by associating each network with a range of network numbers. Each number in a network's *network number range* can represent up to 253 devices (AppleTalk *nodes*). A network number range of 1–5, for example, can provide addressing for up to 1265 nodes (5 times 253).

Each network number range must be unique within the internet to which the AppleTalk network belongs. Ranges cannot overlap and the network numbers used within a range must not be duplicated within the internet.

AppleTalk Ports

Each AppleTalk port on the 6611 is associated with an AppleTalk network, which is defined on the port. The port is treated as a node on the AppleTalk network and maintains a unique node address within the range of network numbers assigned to the network.

An AppleTalk port is defined as a *seed router port* or *nonseed router port*, depending on the port's role. Nonseed router ports acquire network information from a *seed router* attached to the same network. The seed router maintains the configuration data for the network, such as its network number range and zone list. The seed router transmits this information through a seed router port to all other routers directly connected to the network, eliminating the need to separately configure each router port attached to the network. The 6611 can serve as a seed or nonseed router for different AppleTalk networks attached to it.

Network Zone Lists

Each AppleTalk port maintains a *network zone list* for the attached network. Nodes on the network can belong to the zones contained within the network zone list. The list contains the *default zone* for the network and any additional zone names defined by the network administrator when configuring the port.

AppleTalk *zones* provide a way to logically group nodes in an internet regardless of where the nodes are physically located in the internet. Nodes within a zone typically share common characteristics (all nodes in the same department) or provide similar network services (all print servers in the internet). Zones allow users to easily locate and access these nodes.

An AppleTalk node can belong to only one zone. A node's user can assign the node to any one of the zones in the network zone list. Nodes that have not been assigned to a zone belong to the default zone for the network.

AppleTalk Port Filters

As implemented on the 6611, AppleTalk provides two types of port filters:

- Security filters that enable a network administrator and resource owners to control access to AppleTalk zones and resources in the internet. The filters respond to special characters included in the zone or resource names. Refer to the AppleTalk description in the *Introduction and Planning Guide* for information about using these filters.
- A network number range filter that provides the capability to filter inbound and outbound AppleTalk packets on each port based on the source and destination network numbers in the packet. You can filter out all packets received from or destined for a single network number or any range of consecutive network numbers. For example, suppose you want to discard all packets arriving from or destined for network numbers in the range 500–600 and network numbers in the range 700–800. You could specify each of these ranges for the filter, or specify a single range of 500–800 that overlaps the two network number ranges. Note, however, that a filter with the range of 500–800 also would discard any packets arriving from or destined for network numbers 601–699.

Control of Routing Information

The 6611 implementation of AppleTalk enables a network administrator to select which AppleTalk networks the 6611 will maintain routing information about through a specific port. In addition, the network administrator can select the zones in those networks about which the 6611 will maintain information. This feature restricts the 6611's view of the internet, thereby restricting the view of other routers and non-router nodes that obtain information about the internet from the 6611. This capability is useful for controlling the sharing of sensitive network information with portions of the internet that are under separate administrative control.

For a detailed description of this feature, refer to the AppleTalk description in the *Introduction and Planning Guide*.

NBP Broadcast Request Processing

To perform a search for a resource or node within the internet, an AppleTalk workstation node transmits a lookup request to a local AppleTalk router. The lookup request is a Name Binding Protocol (NBP) Broadcast Request and contains the name of the zone to which the target resource or node belongs. Normally, the router responds to the Broadcast Request packet by sending an NBP Forward Request packet to each network in the internet that contains nodes belonging to the zone specified in the original lookup request. Using this method, multiple Forward Request packets may be sent along the same route.

The 6611 implementation of AppleTalk provides an option for reducing the number of Forward Request packets generated by the 6611 when responding to a lookup request. When the Optimize NBP Broadcast Request processing parameter is enabled on the AppleTalk port, the 6611 will respond to a lookup request by forwarding a single Forward Request packet to the next router on each path to one or more destination networks. This technique reduces NBP traffic on the internet by eliminating redundant lookup requests directed toward networks accessible by the same route.

When using this option, the following considerations apply:

- The Optimize NBP Broadcast Request processing parameter must be enabled on all 6611 router ports attached to the same AppleTalk network.
- When a non-6611 router is attached to an AppleTalk network, this option cannot be used on the 6611 router ports on that network.
- Because this option reduces unnecessary traffic, it provides the greatest benefit in situations where conserving bandwidth is an important concern, such as when 6611 routers are connected over low-speed serial links.
- When the next AppleTalk router port on a specified route has this option enabled, that router continues to transmit a single Forward Request packet to adjacent routers on the paths to destination networks. When this option is not enabled on the next router port, the router will generate separate Forward Request packets for each network named in the original lookup request.

For an example of how this option can reduce NBP traffic in your internet, refer to the AppleTalk description in the *Introduction and Planning Guide*.

Preferred Routes

As implemented on the 6611, AppleTalk provides a way for network administrators to select a preferred route for AppleTalk traffic passing through a 6611 router. The Hop weight parameter can be used adjust the hop count assigned to a link connected to an AppleTalk port. If a 6611 router is connected to another AppleTalk router using parallel links, the network administrator can use the parameter to assign a greater hop count to one of the links (normally the slower of the two). Routes with higher hop counts, or *weights*, are given lower priority. Consequently, the link with the lower hop weight would be the primary link and the link with the higher hop weight would be the backup link. The backup link is used when the primary link is unavailable.

When an AppleTalk packet passes through the port, the packet's hop count is adjusted according to the Hop weight parameter. The default value of 1 represents the normal situation in which a single hop is added to the hop count of an outbound packet.

When specifying the Hop weight parameter, it is important to remember that an AppleTalk packet will not be forwarded to another router if the packet's hop count exceeds 15. The number of physical hops a packet can make will be reduced in proportion to the number of hops assigned to the packet using the Hop weight parameter. To avoid making some routers unreachable, ensure that the number of physical hops in a route, plus the hop weight, does not exceed 15.

For additional information on using this option for selecting routes and performing load balancing on links, refer to the AppleTalk description in the *Introduction and Planning Guide*.

Configuration Options

Table 5-300 on page 5-226 summarizes the configuration options for each adapter type that supports the AppleTalk Phase 2 protocol. After configuring AppleTalk on specific ports, you need to enable AppleTalk routing at the node level.

Table 5-300. AppleTalk Configuration Options

WHEN configuring AppleTalk...	THEN optionally...
...on a token-ring port or an Ethernet port: • Enable AppleTalk on the port. • Determine the port type. For seed router ports: – Enter the network number range for the network – Enter the default zone name for the network – Select an initial value for the port's node ID (optional) – Add additional zone names to the network zone list maintained on the port (optional) • Determine whether the port will accept routing and zone information about all networks in the AppleTalk internet, reject all routing and zone information, or accept information about selected networks only. If you choose to accept information about selected networks only, those networks must be explicitly defined.	• Define filters for the port. • Define optional port parameters: – Optimize NBP broadcast request processing – Generate DDP checksum – Hop weight
...on a serial port, using PPP: • Enable AppleTalk on the port. • Determine whether the port will accept routing and zone information about all networks in the AppleTalk internet, reject all routing and zone information, or accept information about selected networks only. If you choose to accept information about selected networks only, those networks must be explicitly defined. **Note:** When connecting AppleTalk networks over a point-to-point link, you need to define AppleTalk on the serial adapter ports at each end of the link.	• Define filters for the port. • Define optional port parameters: – Optimize NBP broadcast request processing – Generate DDP checksum – Hop weight
...on a serial port, using Frame Relay: • Enable AppleTalk on the port. • Determine the port type. For seed router ports: – Enter the network number range for the network – Enter the default zone name for the network – Select an initial value for the port's node ID (optional) – Add additional zone names to the network zone list maintained on the port (optional) • Determine whether the port will accept routing and zone information about all networks in the AppleTalk internet, reject all routing and zone information, or accept information about selected networks only. If you choose to accept information about selected networks only, those networks must be explicitly defined. • Define DLCI numbers for the frame relay connection. **Note:** When connecting AppleTalk networks over a frame relay connection, you need to define AppleTalk on the serial adapter ports at each end of the connection.	• Define filters for the port. • Define optional port parameters: – Optimize NBP broadcast request processing – Generate DDP checksum – Hop weight – Enable split horizon for routing table updates

Sample Network Graphic

Figure 5-32 shows a sample AppleTalk network containing three 6611s configured as AppleTalk routers. The sample network includes:

- 6611 A, which has the following port types and protocols running:
  - Three Ethernet ports running AppleTalk and IP
- 6611 B, which has the following port types and protocols running:
  - An Ethernet port running AppleTalk and IP
  - A token-ring port running AppleTalk and IP
  - A serial port running AppleTalk and IP over PPP
- 6611 C, which has the following port types and protocols running:
  - A serial port running AppleTalk and IP over PPP
  - An Ethernet port running AppleTalk and IP

The following information is shown in Figure 5-32:

- Slot and port numbers, abbreviated S*x* P*y*
- AppleTalk network number ranges and zones
- IP addresses

Note: The configuration of the IP protocol is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to route AppleTalk.

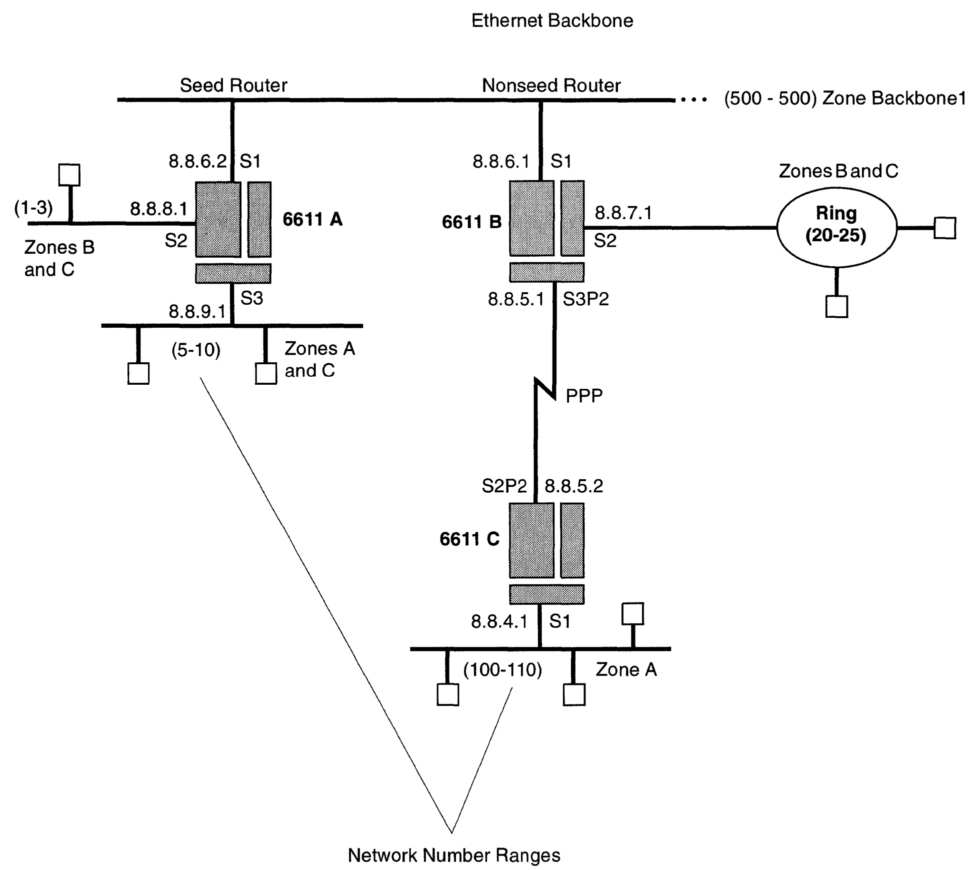


Figure 5-32. Sample AppleTalk Network

In the sample network, 6611 A and 6611 B are attached to an Ethernet backbone network. 6611 A contains the seed router port for the backbone network. 6611 C is connected to 6611 B across a serial link using PPP.

The serial port on 6611 C has been configured to accept information about selected networks only. The intent of this configuration is to restrict the information that 6611 C receives about the internet through its connection to 6611 B, allowing only devices belonging to Zone A on networks 100—110 and 5—10 to share information. 6611 C will accept routing information only about AppleTalk network 5—10, which is attached to router 6611 A. In addition, 6611 C will accept zone information only about Zone A on network 5—10. Consequently, 6611 C will not update its routing table with information about networks 1—3 or 20—25 and will not be aware of the existence of these networks, or of Zones B and C.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-32 on page 5-227. The following tables list the configuration parameters for the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Ethernet Port Parameters Configured - Backbone Network

Table 5-301. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Value (Network 500-500)	6611 B Slot 1 Value (Network 500-500)
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	NA	NA

Table 5-302. Ethernet Port - AppleTalk Port Parameters Configured

Parameter	6611 A Slot 1 Value (Network 500-500)	6611 B Slot 1 Value (Network 500-500)
Enable AppleTalk on this port	Enable	Enable
Port type	Seed router port	Nonseed router port
Control routing information received on this port	Accept information about all networks	Accept information about all networks

Table 5-303. Ethernet Port - AppleTalk Seed Router Port Parameters Configured

Parameter	6611 A Slot 1 Value (Network 500-500)	6611 B Slot 1 Value (Network 500-500)
Network number range	500-500	NA (nonseed port)
Default zone name	Backbone1	NA
Starting value for node ID acquisition	1	NA
Additional zone name	None	NA

Table 5-304. Ethernet Port - IP Port Parameters Configured

Parameter	6611 A Slot 1 Value (Network 500-500)	6611 B Slot 1 Value (Network 500-500)
Enable IP routing on this port	Enable	Enable
IP address	8.8.6.2	8.8.6.1
Subnet mask	None	None
Max. transmission unit (octets)	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Port Parameters Configured - Non-Backbone Networks

Table 5-305. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value (Network 1-3)	6611 A Slot 3 Value (Network 5-10)	6611 C Slot 1 Value (Network 100-110)
Enable physical interface on this port	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA
Enable additional multicast addresses	Disable	Disable	Disable
Multicast MAC address	None	None	None

Table 5-306. Ethernet Port - AppleTalk Port Parameters Configured

Parameter	6611 A Slot 2 Value (Network 1-3)	6611 A Slot 3 Value (Network 5-10)	6611 C Slot 1 Value (Network 100-110)
Enable AppleTalk on this port	Enable	Enable	Enable
Port type	Seed router port	Seed router port	Seed router port
Control routing information received on this port	Accept information about all networks	Accept information about all networks	Accept information about all networks

Table 5-307. Ethernet Port - AppleTalk Seed Router Port Parameters Configured

Parameter	6611 A Slot 2 Value (Network 1-3)	6611 A Slot 3 Value (Network 5-10)	6611 C Slot 1 Value (Network 100-110)
Network number range	1-3	5-10	100-110
Default zone name	B	C	A
Starting value for node ID acquisition	1	1	1
Additional zone name	C	A	None

Table 5-308. Ethernet Port - IP Port Parameters Configured

Parameter	6611 A Slot 2 Value (Network 1-3)	6611 A Slot 3 Value (Network 5-10)	6611 C Slot 1 Value (Network 100-110)
Enable IP routing on this port	Enable	Enable	Enable
IP address	8.8.8.1	8.8.9.1	8.8.4.1
Subnet mask	None	None	None
Max. transmission unit (octets)	1500	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable	Enable
Directed broadcast	Enable	Enable	Enable
Inbound Port Filters	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable

Token-Ring Port Parameters Configured

Table 5-309. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 2 Value (Network 20-25)
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	NA
MAC address format	NA
Token ring data rate	4 Mbps
Broadcast type	Non-local

Table 5-310. Token-Ring Port - AppleTalk Port Parameters Configured

Parameter	6611 B Slot 2 Value (Network 20-25)
Enable AppleTalk on this port	Enable
Port type	Seed router port
Control routing information received on this port	Accept information about all networks

Table 5-311. Token-Ring Port - AppleTalk Seed Router Port Parameters Configured

Parameter	6611 B Slot 2 Value (Network 20-25)
Network number range	20-25
Default zone name	B
Starting value for node ID acquisition	1
Additional zone name	C

Table 5-312. Token-Ring Port - IP Port Parameters Configured

Parameter	6611 B Slot 2 Value (Network 20-25)
Enable IP routing on this port	Enable
IP address	8.8.7.1
Subnet mask	None
Max. transmission unit (octets)	1492
Enable ICMP address mask requests	Enable
Directed broadcast	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Serial Port Parameters Configured

Table 5-313. Serial Port Parameters Configured

Parameter	6611 B Slot 3 Port 2 Value	6611 C Slot 2 Port 2 Value
Data link protocol	PPP	PPP

Table 5-314. Serial Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 3 Port 2 Value	6611 C Slot 2 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56000	56000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for Transmission Group (PPP)	Disable	Disable
Transmission Group name	None	None

Table 5-315. Serial Port - PPP Parameters Configured

Parameter	6611 B Slot 3 Port 2 Value	6611 C Slot 2 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size (octets)	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-316. Serial Port - AppleTalk Port Parameters Configured

Parameter	6611 B Slot 3 Port 2 Value	6611 C Slot 2 Port 2 Value
Enable AppleTalk on this port	Enable	Enable
Control routing information received on this port	Accept information about all networks	Accept information about selected networks only

Table 5-317. Serial Port - AppleTalk Selected Networks Parameters Configured

Parameter	6611 C Slot 2 Port 2 Value
Network number range	5-10
Accept all zone information acquired from selected network	Disable
Allowable zone name	A

Table 5-318. Serial Port - IP Port Parameters Configured

Parameter	6611 B Slot 3 Port 2 Value	6611 C Slot 2 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.5.1	8.8.5.2
Subnet mask	255.255.255.255	255.255.255.255
Destination IP address	8.8.5.2	8.8.5.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable Transmission Group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Node Configuration Parameters Configured

Table 5-319. Node Level - AppleTalk Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value
Enable AppleTalk	Enable	Enable	Enable

Port Level Worksheets

Figure 5-33 on page 5-233 and Figure 5-34 on page 5-233 show the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond directly to the window titles shown in these figures.

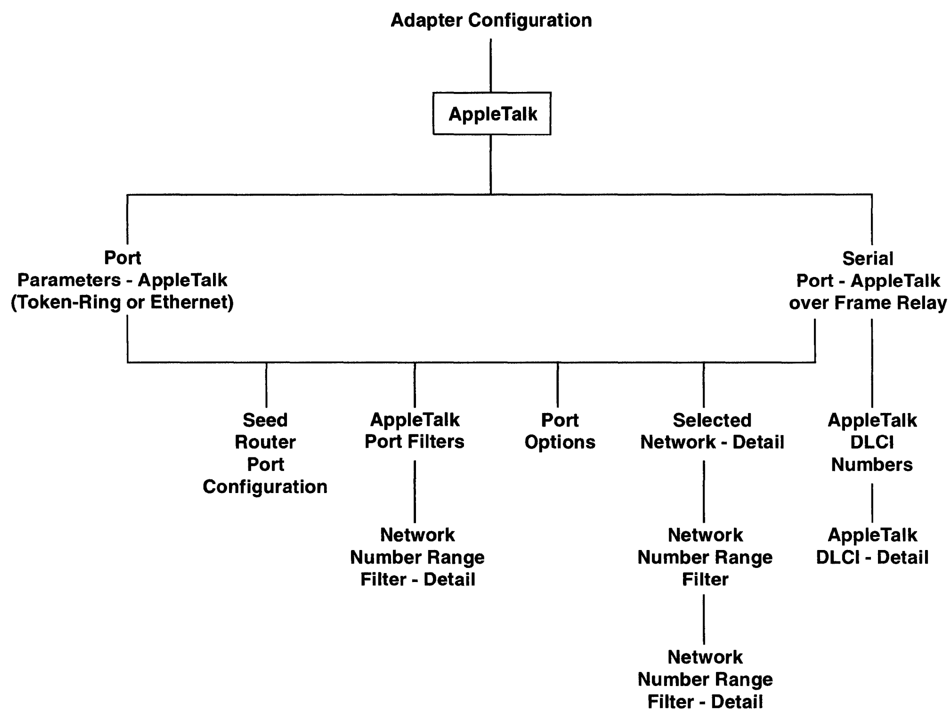


Figure 5-33. Flow of Port Level AppleTalk Help Windows

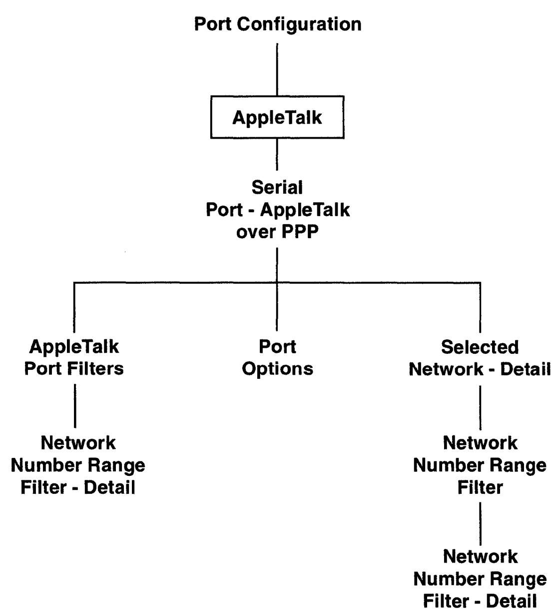


Figure 5-34. Flow of Port Level AppleTalk Help Windows (PPP)

Use the following tables as worksheets for configuring the AppleTalk protocol at the port level.

- AppleTalk parameters on a token-ring port
  - AppleTalk Parameters on page 5-235
  - AppleTalk Seed Router Port Configuration on page 5-235
  - AppleTalk Port Options on page 5-236
  - AppleTalk Port Filters on page 5-237
  - AppleTalk Selected Networks on page 5-238

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-2 on page D-4 for a mapping of parameter names and their associated labels.

Table 5-320. Configuration Worksheet - AppleTalk Parameters (Token Ring)

Parameter Information	Your Value
Parameter Enable AppleTalk on this port **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables the routing of AppleTalk packets on the port.	
Parameter Port type **Valid Values** Nonseed router port, Seed router port **Default** Nonseed router port **Description** This parameter identifies whether this is a seed router port or nonseed router port. Nonseed router ports acquire network information from a seed router. The seed router maintains the configuration data for a network, such as its network range and zone list.	
Parameter Control routing information received on this port **Valid Values** One of the following options: • Accept information about all networks • Accept information about selected networks only • Do not accept routing information **Default** Accept information about all networks **Description** This parameter specifies how AppleTalk routing and zone information received on the port should be handled. When this parameter is set to **Accept information about selected networks only**, the port will accept and maintain routing and zone information only about certain networks that you have selected. These networks must be specified in the list of selected networks. (See Table 5-324 on page 5-238.)	

| *Table 5-321 (Page 1 of 2). Configuration Worksheet - AppleTalk Seed Router Port Configuration (Token Ring)*

Parameter Information	Your Value
Parameter Network number range (required) **Valid Values** A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). An example of a valid network number range is: 98–105. If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be specified. **Default** None **Description** This parameter specifies the range of network numbers that defines the AppleTalk network attached to the port.	
Parameter Default zone name (required) **Valid Values** A string of 1 to 32 ASCII characters, including blank spaces and special characters. A single asterisk (*) is not allowed as a zone name. This character is reserved for use by the AppleTalk protocol. **Default** None **Description** This parameter specifies the default zone name for the network attached to the port.	

Table 5-321 (Page 2 of 2). Configuration Worksheet - AppleTalk Seed Router Port Configuration (Token Ring)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Starting value for node ID acquisition 1 to 253 1 This parameter specifies the initial node identifier (node ID) used by the AppleTalk port on the 6611 when it attempts to acquire a node address. The node address consists of a network number (within the range defined for the network) and a node ID. The node address uniquely identifies the node within the AppleTalk internet.	
Parameter **Valid Values** **Default** **Description**	Additional zone name (required for each zone name defined) A string of 1 to 32 ASCII characters, including blank spaces and special characters. A single asterisk (*) is not allowed as a zone name. This character is reserved for use by the AppleTalk protocol. None This parameter specifies a zone name to add to the network zone list associated with the port.	

Notes:

- The parameters in this table are configured only if the port is defined as a seed router port. Refer to the *Introduction and Planning Guide* for information on how AppleTalk ports on the 6611 acquire their node addresses.
- A maximum of 50 additional zone names can be added to the network zone list. Additional zone names are optional.

Table 5-322 (Page 1 of 2). Configuration Worksheet - AppleTalk Port Options (Token Ring)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Optimize NBP Broadcast Request processing Enable, Disable Disable This parameter specifies how the 6611 should handle Name Binding Protocol (NBP) Broadcast Request packets received from locally attached AppleTalk workstation nodes. When this parameter is enabled, the 6611 responds to a Broadcast Request packet by forwarding a single Forward Request packet to the next router on each path to destination networks. This technique reduces NBP traffic on the internet by eliminating redundant lookup requests for networks accessible by the same route.	
Parameter **Valid Values** **Default** **Description**	Generate DDP checksum Enable, Disable Disable When enabled, this parameter causes a checksum to be generated and included in each Datagram Delivery Protocol (DDP) packet created by the 6611 and transmitted over the port. The 6611 will verify checksums in all DDP packets received on the port, regardless of whether this parameter is enabled or disabled.	

Table 5-322 (Page 2 of 2). Configuration Worksheet - AppleTalk Port Options (Token Ring)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Hop weight 1 to 15, where 1 represents the normal situation in which a single hop is added to the hop count of an outbound packet. 1 This parameter specifies the hop count assigned to a link connected to an AppleTalk port. By controlling the hop counts assigned to links attached to the 6611, a network administrator can designate a preferred route for packets leaving the router. Routes with higher hop counts, or *weights* are given lower priority. The value of this parameter is added to the hop count of AppleTalk packets leaving the port.	

Table 5-323 (Page 1 of 2). Configuration Worksheet - AppleTalk Port Filters (Token Ring)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable security filter for resource names Enable, Disable Disable This parameter enables or disables the port security filter for resource names. The AppleTalk resource name security filter enables a network administrator or resource owners to restrict access to particular resources within the AppleTalk internet by including special characters (˜ and ˜˜) as suffixes on resource names. When enabled, this filter controls the response to name binding queries coming into the port from locally attached nodes.	
Parameter **Valid Values** **Default** **Description**	Enable security filter for zone names Enable, Disable Disable This parameter enables or disables the port security filter for zone names. The AppleTalk zone name security filter enables a network administrator to restrict access to particular zones within the AppleTalk internet by including a special character (#) as part of the zone name. When enabled, this filter restricts the view that nodes have of zones in the network that use the special character within their names.	
Parameter **Valid Values** **Default** **Description**	Enable network number range filter Enable, Disable Disable This parameter enables or disables the network number range filter defined for the AppleTalk port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is discarded. Otherwise, the packet is forwarded.	

Table 5-323 (Page 2 of 2). Configuration Worksheet - AppleTalk Port Filters (Token Ring)

Parameter Information		Your Value
Filter List - Parameter configured for each filter defined		
Parameter	Network number range (required for each filter defined)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–).	
Default	None	
Description	This parameter specifies a range of network numbers used by the network number range filter to evaluate inbound and outbound AppleTalk packets.	

Notes:

- A maximum of 10 network number ranges can be defined for the network number range filter.
- For a detailed description of the AppleTalk security filters and their use, refer to the explanation of the AppleTalk protocol in the *Introduction and Planning Guide*.

Table 5-324 (Page 1 of 2). Configuration Worksheet - AppleTalk Selected Networks (Token Ring)

Parameter Information		Your Value
Selected Networks List - Parameters configured for each network defined		
Parameter	Network number range (required for each network defined)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be specified.	
Default	None	
Description	This parameter specifies a range of network numbers that identifies an AppleTalk network that the 6611 will accept routing and zone information about through the port.	
Parameter	Accept all zone information acquired from selected network	
Valid Values	Enable, Disable	
Default	Enable	
Description	This parameter specifies how the port should handle zone information acquired from the selected network. When this parameter is enabled, the port will accept and maintain information about all zones associated with the selected network. When this parameter is disabled, the port will maintain information only about zones that you have defined using the Allowable zone name parameter. All other zone information will be discarded. **Note:** When this parameter is disabled, you must specify at least one allowable zone name for the selected network.	

Table 5-324 (Page 2 of 2). Configuration Worksheet - AppleTalk Selected Networks (Token Ring)

Parameter Information		Your Value
Filter List - Parameter configured for each zone name defined		
Parameter	Allowable zone name	
Valid Values	A string of 1 to 32 ASCII characters, including blank spaces and special characters.	
Default	None	
Description	This parameter specifies the name of a zone associated with a selected network. If a zone name appears in the list of zone names defined by this parameter, the port will forward information about the zone to other AppleTalk networks. The port discards information received from the selected network about zones not included in the list.	

Notes:

- A list of selected networks needs to be defined when the Control routing information received on this port parameter is set to **Accept information about selected networks only**. The 6611 will maintain routing and zone information about each of the networks in the list and will discard routing and zone information received at the port about networks not included in the list.
- A maximum of 255 zone names can be defined for a selected network.

Table 5-325 (Page 1 of 2). Configuration Worksheet - AppleTalk Selected Networks Filter (Token Ring)

Parameter Information		Your Value
Parameter	Enable network number range filter	
Valid Values	Enable, Disable	
Default	Disable	
Description	The parameter enables or disables a network number range filter that evaluates AppleTalk traffic flowing to and from the selected network. By using this filter, you can control which networks communicate with the selected network over the port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is discarded. Otherwise, the packet is forwarded.	

Table 5-325 (Page 2 of 2). Configuration Worksheet - AppleTalk Selected Networks Filter (Token Ring)

Parameter Information		Your Value
Filter List - Parameter configured for each filter defined		
Parameter	Network number range (required for each filter defined)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–).	
Default	None	
Description	This parameter specifies a range of network numbers used by the network number range filter to evaluate AppleTalk traffic flowing to and from the selected network.	

Note: A maximum of 10 network number ranges can be defined for the network number range filter.

Table 5-326. Configuration Worksheet - AppleTalk Parameters (Ethernet)

Parameter Information		Your Value
Parameter	Enable AppleTalk on this port	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables the routing of AppleTalk packets on the port.	
Parameter	Port type	
Valid Values	Nonseed router port, Seed router port	
Default	Nonseed router port	
Description	This parameter identifies whether this is a seed router port or nonseed router port. Nonseed router ports acquire network information from a seed router. The seed router maintains the configuration data for a network, such as its network range and zone list.	
Parameter	Control routing information received on this port	
Valid Values	One of the following options: • Accept information about all networks • Accept information about selected networks only • Do not accept routing information	
Default	Accept information about all networks	
Description	This parameter specifies how AppleTalk routing and zone information received on the port should be handled. When this parameter is set to **Accept information about selected networks only**, the port will accept and maintain routing and zone information only about certain networks that you have selected. These networks must be specified in the list of selected networks. (See Table 5-330 on page 5-244.)	

Table 5-327. Configuration Worksheet - AppleTalk Seed Router Port Configuration (Ethernet)

Parameter Information		Your Value
Parameter	Network number range (required)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). An example of a valid network number range is: 98–105. If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be specified.	
Default	None	
Description	This parameter specifies the range of network numbers that defines the AppleTalk network attached to the port.	
Parameter	Default zone name (required)	
Valid Values	A string of 1 to 32 ASCII characters, including blank spaces and special characters. A single asterisk (*) is not allowed as a zone name. This character is reserved for use by the AppleTalk protocol.	
Default	None	
Description	This parameter specifies the default zone name for the network attached to the port.	
Parameter	Starting value for node ID acquisition	
Valid Values	1 to 253	
Default	1	
Description	This parameter specifies the initial node identifier (node ID) used by the AppleTalk port on the 6611 when it attempts to acquire a node address. The node address consists of a network number (within the range defined for the network) and a node ID. The node address uniquely identifies the node within the AppleTalk internet.	
Parameter	Additional zone name (required for each zone name defined)	
Valid Values	A string of 1 to 32 ASCII characters, including blank spaces and special characters. A single asterisk (*) is not allowed as a zone name. This character is reserved for use by the AppleTalk protocol.	
Default	None	
Description	This parameter specifies a zone name to add to the network zone list associated with the port.	

Notes:

- The parameters in this table are configured only if the port is defined as a seed router port. Refer to the *Introduction and Planning Guide* for information on how AppleTalk ports on the 6611 acquire their node addresses.
- A maximum of 50 additional zone names can be added to the network zone list. Additional zone names are optional.

Table 5-328. Configuration Worksheet - AppleTalk Port Options (Ethernet)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Optimize NBP Broadcast Request processing Enable, Disable Disable This parameter specifies how the 6611 should handle Name Binding Protocol (NBP) Broadcast Request packets received from locally attached AppleTalk workstation nodes. When this parameter is enabled, the 6611 responds to a Broadcast Request packet by forwarding a single Forward Request packet to the next router on each path to destination networks. This technique reduces NBP traffic on the internet by eliminating redundant lookup requests for networks accessible by the same route.	
Parameter **Valid Values** **Default** **Description**	Generate DDP checksum Enable, Disable Disable When enabled, this parameter causes a checksum to be generated and included in each Datagram Delivery Protocol (DDP) packet created by the 6611 and transmitted over the port. The 6611 will verify checksums in all DDP packets received on the port, regardless of whether this parameter is enabled or disabled.	
Parameter **Valid Values** **Default** **Description**	Hop weight 1 to 15, where 1 represents the normal situation in which a single hop is added to the hop count of an outbound packet. 1 This parameter specifies the hop count assigned to a link connected to an AppleTalk port. By controlling the hop counts assigned to links attached to the 6611, a network administrator can designate a preferred route for packets leaving the router. Routes with higher hop counts, or *weights* are given lower priority. The value of this parameter is added to the hop count of AppleTalk packets leaving the port.	

Table 5-329 (Page 1 of 2). Configuration Worksheet - AppleTalk Port Filters (Ethernet)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable security filter for resource names Enable, Disable Disable This parameter enables or disables the port security filter for resource names. The AppleTalk resource name security filter enables a network administrator or resource owners to restrict access to particular resources within the AppleTalk internet by including special characters (˜ and ¯) as suffixes on resource names. When enabled, this filter controls the response to name binding queries coming into the port from locally attached nodes.	
Parameter **Valid Values** **Default** **Description**	Enable security filter for zone names Enable, Disable Disable This parameter enables or disables the port security filter for zone names. The AppleTalk zone name security filter enables a network administrator to restrict access to particular zones within the AppleTalk internet by including a special character (#) as part of the zone name. When enabled, this filter restricts the view that nodes have of zones in the network that use the special character within their names.	

Table 5-329 (Page 2 of 2). Configuration Worksheet - AppleTalk Port Filters (Ethernet)

Parameter Information		Your Value
Parameter	Enable network number range filter	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables the network number range filter defined for the AppleTalk port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is discarded. Otherwise, the packet is forwarded.	
Filter List - Parameter configured for each filter defined		
Parameter	Network number range (required for each filter defined)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–).	
Default	None	
Description	This parameter specifies a range of network numbers used by the network number range filter to evaluate inbound and outbound AppleTalk packets.	

Notes:

- A maximum of 10 network number ranges can be defined for the network number range filter.
- For a detailed description of the AppleTalk security filters and their use, refer to the explanation of the AppleTalk protocol in the *Introduction and Planning Guide*.

Table 5-330 (Page 1 of 2). Configuration Worksheet - AppleTalk Selected Networks (Ethernet)

Parameter Information		Your Value
Selected Networks List - Parameters configured for each network defined		
Parameter	Network number range (required for each network defined)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be specified.	
Default	None	
Description	This parameter specifies a range of network numbers that identifies an AppleTalk network that the 6611 will accept routing and zone information about through the port.	
Parameter	Accept all zone information acquired from selected network	
Valid Values	Enable, Disable	
Default	Enable	
Description	This parameter specifies how the port should handle zone information acquired from the selected network. When this parameter is enabled, the port will accept and maintain information about all zones associated with the selected network. When this parameter is disabled, the port will maintain information only about zones that you have defined using the Allowable zone name parameter. All other zone information will be discarded. **Note:** When this parameter is disabled, you must specify at least one allowable zone name for the selected network.	

Table 5-330 (Page 2 of 2). Configuration Worksheet - AppleTalk Selected Networks (Ethernet)

Parameter Information		Your Value
Filter List - Parameter configured for each zone name defined		
Parameter	Allowable zone name (required for each zone name defined)	
Valid Values	A string of 1 to 32 ASCII characters, including blank spaces and special characters.	
Default	None	
Description	This parameter specifies the name of a zone associated with a selected network. If a zone name appears in the list of zone names defined by this parameter, the port will forward information about the zone to other AppleTalk networks. The port discards information received from the selected network about zones not included in the list.	

Notes:

- A list of selected networks needs to be defined when the Control routing information received on this port parameter is set to **Accept information about selected networks only**. The 6611 will maintain routing and zone information about each of the networks in the list and will discard routing and zone information received at the port about networks not included in the list.
- A maximum of 255 zone names can be defined for a selected network.

Table 5-331. Configuration Worksheet - AppleTalk Selected Networks Filter (Ethernet)

Parameter Information		Your Value
Parameter	Enable network number range filter	
Valid Values	Enable, Disable	
Default	Disable	
Description	The parameter enables or disables a network number range filter that evaluates AppleTalk traffic flowing to and from the selected network. By using this filter, you can control which networks communicate with the selected network over the port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is discarded. Otherwise, the packet is forwarded.	
Filter List - Parameter configured for each filter defined		
Parameter	Network number range (required for each filter defined)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–).	
Default	None	
Description	This parameter specifies a range of network numbers used by the network number range filter to evaluate AppleTalk traffic flowing to and from the selected network.	

Table 5-332. Configuration Worksheet - AppleTalk over PPP

Parameter Information	Your Value
Parameter Enable AppleTalk on this port **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables the routing of AppleTalk packets on the port.	
Parameter Control routing information received on this port **Valid Values** One of the following options: • Accept information about all networks • Accept information about selected networks only • Do not accept routing information **Default** Accept information about all networks **Description** This parameter specifies how AppleTalk routing and zone information received on the port should be handled. When this parameter is set to **Accept information about selected networks only**, the port will accept and maintain routing and zone information only about certain networks that you have selected. These networks must be specified in the list of selected networks. (See Table 5-335 on page 5-247.)	

Table 5-333. Configuration Worksheet - AppleTalk Port Options (PPP)

Parameter Information	Your Value
Parameter Optimize NBP Broadcast Request processing **Valid Values** Enable, Disable **Default** Disable **Description** This parameter specifies how the 6611 should handle Name Binding Protocol (NBP) Broadcast Request packets received from locally attached AppleTalk workstation nodes. When this parameter is enabled, the 6611 responds to a Broadcast Request packet by forwarding a single Forward Request packet to the next router on each path to destination networks. This technique reduces NBP traffic on the internet by eliminating redundant lookup requests for networks accessible by the same route.	
Parameter Generate DDP checksum **Valid Values** Enable, Disable **Default** Disable **Description** When enabled, this parameter causes a checksum to be generated and included in each Datagram Delivery Protocol (DDP) packet created by the 6611 and transmitted over the port. The 6611 will verify checksums in all DDP packets received on the port, regardless of whether this parameter is enabled or disabled.	
Parameter Hop weight **Valid Values** 1 to 15, where 1 represents the normal situation in which a single hop is added to the hop count of an outbound packet. **Default** 1 **Description** This parameter specifies the hop count assigned to a link connected to an AppleTalk port. By controlling the hop counts assigned to links attached to the 6611, a network administrator can designate a preferred route for packets leaving the router. Routes with higher hop counts, or *weights* are given lower priority. The value of this parameter is added to the hop count of AppleTalk packets leaving the port.	

Table 5-334. Configuration Worksheet - AppleTalk Port Filters (PPP)

Parameter Information		Your Value
Parameter	Enable security filter for resource names	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables the port security filter for resource names. The AppleTalk resource name security filter enables a network administrator or resource owners to restrict access to particular resources within the AppleTalk internet by including special characters (˜ and ˜˜) as suffixes on resource names. When enabled, this filter controls the response to name binding queries coming into the port from locally attached nodes.	
Parameter	Enable security filter for zone names	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables the port security filter for zone names. The AppleTalk zone name security filter enables a network administrator to restrict access to particular zones within the AppleTalk internet by including a special character (#) as part of the zone name. When enabled, this filter restricts the view that nodes have of zones in the network that use the special character within their names.	
Parameter	Enable network number range filter	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables the network number range filter defined for the AppleTalk port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is discarded. Otherwise, the packet is forwarded.	
Filter List - Parameter configured for each filter defined		
Parameter	Network number range (required for each filter defined)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65 279. The network numbers are separated by a dash (–).	
Default	None	
Description	This parameter specifies a range of network numbers used by the network number range filter to evaluate inbound and outbound AppleTalk packets.	

Notes:

- A maximum of 10 network number ranges can be defined for the network number range filter.
- For a detailed description of the AppleTalk security filters and their use, refer to the explanation of the AppleTalk protocol in the *Introduction and Planning Guide*.

Table 5-335 (Page 1 of 2). Configuration Worksheet - AppleTalk Selected Networks (PPP)

Parameter Information	Your Value
Selected Networks List - Parameters configured for each network defined	

Table 5-335 (Page 2 of 2). Configuration Worksheet - AppleTalk Selected Networks (PPP)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Network number range (required for each network defined) A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be specified. None This parameter specifies a range of network numbers that identifies an AppleTalk network that the 6611 will accept routing and zone information about through the port.	
Parameter **Valid Values** **Default** **Description**	Accept all zone information acquired from selected network Enable, Disable Enable This parameter specifies how the port should handle zone information acquired from the selected network. When this parameter is enabled, the port will accept and maintain information about all zones associated with the selected network. When this parameter is disabled, the port will maintain information only about zones that you have defined using the Allowable zone name parameter. All other zone information will be discarded. **Note:** When this parameter is disabled, you must specify at least one allowable zone name for the selected network.	
Filter List - Parameter configured for each zone name defined		
Parameter **Valid Values** **Default** **Description**	Allowable zone name (required for each zone name defined) A string of 1 to 32 ASCII characters, including blank spaces and special characters. None This parameter specifies the name of a zone associated with a selected network. If a zone name appears in the list of zone names defined by this parameter, the port will forward information about the zone to other AppleTalk networks. The port discards information received from the selected network about zones not included in the list.	

Notes:

- A list of selected networks needs to be defined when the Control routing information received on this port parameter is set to **Accept information about selected networks only**. The 6611 will maintain routing and zone information about each of the networks in the list and will discard routing and zone information received at the port about networks not included in the list.
- A maximum of 255 zone names can be defined for a selected network.

Table 5-336. Configuration Worksheet - AppleTalk Selected Networks Filter (PPP)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable network number range filter Enable, Disable Disable The parameter enables or disables a network number range filter that evaluates AppleTalk traffic flowing to and from the selected network. By using this filter, you can control which networks communicate with the selected network over the port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is discarded. Otherwise, the packet is forwarded.	
Filter List - Parameter configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Network number range (required for each filter defined) A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). None This parameter specifies a range of network numbers used by the network number range filter to evaluate AppleTalk traffic flowing to and from the selected network.	

Table 5-337. Configuration Worksheet - AppleTalk over Frame Relay

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable AppleTalk on this port Enable, Disable Disable This parameter enables or disables the routing of AppleTalk packets on the port.	
Parameter **Valid Values** **Default** **Description**	Port type Nonseed router port, Seed router port Nonseed router port This parameter identifies whether this is a seed router port or nonseed router port. Nonseed router ports acquire network information from a seed router. The seed router maintains the configuration data for a network, such as its network range and zone list.	
Parameter **Valid Values** **Default** **Description**	Control routing information received on this port One of the following options: • Accept information about all networks • Accept information about selected networks only • Do not accept routing information Accept information about all networks This parameter specifies how AppleTalk routing and zone information received on the port should be handled. When this parameter is set to **Accept information about selected networks only**, the port will accept and maintain routing and zone information only about certain networks that you have selected. These networks must be specified in the list of selected networks. (See Table 5-342 on page 5-253.)	

Table 5-338. Configuration Worksheet - AppleTalk Seed Router Port Configuration (Frame Relay)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Network number range (required) A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). An example of a valid network number range is: 98–105. If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be specified. None This parameter specifies the range of network numbers that defines the AppleTalk network attached to the port.	
Parameter **Valid Values** **Default** **Description**	Default zone name (required) A string of 1 to 32 ASCII characters, including blank spaces and special characters. A single asterisk (*) is not allowed as a zone name. This character is reserved for use by the AppleTalk protocol. None This parameter specifies the default zone name for the network attached to the port.	
Parameter **Valid Values** **Default** **Description**	Starting value for node ID acquisition 1 to 253 1 This parameter specifies the initial node identifier (node ID) used by the AppleTalk port on the 6611 when it attempts to acquire a node address. The node address consists of a network number (within the range defined for the network) and a node ID. The node address uniquely identifies the node within the AppleTalk internet.	
Parameter **Valid Values** **Default** **Description**	Additional zone name (required for each zone name defined) A string of 1 to 32 ASCII characters, including blank spaces and special characters. A single asterisk (*) is not allowed as a zone name. This character is reserved for use by the AppleTalk protocol. None This parameter specifies a zone name to add to the network zone list associated with the port.	

Notes:

- The parameters in this table are configured only if the port is defined as a seed router port. Refer to the *Introduction and Planning Guide* for information on how AppleTalk ports on the 6611 acquire their node addresses.
- A maximum of 50 additional zone names can be added to the network zone list. Additional zone names are optional.

Table 5-339. Configuration Worksheet - AppleTalk Port Options (Frame Relay)

Parameter Information		Your Value
Parameter	Optimize NBP Broadcast Request processing (see table note)	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter specifies how the 6611 should handle Name Binding Protocol (NBP) Broadcast Request packets received from locally attached AppleTalk workstation nodes. When this parameter is enabled, the 6611 responds to a Broadcast Request packet by forwarding a single Forward Request packet to the next router on each path to destination networks. This technique reduces NBP traffic on the internet by eliminating redundant lookup requests for networks accessible by the same route.	
Parameter	Generate DDP checksum	
Valid Values	Enable, Disable	
Default	Disable	
Description	When enabled, this parameter causes a checksum to be generated and included in each Datagram Delivery Protocol (DDP) packet created by the 6611 and transmitted over the port. The 6611 will verify checksums in all DDP packets received on the port, regardless of whether this parameter is enabled or disabled.	
Parameter	Hop weight	
Valid Values	1 to 15, where 1 represents the normal situation in which a single hop is added to the hop count of an outbound packet.	
Default	1	
Description	This parameter specifies the hop count assigned to a link connected to an AppleTalk port. By controlling the hop counts assigned to links attached to the 6611, a network administrator can designate a preferred route for packets leaving the router. Routes with higher hop counts, or *weights* are given lower priority. The value of this parameter is added to the hop count of AppleTalk packets leaving the port.	
Parameter	Enable split horizon for routing table updates	
Valid Values	Enable, Disable	
Default	Enable	
Description	When this parameter is enabled, the split horizon technique is used to control the broadcast of routing table updates. Routes learned through this port are not broadcast out this port. The affected routing table entries are not included in the Routing Table Maintenance Protocol (RTMP) packet when the packet is transmitted. When this parameter is disabled, the entire routing table will be sent out the port in the RTMP packet. In most cases, this parameter should be enabled to limit the size of routing table broadcasts in the network. However, by disabling this parameter, you can configure a frame-relay network for AppleTalk that is partially meshed, meaning that a frame-relay connection (DLCI) does not need to exist between each pair of routers in the network.	

Note: The Optimize NBP Broadcast Request processing parameter is automatically disabled when the Enable split horizon for routing table updates parameter is disabled. Both of these parameters must be disabled when this port is part of a partially-meshed frame-relay configuration.

Table 5-340. Configuration Worksheet - AppleTalk Port Filters (Frame Relay)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable security filter for resource names Enable, Disable Disable This parameter enables or disables the port security filter for resource names. The AppleTalk resource name security filter enables a network administrator or resource owners to restrict access to particular resources within the AppleTalk internet by including special characters (˜ and ¯) as suffixes on resource names. When enabled, this filter controls the response to name binding queries coming into the port from locally attached nodes.	
Parameter **Valid Values** **Default** **Description**	Enable security filter for zone names Enable, Disable Disable This parameter enables or disables the port security filter for zone names. The AppleTalk zone name security filter enables a network administrator to restrict access to particular zones within the AppleTalk internet by including a special character (#) as part of the zone name. When enabled, this filter restricts the view that nodes have of zones in the network that use the special character within their names.	
Parameter **Valid Values** **Default** **Description**	Enable network number range filter Enable, Disable Disable This parameter enables or disables the network number range filter defined for the AppleTalk port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is discarded. Otherwise, the packet is forwarded.	
Filter List - Parameter configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Network number range (required for each filter defined) A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). None This parameter specifies a range of network numbers used by the network number range filter to evaluate inbound and outbound AppleTalk packets.	

Notes:

- A maximum of 10 network number ranges can be defined for the network number range filter.
- For a detailed description of the AppleTalk security filters and their use, refer to the explanation of the AppleTalk protocol in the *Introduction and Planning Guide*.

Table 5-341. Configuration Worksheet - AppleTalk DLCI Numbers (Frame Relay)

Parameter Information	Your Value
DLCIs List - Parameter configured for each DLCI defined	
Parameter DLCI number (required) **Valid Values** Any of the listed DLCIs **Default** None **Description** This parameter identifies a DLCI that will be used to transmit AppleTalk packets over a frame relay network. Select one of the DLCIs from the list defined for the port. At least one DLCI must be specified to configure AppleTalk on the port.	

Note: To specify which DLCIs are available for AppleTalk, you first need to assign DLCIs to the serial adapter port. DLCIs are assigned when configuring the frame relay parameters for the port.

Table 5-342 (Page 1 of 2). Configuration Worksheet - AppleTalk Selected Networks (Frame Relay)

Parameter Information	Your Value
Selected Networks List - Parameters configured for each network defined	
Parameter Network number range (required for each network defined) **Valid Values** A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be specified. **Default** None **Description** This parameter specifies a range of network numbers that identifies an AppleTalk network that the 6611 will accept routing and zone information about through the port.	
Parameter Accept all zone information acquired from selected network **Valid Values** Enable, Disable **Default** Enable **Description** This parameter specifies how the port should handle zone information acquired from the selected network. When this parameter is enabled, the port will accept and maintain information about all zones associated with the selected network. When this parameter is disabled, the port will maintain information only about zones that you have defined using the Allowable zone name parameter. All other zone information will be discarded. **Note:** When this parameter is disabled, you must specify at least one allowable zone name for the selected network.	
Filter List - Parameter configured for each zone name defined	

Table 5-342 (Page 2 of 2). Configuration Worksheet - AppleTalk Selected Networks (Frame Relay)

Parameter Information		Your Value
Parameter	Allowable zone name (required for each zone name defined)	
Valid Values	A string of 1 to 32 ASCII characters, including blank spaces and special characters.	
Default	None	
Description	This parameter specifies the name of a zone associated with a selected network. If a zone name appears in the list of zone names defined by this parameter, the port will forward information about the zone to other AppleTalk networks. The port discards information received from the selected network about zones not included in the list.	

Notes:

- A list of selected networks needs to be defined when the Control routing information received on this port parameter is set to **Accept information about selected networks only**. The 6611 will maintain routing and zone information about each of the networks in the list and will discard routing and zone information received at the port about networks not included in the list.
- A maximum of 255 zone names can be defined for a selected network.

Table 5-343 (Page 1 of 2). Configuration Worksheet - AppleTalk Selected Networks Filter (Frame Relay)

Parameter Information		Your Value
Parameter	Enable network number range filter	
Valid Values	Enable, Disable	
Default	Disable	
Description	The parameter enables or disables a network number range filter that evaluates AppleTalk traffic flowing to and from the selected network. By using this filter, you can control which networks communicate with the selected network over the port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is discarded. Otherwise, the packet is forwarded.	

Table 5-343 (Page 2 of 2). Configuration Worksheet - AppleTalk Selected Networks Filter (Frame Relay)

Parameter Information		Your Value
Filter List - Parameter configured for each filter defined		
Parameter	Network number range (required for each filter defined)	
Valid Values	A range of consecutive network numbers in the form: lowest network number - highest network number Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–).	
Default	None	
Description	This parameter specifies a range of network numbers used by the network number range filter to evaluate AppleTalk traffic flowing to and from the selected network.	

Note: A maximum of 10 network number ranges can be defined for the network number range filter.

Node Level Worksheet

Use the following table as a worksheet for configuring the AppleTalk protocol at the node level. For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter.

Table 5-344. Configuration Worksheet - Enable AppleTalk (Node Configuration)

Parameter Information		Your Value
Parameter	Enable AppleTalk	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables the routing of AppleTalk packets on all ports configured to support AppleTalk. If this parameter is disabled, but bridging has been defined, the 6611 will bridge AppleTalk packets.	

DECnet

DECnet is a network protocol developed by the Digital Equipment Corporation. DECnet allows routing nodes and end nodes to communicate and share resources. The 6611 supports DECnet Phase IV and DECnet Phase IV-Prime. The DECnet Phase IV supports routing functions across both LAN segments and WAN segments. The DECnet Phase IV-Prime supports arbitrary MAC addressing, extending the DECnet Phase IV addressing scheme to allow use of both locally administered and universally administered MAC addresses.

Port Types Supported

Table 5-345. Port Types Supported for DECnet Phase IV and Phase IV-Prime Routing

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	
		SNAP	
Token-Ring Network	IEEE 802.5	LLC	
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	

Restrictions

- You can only have one port configured with a DECnet Phase IV circuit type on any given physical LAN segment.
- If you want to run DECnet Phase IV and DECnet Phase IV-Prime on a physical LAN segment, you must configure a bilingual circuit in a routing node with access to both the DECnet Phase IV nodes and the DECnet Phase IV-Prime nodes.
- If you configure a bilingual circuit within a 6611 and you enable split horizon with poison reverse, the Multiprotocol Network Program will not use the split horizon with poison reverse option on the bilingual circuit.
- For a physical LAN segment with a mixture of DECnet Phase IV and DECnet Phase IV-Prime nodes, a 6611 with a bilingual circuit must be the designated router for correct translation between DECnet Phase IV and DECnet Phase IV-Prime to occur. Refer to the *Introduction and Planning Guide* for more information about designated routers.
- When DECnet is configured on a frame-relay port with either AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by DECnet on the port.

Configuration Changes ...

That Require the DECnet Function to Restart

- DECnet routing parameters (node level)
  - Enable DECnet routing
  - Local DECnet address
  - Node type
  - Routing-IV maximum cost
  - Routing-IV maximum hops
  - Area maximum cost
  - Area maximum hops
- DECnet option parameters
  - Maximum address (1-1023)
  - Maximum area (1-63)
  - Maximum visits (1-63)
  - Buffer size (260-17800 bytes)
  - Maximum broadcast non-routers (1-1022)
  - Maximum broadcast routers (1-1022)
- DECnet packet filters
  - Filter ID
  - Filter type
  - Permit or deny traffic
  - Filter DECnet address 1
  - Filter mask 1
  - Filter DECnet address 2
  - Filter mask 2

That Require the 6611 to Restart DECnet Ports

- DECnet parameters (port level)
  - Enable DECnet on this port
  - Router priority (0-127)
  - Circuit cost (1-63)
  - Hello timer (1-8191 seconds)
  - Routing timer (1-65535 seconds)
  - Maximum routers (1-1022)
- DECnet port filters
  - Enable DECnet filters on this port
  - Filter ID
  - Direction in which packet is moving
- DECnet destinations per DLCI parameter
  - DLCI number
  - Destination DECnet address
  - Destination DECnet node type

Before You Configure...

This section contains additional information to assist you in configuring DECnet. Refer to the *Introduction and Planning Guide* for more information.

- Functional Addresses

  The Multiprotocol Network Program Version 1 Release 1.0, Release 1.1.0, and Release 1.1.1 automatically set all functional addresses. Therefore, the functional addresses for all DECnet Phase IV routers may differ if you concurrently:

  - Use DECnet Phase IV
  - Do not upgrade all of your 6611s to the Multiprotocol Network Program Version 1 Release 1.1.2 or above
  - Change one or more functional address parameters[2]

  The 6611 uses the All routers functional address to exchange routing information. If this functional address differs on one or more 6611s, a loss of communication will occur resulting in inconsistent routing databases across the network.

- Packet Filters

  To configure DECnet packet filters for a 6611, you must:

  1. Define each filter at the node level with a unique filter ID.
  2. Identify which filters to apply on a particular port using the filter ID.

Configuration Options

Table 5-346 on page 5-259 summarizes the configuration options for each adapter type that supports the DECnet Phase IV protocol. You need to enable DECnet routing at the node level, then configure DECnet on specific ports.

[2] Regardless of any changes you make to the token-ring functional addresses, the equivalent multicast address does not change.

Table 5-346. DECnet Configuration Options

WHEN configuring DECnet...	THEN optionally...
...on a token-ring port or an Ethernet port: • Enable DECnet on the port.	• Define DECnet filters for this port. • Determine the DECnet circuit type. • Determine the router priority value. • Determine the circuit cost value. • Determine the hello time value. • Determine the routing timer value. • Determine the maximum routers value.
...on a serial port using PPP: • Enable DECnet on the port.	• Define DECnet filters for this port. • Enter the remote DECnet address to identify the router at the other end of the connection. • Determine the remote DECnet node type. • Determine the DECnet circuit type. • Determine the router priority value. • Determine the circuit cost value. • Determine the hello time value. • Determine the routing timer value. • Determine the maximum routers value.
...on a serial port using frame relay: • Enable DECnet on the port.	• Define DECnet destinations for each DLCI to provide a logical mapping between the DLCI number and the destination DECnet address. • Define DECnet filters for this port. • Determine the DECnet circuit type. • Determine the router priority value. • Determine the circuit cost value. • Determine the hello time value. • Determine the routing timer value. • Determine the maximum routers value.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform DECnet routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-347 (Page 1 of 2). DECnet Configuration Verification Checklist

DECNET Rule	Configuration Parameter	√
Node-Level Parameters:		
Enable the Enable DECnet router parameter. on all routers that transport DECnet.	Enable DECnet router	
Ensure that all configured DECnet addresses in the network are unique.	Local DECnet address	

Table 5-347 (Page 2 of 2). DECnet Configuration Verification Checklist		
DECNET Rule	**Configuration Parameter**	√
Ensure that there is at least one level 2 router in each area where inter-area communication is needed. Level 2 routers are indicated by a value of area for the Node type parameter.	Node type	
Ensure that any two areas are connected by level 2 routers. Level 2 routers are indicated by a value of area for the Node type parameter.	Node type	
Ensure that the value of the Maximum address parameter is at least as large as the largest DECnet address in the area.	Maximum address	
	Local DECnet address	
Ensure that the value of the Maximum area parameter is at least as large as the largest area number specified.	Maximum area	
	Local DECnet address	
Ensure that the value of the Maximum address parameter is the same across all DECnet routers in the area.	Maximum address	
	Local DECnet address	
Ensure that the value of the Maximum area parameter is the same across all routers in an area.	Maximum area	
	Local DECnet address	
Ensure that the value of the Routing buffer size parameter is the same across all DECnet routers in an area.	Routing buffer size	
	Local DECnet address	
For each 6611, ensure that the value of the All end nodes functional address parameter is not the same as the value of the All routers functional address parameter.	All end nodes functional address	
	All routers functional address	
Ensure that all DECnet nodes on a token-ring LAN segment have the same value for the following parameters:	All routers functional address	
• All routers functional address • All end nodes functional address	All end nodes functional address	
Port-Level Parameters:		
Ensure that the Enable DECnet parameter is enabled on this port.	Enable DECnet on this port	
Ensure the value of the Circuit cost parameter is less that the value of the area maximum cost and Maximum Cost parameters.	Circuit cost	
	Area maximum cost	
	Maximum cost	
Ensure that bilingual routers have a higher priority than AMA or Phase IV routers in a LAN or extened LAN segment.	DECnet circuit type	
	Router priority	
	Node type	
When a network has a mixture of DECnet Phase IV and DECnet Phase IV Prime nodes in a LAN or extended LAN segment, at least one bilingual router must exist between the nodes.	Node type	
	DECnet circuit type	
Ensure that the number of routers connected to one circuit is not greater than the maximum number of routers entered.	Maximum routers	
Ensure that the Maximum broadcast routers value specified at the node level is always greater than the Maximum routers value specified at the port level.	Maximum broadcast routers	
	Maximum routers	
Ensure that the value of the Circuit cost parameter is the same for all DECnet nodes on the same segment.	Circuit cost	

Sample Network Graphic

Figure 5-35 shows two 6611s (6611 A and 6611 B) that are configured to route DECnet.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running DECnet over PPP
  - An Ethernet port running DECnet
- 6611 B, which has the following port types and protocols running:
  - A serial port running DECnet over PPP
  - A token-ring port running DECnet

The following information is shown in Figure 5-41 on page 5-307:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*
- DECnet addresses

Note: The configuration of the IP protocol is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to route DECnet.

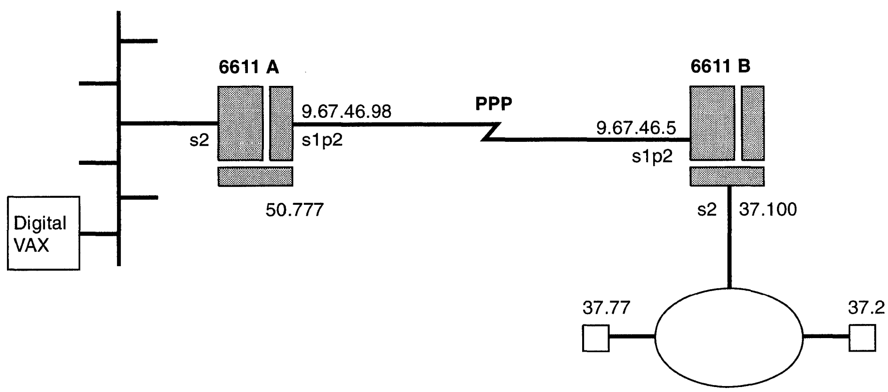


Figure 5-35. Sample Network for Routing DECnet

Summary of All Customized Parameters in Sample One

Use this section as a reference for Figure 5-35. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and the Protocols Running on Them

Table 5-348. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-349. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	None	None

Table 5-350. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size (1500–2052 octets)	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-351. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.98	9.67.46.5
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	9.67.46.5	9.67.46.98
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-352. Serial Port - DECnet Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable DECnet on this port	Enable	Enable
DECnet circuit type	Phase IV	Phase IV
Remote DECnet address	37.100	50.777
Remote DECnet node type	Area	Area
Router priority	64	64
Circuit cost	4	4
Hello timer	15	15
Routing timer	180	180
Maximum routers	32	32
Port filters	Enable	Enable

Token-Ring Ports and Protocols Running on Them

Table 5-353. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 2 Value
Enable physical interface on this port	Enable
MAC address	Locally administered address
Locally administered address	5500 2000 2629
MAC address format	Noncanonical
Token ring data rate	16 Mbps
Broadcast type	Non-local

Note: The Configuration Program automatically sets the MAC address parameter to **Locally administered address** and calculates the locally administered MAC address using the Local DECnet address parameter.

Table 5-354. Token-Ring Port - DECnet Parameters Configured

Parameter	6611 B Slot 2 Value
Enable DECnet on this port	Enable
DECnet circuit type	Bilingual
Router priority	64
Circuit cost	4
Hello timer	15
Routing timer	40
Maximum routers	32
Port Filters	Enable

Ethernet Ports and Protocols Running on Them

Table 5-355. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value
Enable physical interface on this port	Enable
MAC Address	Locally administered address
Locally administered address	AA00040009CB
Enable additional multicast addresses	Disable
Multicast MAC address	None

Note: The Configuration Program automatically sets the MAC address parameter to **Locally administered address** and calculates the locally administered MAC address using the Local DECnet address parameter.

Table 5-356. Ethernet Port - DECnet Parameters Configured

Parameter	6611 A Slot 2 Value
Enable DECnet on this port	Enable
DECnet circuit type	Phase IV
Router priority	64
Circuit cost	4
Hello timer	15
Routing timer	40
Maximum routers	32
Port filters	Enable

Node-Level Parameters Configured

Table 5-357. Node Level - DECnet Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable DECnet	Enable	Enable
Local DECnet address	50.777	37.100
Node type	Area (Level 2)	Area (Level 2)
Routing-IV		
Maximum hops	30	30
Maximum cost	1022	1022
Area		
Maximum hops	30	30
Maximum cost	1022	1022

Node Level Worksheets

Figure 5-36 on page 5-265 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-36 on page 5-265.

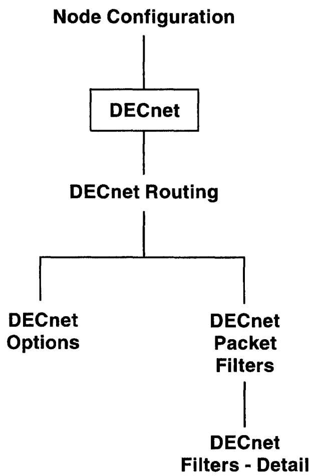


Figure 5-36. Flow of Node Level DECnet Help Windows

Use the following tables as worksheets for your node level configurations:

- DECnet Routing on page 5-265
- DECnet Options on page 5-266
- DECnet Packet Filters on page 5-268

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-8 on page D-10 for a mapping of parameter names and their associated labels.

Table 5-358 (Page 1 of 2). Configuration Worksheet - DECnet Routing

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable DECnet Enable, Disable Disable This parameter enables or disables DECnet routing on all ports configured for DECnet.	
Parameter **Valid Values** **Default Value** **Description**	Local DECnet address An address in the form of <area number>.<node number>, where: • Area number is from 1 to 63 • Node number is from 1 to 1023 None This parameter defines the DECnet address of this 6611.	
Parameter **Valid Values** **Default Value** **Description**	Node type Routing-IV, Area Area If you select **Routing-IV** (Level 1), the 6611 performs DECnet Level 1 router functions, forwarding packets to destinations within the same area or to the closest DECnet area router within its area. If you select **Area** (Level 2), the 6611 performs DECnet Level 2 router functions, forwarding packets to DECnet routers in other areas and to nodes within its area.	

Table 5-358 (Page 2 of 2). Configuration Worksheet - DECnet Routing

Parameter Information		Your Value
Routing-IV		
Parameter **Valid Values** **Default Value** **Description**	Maximum cost 1 to 1022 1022 This parameter represents the maximum path cost allowed from the 6611 to any other node in its area. A node is unreachable if the cost of the least costly path exceeds the value of this parameter. A node is reachable if the total path cost and path length are less than the values specified for this parameter and the Maximum hops parameter.	
Parameter **Valid Values** **Default Value** **Description**	Maximum hops 1 to 30 30 This parameter represents the maximum number of routing hops allowed from the router to any other node within its own area. A node is unreachable if the length of the shortest path between two nodes exceeds the value of this parameter. A node is reachable if the total path cost and path length are less than the value specified for this parameter and the value specified for the Maximum cost parameter.	
Area		
Parameter **Valid Values** **Default Value** **Description**	Maximum cost 1 to 1022 1022 This parameter specifies the maximum total path cost between the local Area (Level 2) router and any other Area router in the network. A remote area is reachable if the total path cost and path length to the nearest Area router in the remote area are less than the values specified for this parameter and the Area maximum hops parameter.	
Parameter **Valid Values** **Default Value** **Description**	Maximum hops 1 to 30 30 This parameter specifies the maximum number of hops that a packet can traverse between the local Area router and any other Area router in the network. A remote area is reachable if the total path cost and path length to the nearest Area router in the remote area are less than the values specified for this parameter and the Area maximum cost parameter.	

Table 5-359 (Page 1 of 3). Configuration Worksheet - DECnet Options

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Maximum address 1 to 1023 1023 This parameter represents the largest node number that the 6611 recognizes within its area. It also specifies the maximum number of nodes within the area.	
Parameter **Valid Values** **Default Value** **Description**	Maximum area 1 to 63 63 This parameter represents the largest area number within a DECnet network. It also specifies the maximum number of areas within a DECnet network.	

Table 5-359 (Page 2 of 3). Configuration Worksheet - DECnet Options

Parameter Information		Your Value
Parameter	Maximum visits	
Valid Values	1 to 63	
Default Value	63	
Description	This parameter limits the maximum number of nodes through which a packet can be routed before arriving at its destination, preventing packets from being looped endlessly through the network. If the number of nodes that a packet visits exceeds the value of this parameter, then the packet is discarded. The value of this parameter should be at least twice the size of the value of the Maximum hops parameter.	
Parameter	Routing buffer size	
Valid Values	260 to 17800	
Default Value	1500	
Description	This parameter determines the maximum size of a DECnet Phase IV or DECnet Phase IV-Prime packet (routing data or control) that would be received by the Multiprotocol Network Program. It includes the routing headers and any pad bytes that might be prefixed to the packets. **Note:** The default is set to allow you to send frames across both token-ring and Ethernet LAN segments.	
Parameter	Enable split horizon with poison reverse	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables the use of split horizon with poison reverse.	
Maximum Broadcast		
Parameter	Non-routers	
Valid Values	1 to 1022	
Default Value	1022	
Description	This parameter defines the maximum number of end nodes (non-routing nodes) allowed on all LAN segments attached to the 6611. This maximum, or total, should be larger or equal to the total number of end nodes already present on these segments (combined total).	
Parameter	Routers	
Valid Values	1 to 1022	
Default Value	32	
Description	This parameter sets the maximum number of routing nodes permitted on all directly attached LAN segments. • On a Level 1 (Routing-IV) router in a multiple area network, this parameter should be greater than or equal to the total number of routers (Level 1 and Level 2) in the same area on all segments to which the router is attached. • On a Level 2 (Area) router in a multiple area network, this parameter should be greater than or equal to the total number of routers (Level 1 and Level 2) in the same area on the connected segments, plus all the Level 2 routers in all the other areas on connected LANs.	
Token-ring functional addresses		
Parameter	All routers	
Valid Values	A valid token-ring functional address	
Default Value	X'C000 1000 0000'	
Description	This parameter defines the functional address used to communicate with all DECnet Phase IV and DECnet Phase IV-Prime routers on a token-ring LAN.	

Table 5-359 (Page 3 of 3). Configuration Worksheet - DECnet Options

Parameter Information	Your Value
Parameter All end nodes **Valid Values** A valid token-ring functional address **Default Value** X'C000 0800 0000' **Description** This parameter defines the functional address used to communicate with all DECnet Phase IV and DECnet Phase IV-Prime end nodes on a token-ring LAN segment.	

Table 5-360 (Page 1 of 2). Configuration Worksheet - DECnet Packet Filters

Parameter Information	Your Value
DECnet Packet Filter List - Parameters configured for each filter defined	
Parameter Filter ID **Valid Values** 1 to 100 **Default Value** None **Description** This parameter specifies the filter ID. It is important to choose the number with regard to the sequence in which you want the incoming traffic to be filtered. A filter with a lower ID number will be applied before a filter with a higher ID number.	
Parameter Filter type **Valid Values** Singular, Dual **Default Value** Singular **Description** This parameter specifies the type of filter. If you select **Singular**, this filter will apply to all traffic from the node or subnetwork specified in the Filter DECnet Address 1 and Filter mask 1 parameters. If you select **Dual**, this filter will apply to all traffic between the nodes or subnetworks specified in the Filter DECnet address 1 and Filter mask 1 parameters, and the Filter DECnet address 2 and Filter mask 2 parameters.	
Parameter Filtering mode **Valid Values** Permit, Deny **Default Value** Permit **Description** This parameter specifies whether the traffic for this filter is permitted through the router or is discarded.	
Parameter Filter DECnet address 1 **Valid Values** An address in the form of <area number>.<node number>, where: • Area number is from 1 to 63 • Node number is from 1 to 1023 **Default Value** None **Description** This parameter specifies the address of a DECnet node.	
Parameter Filter mask 1 **Valid Values** 0.0 to 63.1023 **Default Value** 63.1023 **Description** This parameter specifies the mask for Filter DECnet address 1. Filter masks are used to create a range of addresses to be filtered.	
Parameter Filter DECnet address 2 **Valid Values** An address in the form of <area number>.<node number>, where: • Area number is from 1 to 63 • Node number is from 1 to 1023 **Default Value** None **Description** This parameter specifies the address of a DECnet node. This parameter only used when defining a dual filter.	

Table 5-360 (Page 2 of 2). Configuration Worksheet - DECnet Packet Filters

Parameter Information		Your Value
Parameter	Filter mask 2	
Valid Values	0.0 to 63.1023	
Default Value	63.1023	
Description	This parameter specifies the mask for Filter DECnet address 2. Filter masks are used to create a range of addresses to be filtered.	

Note: You can configure up to 100 filters.

Port Level Worksheets

Figure 5-37 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-37.

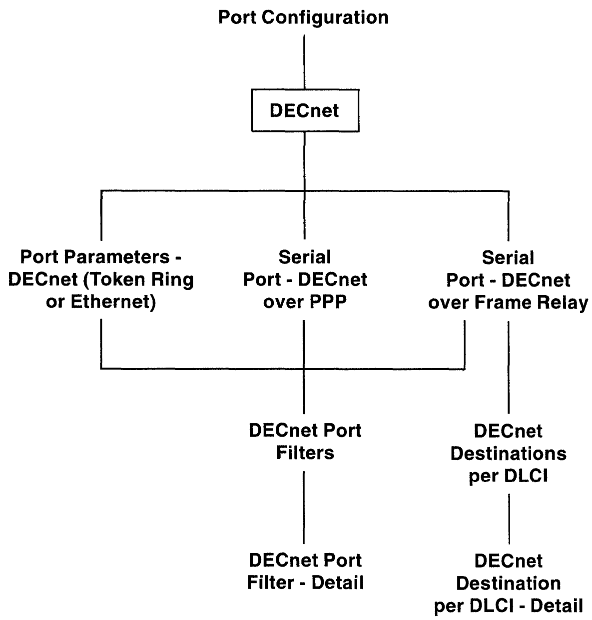


Figure 5-37. Flow of Port Level DECnet Help Windows

To enable adapters to transmit and receive DECnet packets, you need to enable DECnet routing at the port level. *Configure DECnet at the node level first.* Then configure DECnet on each adapter that will transmit and receive DECnet packets.

Use the following tables as worksheets for your port level configurations:

- Port Parameters - DECnet on page 5-270
- Serial Port - DECnet over PPP on page 5-271
- Serial Port - DECnet over Frame Relay on page 5-272
- DECnet Destination per DLCI on page 5-273
- DECnet Filters - Detail on page 5-273

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-8 on page D-10 for a mapping of parameter names and their associated labels.

Table 5-361. Configuration Worksheet - Port Parameters - DECnet

Parameter Information	Your Value
Parameter Enable DECnet routing on this port **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables DECnet on this port.	
Parameter DECnet circuit type **Valid Values** Bilingual, AMA, Phase IV **Default Value** Phase IV **Description** This parameter specifies how the router will run on a given port. The choices are: • Bilingual; communicates with DECnet Phase IV and DECnet Phase IV-Prime routers • AMA (arbitrary MAC address); a DECnet Phase IV-Prime router • DECnet Phase IV; a standard DECnet Phase IV router	
Parameter Router priority **Valid Values** 0 to 127 **Default Value** 64 **Description** This parameter sets the priority for the router on the specified port. DECnet Phase IV and DECnet Phase IV-Prime protocols choose the router whose port has the highest priority to act as the designated router for the attached LAN segment. If you want a particular router to be chosen as the designated router, you need to set the router priorities accordingly.	
Parameter Circuit cost **Valid Values** 1 to 63 **Default Value** 4 **Description** This parameter contains a cost value assigned by the system administrator to optimize network performance. Because the routing layer forwards packets on the least costly path to a destination, a higher cost reduces traffic on the circuit. All hosts on the same segment must share the same value.	
Parameter Hello timer **Valid Values** 1 to 8191 seconds **Default Value** 15 seconds **Description** This parameter specifies how often the 6611 sends Hello messages.	
Parameter Routing timer **Valid Values** 1 to 65 535 seconds **Default Value** 40 seconds **Description** This parameter specifies how often the 6611 sends out network topology updates in the absence of any network changes. When the timer expires for an interface, the 6611 sends a routing message on the interface.	
Parameter Maximum routers **Valid Values** 1 to 1022 **Default Value** 32 **Description** This parameter defines the maximum number of DECnet routers that are allowed on a specific circuit. This parameter must be less than or equal to the node-level Maximum broadcast routers parameter.	

Table 5-362 (Page 1 of 2). Configuration Worksheet - Serial Port - DECnet over PPP

Parameter Information		**Your Value**
Parameter	Enable DECnet routing on this port	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables DECnet on this port.	
Parameter	DECnet circuit type	
Valid Values	Bilingual, AMA, Phase IV	
Default Value	Phase IV	
Description	This parameter specifies how the router will run on a given port. The choices are: • Bilingual; communicates with DECnet Phase IV and DECnet Phase IV-Prime routers • AMA (arbitrary MAC address); a DECnet Phase IV-Prime router • DECnet Phase IV; a standard DECnet Phase IV router	
Parameter	Remote DECnet address	
Valid Values	An address in the form of <area number>.<node number>, where: • Area number is from 1 to 63 • Node number is from 1 to 1023.	
Default Value	None	
Description	This parameter defines the DECnet address of the node at the other end of the serial link.	
Parameter	Remote DECnet node type	
Valid Values	Area, Routing-IV, Endnode	
Default Value	Area	
Description	This parameter defines the node type of the node at the other end of the serial link.	
Parameter	Router priority	
Valid Values	0 to 127	
Default Value	64	
Description	This parameter sets the priority for the router on the specified port. DECnet Phase IV and DECnet Phase IV-Prime protocols choose the router whose port has the highest priority to act as the designated router for the attached LAN segment. If you want a particular router to be chosen as the designated router, you need to set the router priorities accordingly.	
Parameter	Circuit cost	
Valid Values	1 to 63	
Default Value	4	
Description	This parameter contains a cost value assigned by the system administrator to optimize network performance. Because the routing layer forwards packets on the least costly path to a destination, a higher cost reduces traffic on the circuit. All hosts on the same segment must share the same value.	
Parameter	Hello timer	
Valid Values	1 to 8191 seconds	
Default Value	15 seconds	
Description	This parameter specifies how often the 6611 sends hello messages.	
Parameter	Routing timer	
Valid Values	1 to 65535 seconds	
Default Value	180 seconds	
Description	This parameter specifies how often the 6611 sends out network topology updates in the absence of any network changes. When the timer expires for an interface, the 6611 sends a routing message on the interface.	

Table 5-362 (Page 2 of 2). Configuration Worksheet - Serial Port - DECnet over PPP

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Maximum routers 1 to 1022 32 This parameter defines the maximum number of DECnet routers that are allowed on a specific circuit. This parameter must be less than or equal to the node-level Maximum broadcast routers parameter.	

Table 5-363 (Page 1 of 2). Configuration Worksheet - Serial Port - DECnet over Frame Relay

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable DECnet routing on this port Enable, Disable Disable This parameter enables or disables DECnet on this port.	
Parameter **Valid Values** **Default Value** **Description**	DECnet circuit type Bilingual, AMA, Phase IV Phase IV This parameter specifies how the router will run on a given port. The choices are: • Bilingual; communicates with DECnet Phase IV and DECnet Phase IV-Prime routers • AMA (arbitrary MAC address); a DECnet Phase IV-Prime router • DECnet Phase IV; a standard DECnet Phase IV router	
Parameter **Valid Values** **Default Value** **Description**	Router priority 0 to 127 64 This parameter sets the priority for the router on the specified port. DECnet Phase IV and DECnet Phase IV-Prime protocols choose the router whose port has the highest priority to act as the designated router for the attached LAN segment. If you want a particular router to be chosen as the designated router, you need to set the router priorities accordingly.	
Parameter **Valid Values** **Default Value** **Description**	Circuit cost 1 to 63 4 This parameter contains a cost value assigned by the system administrator to optimize network performance. Because the routing layer forwards packets on the least costly path to a destination, a higher cost reduces traffic on the circuit. All hosts on the same segment must share the same value.	
Parameter **Valid Values** **Default Value** **Description**	Hello timer 1 to 8191 seconds 15 seconds This parameter specifies how often the 6611 sends hello messages.	
Parameter **Valid Values** **Default Value** **Description**	Routing timer 1 to 65 535 seconds 180 seconds This parameter specifies how often the 6611 sends out network topology updates in the absence of any network changes. When the timer expires for an interface, the 6611 sends a routing message on the interface.	

Table 5-363 (Page 2 of 2). Configuration Worksheet - Serial Port - DECnet over Frame Relay

Parameter Information	Your Value
Parameter Maximum routers **Valid Values** 1 to 1022 **Default Value** 32 **Description** This parameter defines the maximum number of DECnet routers that are allowed on a specific circuit. This parameter must be less than or equal to the node-level Maximum broadcast routers parameter.	

Table 5-364. Configuration Worksheet - DECnet Destination per DLCI

Parameter Information	Your Value
DECnet Destination per DLCI List - Parameters configured for each destination defined	
Parameter DLCI Number **Valid Values** A valid DLCI number **Default Value** None **Description** This parameter defines the data link control identifier (DLCI) number used to communicate with the destination defined in the Remote DECnet address and Remote DECnet node type parameters.	
Parameter Destination DECnet address **Valid Values** An address in the form of <area number>.<node number>, where: • Area number is from 1 to 63 • Node number is from 1 to 1023 **Default Value** None **Description** This parameter contains the DECnet address of the router at the other end of the serial link.	
Parameter Destination DECnet node type **Valid Values** Area, Routing-IV, Endnode **Default Value** Area **Description** This parameter defines the node type of the node at the other end of the serial link.	

Table 5-365. Configuration Worksheet - DECnet Port Filters

Parameter Information	Your Value
Parameter Enable DECnet filters on this port **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables all DECnet filters defined for this port.	
DECnet Port Filters List Parameters - Configured for each filter defined	
Parameter Filter ID **Valid Values** Any filter ID entered in the list of DECnet packet filters configured for the 6611 **Default Value** None **Description** This parameter identifies which filter is applied on this port.	
Parameter Direction in which packet is moving **Valid Values** Inbound, Outbound, Inbound and Outbound **Default Value** Inbound and Outbound **Description** This parameter identifies the direction in which a packet must be moving in order for DECnet to apply this filter. If you select **Inbound**, this filter applies to all DECnet packets coming into the 6611 through this port. If you select **Outbound**, this filter applies to all DECnet packets going out of the 6611 through this port.	

Internetwork Packet Exchange (IPX)

IPX is a network protocol that Novell** developed to perform routing in the NetWare** environment. Derived from Xerox Network Systems, IPX has become a defacto industry standard in computer networking.

While the 6611 will route native IPX traffic, it will also participate in Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) exchanges in an IPX network. NetBIOS traffic will be bridged.

The 6611 implements several additional features such as:

- NetWare RIP packet filters
- SAP packet filters
- IPX packet filters
- Control of RIP and SAP broadcast intervals and aging on each port
- Staggering of RIP and SAP broadcasts intervals in frame-relay networks
- Override of the tick value used to control IPX routing decisions on the network interface

For more information about the 6611 IPX functions, see the *Introduction and Planning Guide*.

Port Types Supported

Table 5-366. Port Types Supported for IPX Routing

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	Standard Novell	√
		LLC	√
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	√

Terms used by Novell and how they are referenced in this manual, as well as the corresponding protocol identifiers used in Table 5-366 and in the Configuration Program, are shown in Table 5-367 on page 5-275.

Table 5-367. Relationship between Terms Used

Novell Term	6611 Term	Protocol ID Value
Ethernet II	Ethernet Version 2	X'8137'
Ethernet 802.3	IEEE 802.3	None
Ethernet 802.2	IEEE 802.3 LLC	X'E0'
Ethernet SNAP	IEEE 802.3 SNAP	X'000000008137'
Token-Ring	IEEE 802.5 LLC	X'E0'
Token-Ring SNAP	IEEE 802.5 SNAP	X'000000008137'

Restrictions

- When you configure IPX on a token-ring port and use Token-Ring 802.5 LLC encapsulation, you cannot use the SAP value X'E0' to route data link switching traffic.
- When IPX is configured on a frame-relay port with either AppleTalk or a bridging protocol, you must explicitly define the DLCIs that will be used by IPX on the port.

Before You Configure...

The 6611 supports IPX routing for the following WAN topologies in meshed frame-relay and X.25 networks:

- Fully meshed
- Partially meshed

For more information about these topologies, read the *Introduction and Planning Guide*.

How the 6611 Views the Meshed Network

The 6611 IPX implementation views each port that connects to the meshed WAN as a broadcast port. This is to say that regardless of the number of virtual circuits that are attached to that port, the 6611 views the port as one network. Packets destined for the WAN port are broadcast on all virtual circuits attached to that port.

Fully Meshed Networks

A fully meshed network is required to enable any two devices in the network to communicate directly.

Configuration Summary: To configure IPX for a fully meshed network, use the Configuration Program to create a configuration and assign the following values:

- One network number per port, as assigned by the IPX network number parameter, regardless of the number of circuits attached to that port
- Local node address, as statically assigned by the Locally administered address parameter
- Remote node addresses, assigned dynamically using InARP or statically using IPX Destinations per DLCI

Partially Meshed Networks

You can configure IPX routing in a partially meshed network when any-to-any-connectivity is not required by your network *or* when your network does not forward IPX traffic between multiple virtual circuits attached to the same physical port. The 6611 does not forward broadcast traffic or perform intermediate routing between virtual circuits attached to the same physical port. To enable devices that are not directly connected to communicate, intermediate routing must be enabled on the ports that connect these devices to the partially meshed network to forward IPX traffic. To enable intermediate routing, the split horizon function must be disabled on these ports. When the split horizon function is disabled, the network converges at a slower rate.

Partially Meshed Networks Without Intermediate Routing: The configuration of a partially meshed network that does not provide intermediate routing is the same as that of a fully meshed network. See the Configuration Summary under "Fully Meshed Networks" on page 5-275 for more information.

Partially Meshed Networks With Intermediate Routing: To enable the 6611 to perform intermediate routing of IPX, use the Configuration Program to create a configuration and assign the values specified for a fully meshed network. See Configuration Summary under "Fully Meshed Networks" on page 5-275 for more information. Then, on each port that performs intermediate routing, set the Split horizon for RIP/SAP updates parameter to **Off**.

Note: The 6611 does not forward broadcast traffic and cannot perform intermediate routing between virtual circuits attached to the same physical port.

Configuration Changes...

That Require the IPX Function to Restart

- Port-level parameters

  None

- Node-level parameters

  None

That Require the 6611 to Restart

- Port-level parameters
  - Enable IPX routing on this port
  - IPX network number
  - Destination IPX address
  - DLCI number
- Node-level parameters
  - Enable IPX router

Configuration Options

Table 5-368 summarizes the configuration options for each adapter type that supports IPX. After configuring IPX on specific ports, you need to enable IPX routing at the system level.

Table 5-368. IPX Configuration Options

WHEN configuring IPX...	THEN optionally...
...on a token-ring port or an Ethernet port: • Enable IPX on the port. • Enter the IPX network number. • Determine the encapsulation method.	• Define filters for this port. • Enable tick override and specify a tick value to override the tick used by the 6611 to make IPX routing decisions. • Select RIP and SAP broadcasting options.
...on an serial port or a V.35/V.36 Serial Adapter, using PPP: • Enable IPX routing on the port. • Enter the IPX network number. • On the physical interface, enter the locally administered MAC address assigned to this port.	• Define filters for this port. • Enable tick override and specify a tick value to override the tick used by the 6611 to make IPX routing decisions. • Select RIP and SAP broadcasting options.
...on an serial port or a V.35/V.36 Serial Adapter, using Frame Relay: • Enable IPX routing on the port. • Enter the IPX network number. • Define DLCIs assigned to the frame-relay port, and enable InARP *or* define IPX destinations for each DLCI to provide a logical mapping between the DLCI number and the destination IPX address. **Note:** When IPX is configured on a frame-relay port with either AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by IPX on the port. • On the physical interface, enter the locally administered MAC address assigned to this port.	• Define filters for this port. • Enable tick override and specify a tick value to override the tick used by the 6611 to make IPX routing decisions. • Select RIP and SAP broadcasting options. **Notes:** To conserve bandwidth on large frame-relay networks, it is recommended that you: 1. Increase the value of the RIP update interval and the SAP update interval parameters. 2. Enable SAP and RIP pacing when you experience network congestion due to SAP and RIP traffic.
...on a X.25 adapter: • Enable X.25 interface on this port. • Set the Type of line parameter to **DTE** or **DTE back-to-back**. • Enter the locally administered MAC address assigned to this port. • On the Subscription Mapping window, enter the local DTE address. • On the X.25 Port - IPX window, enable IPX routing on the port and enter the IPX network number. • Specify X.25 remote hosts. For each remote host, enter the destination IPX address and the remote DTE address.	• Specify subscription mapping parameters and options. • Specify network tuning options. • Enable tick override and specify a tick value to override the tick used by the 6611 to make IPX routing decisions. • Set the Split horizon for RIP and SAP updates parameter to **Off** to enable intermediate routing in a non-fully meshed X.25 network. • Select RIP and SAP broadcasting options. • Select SVC options.
...at the node level: • Enable the IPX router.	• Define RIP and SAP filters.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform IPX routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-369. IPX Configuration Verification Checklist

IPX Rule	**Configuration Parameter**	√
Node-Level Parameters:		
Ensure that the Enable IPX parameter is enabled.	Enable IPX	
Port-Level Parameters:		
Ensure that the Enable IPX routing on this port parameter is enabled on 2 or more ports on each 6611.	Enable IPX routing on this port	
Ensure that the product of the value of the SAP update interval parameter multiplied by the value of the SAP age multiplier parameter is greater than the value of the SAP update interval for the ports in other IPX routers and servers that are physically attached to the network to which this port is connected.	SAP update interval	
	SAP age multiplier	
Ensure that product of the value of the RIP update interval parameter multiplied by the value of the RIP age multiplier parameter is greater than the value of the RIP update interval for the ports in other IPX routers and servers that are physically attached to the network to which this port is connected.	RIP update interval	
	RIP age multiplier	
To enable an IPX connection, the following parameters must have the same value for both ends of an IPX connection: • The Enable physical interface parameter must be enabled • Media types (token-ring, Ethernet, serial, or X.25) must be the same • For serial connections, the value of the Framing method parameter must be the same and must be enabled • For serial connections, the value of the Serial line speed parameter must be the same	Enable physical interface on this port	
	Framing method	
	Enable Point-to-Point Protocol on this port	
	Enable Frame Relay on this port	
	Serial line speed	
For an IPX connection between token-ring ports or Ethernet ports, ensure that the value of the following parameters is the same for both ends of the IPX connection: • Encapsulation method • IPX network number	Encapsulation method	
	IPX network number	
If the Use InARP to resolve remote protocol addresses parameter is disabled or if the LMI option parameter is set to **None**, ensure that the IPX host addresses match the DLCI destinations and that the values of the following parameters on the local port correspond to the values on the remote port: • Destination IPX address • DLCI number	Use InARP to resolve remote protocol addresses	
	Local Management Interface Option	
	Destination IPX address	
	DLCI number	
	Host address	

Sample Network Graphic

Figure 5-38 on page 5-280 illustrates a network where IPX routing is enabled between workstations and file servers that are located on different LANs. A filter has been configured on 6611 C to prevent the workstations on the token-ring LAN from accessing Server 1.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and IPX over PPP
  - A token-ring port running IP and IPX
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and IPX over PPP
  - A serial port running IP and IPX over frame relay
  - A token-ring port running IP and IPX
  - An Ethernet port running IP and IPX
- 6611 C, which has the following port types and protocols running:
  - A serial port running IP and IPX over frame relay
  - A token-ring port running IP and IPX

The following information is shown in Figure 5-38 on page 5-280:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*
- IPX network numbers (hex)
- Locally administered addresses

Note: The configuration of the IP protocol is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to route IPX.

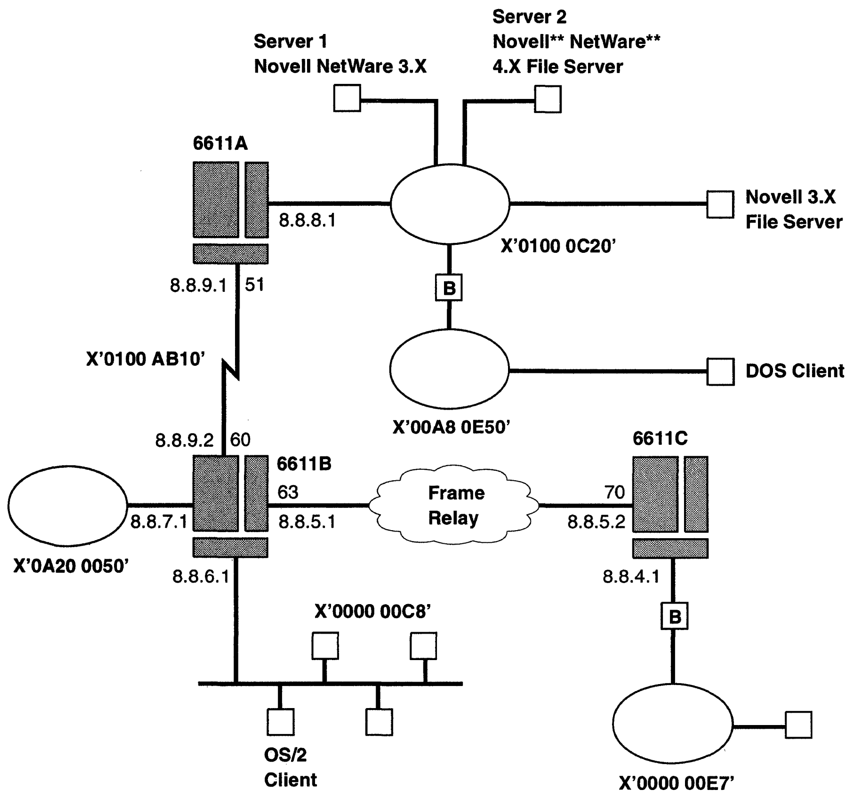


Figure 5-38. Sample Network for Routing IPX

This sample network shows the configuration for:

- IPX routing
- IPX filtering
- Serial, token-ring, and Ethernet ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-38. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 5-370. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Data link protocol	PPP	PPP	Frame Relay	Frame Relay

Table 5-371. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None	None	None
Transmit clock source	DTE	DTE	DTE	DTE
Serial line speed	19200	19200	19200	19200
Data encoding	NRZI	NRZI	NRZI	NRZI
Locally administered MAC address	51	60	63	70
Enable port for transmission group	Disable	Disable	Disable	Disable
Transmission group name	None	None	None	None

Table 5-372. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-373. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.9.1	8.8.9.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.9.2	8.8.9.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	Disable	Disable
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-374. Serial Port - IPX over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IPX routing on this port	Enable	Enable
IPX network number	0100AB10	0100AB10
Tick override	Disable	Disable
Tick value	NA	NA
Control RIP and SAP broadcasting		
SAP update interval	30	30
SAP age multiplier	4	4
RIP update interval	30	30
RIP age multiplier	4	4
Inbound Port Filters	Disable	Disable

Table 5-375. Serial Port - Frame-Relay Parameters Configured

Parameter	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Enable Frame Relay on this port	Enable	Enable
Polling interval	10	10
Full inquiry interval	6	6
LMI option	ANSI T1.617 Annex D	ANSI T1.617 Annex D
Use InARP to resolve remote protocol addresses	Enable	Enable
DLCIs assigned to this port	None	None

Table 5-376. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.5.1	8.8.5.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Disable	Disable
Point-to-point only	Disable	Disable
Assignment for discovered DLCIs	Mesh	Mesh
IP Priority	Disable	Disable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-377. Serial Port - IPX over Frame-Relay Parameters Configured

Parameter	6611 B Slot 2 Port 2 Value	6611 C Slot 1 Port 2 Value
Enable IPX routing on this port	Enable	Enable
Enable IPXWAN	Enable	Enable
IPX network number	00A80E50	00A80E50
Inbound Port Filters	Disable	Disable

Token-Ring Ports and Protocols Running on Them

Table 5-378. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 3 Value	6611 C Slot 2 Value
Enable physical interface on this port	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA
MAC address format	NA	NA	NA
Token ring data rate	4 Mbps	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local	Non-local

Table 5-379. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 3 Value	6611 C Slot 2 Value
Enable IP routing on this port	Enable	Enable	Enable
IP address	8.8.8.1	8.8.7.1	8.8.4.1
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492	1492
Enable ICMP address mask requests	Enable	Enable	Enable
Inbound Port Filters	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable

Table 5-380. Token-Ring Port - IPX Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 3 Value	6611 C Slot 2 Value
Enable IPX routing on this port	Enable	Enable	Enable
IPX network number	00100C20	0A200050	000000E7
Encapsulation method	Token-Ring 802.5 LLC	Token-Ring 802.5 LLC	Token-Ring 802.5 LLC
Tick override	Disable	Disable	Disable
Tick value	NA	NA	NA
Control RIP and SAP broadcasting			
SAP update interval	1	1	1
SAP age multiplier	4	4	4
RIP update interval	1	1	1
RIP age multiplier	4	4	4
Inbound Port Filters	Disable	Disable	Disable

Ethernet Port and the Protocols Running on It

Table 5-381. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 4 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	None
Enable additional multicast addresses	Disable
Multicast MAC address	None

Table 5-382. Ethernet Port - IP Parameters Configured

Parameter	6611 B Slot 4 Value
Enable IP routing on this port	Enable
IP address	8.8.6.1
Subnet mask	255.255.255.0
Max. transmission unit (octets)	1500
Ethernet framing for IP	Ethernet V2.0
Enable ICMP address mask requests	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Table 5-383. Ethernet Port - IPX Parameters Configured

Parameter	6611 B Slot 4 Value
Enable IPX routing on this port	Enable
IPX network number	000000C8
Encapsulation method	Ethernet 802.3
Tick override	Disable
Tick value	NA
Control SAP and RIP broadcasting	
SAP update interval	1
SAP age multiplier	4
RIP update interval	1
RIP age multiplier	4
Inbound Port Filters	Disable

Node-Level Parameters Configured

Table 5-384. Node Level - IPX Routing Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value
Enable IPX router	Enable	Enable	Enable
SAP Filters	Disable	Disable	Enable
RIP Router Filters	Disable	Disable	Disable
Inbound RIP Filters	Disable	Disable	Disable
Outbound RIP Filters	Disable	Disable	Disable

Table 5-385. Node Level - IPX SAP Filter Parameters Configured

Parameter	6611 C Value
Enable SAP Filters	Enable
Filtering mode	Deny
SAP Filter List Parameters - Configured for each SAP filter defined	
Filter ID	1
Server type	All server types
Type	NA
Network number	All networks
Network	NA
Server name	All servers
Name	NA

Port Level Worksheets

Figure 5-39 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-39.

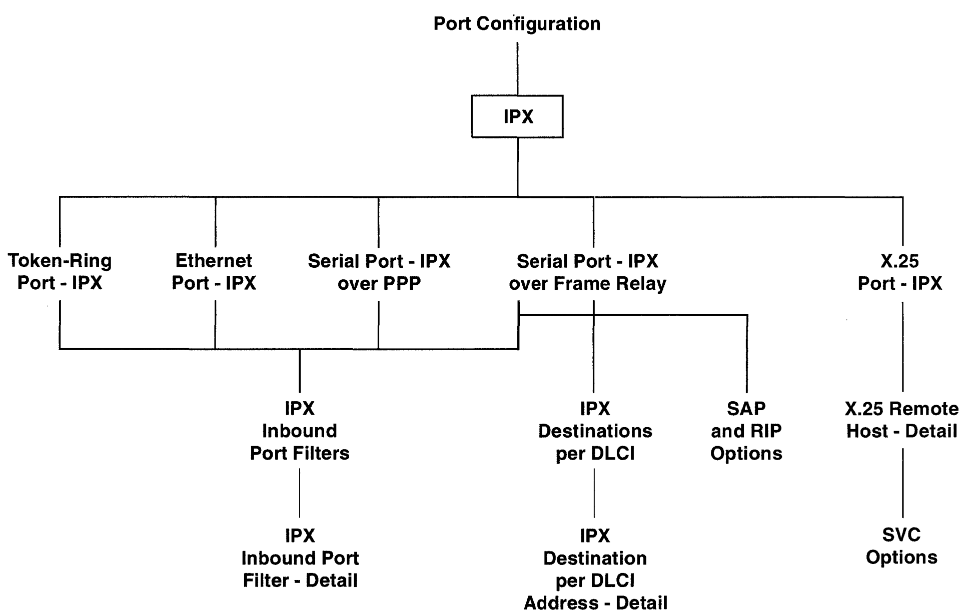


Figure 5-39. Flow of Port Level IPX Help Windows

To enable adapters to transmit and receive IPX packets, you need to enable IPX routing at the port level. Configure IPX on each adapter that will transmit and receive IPX packets. Then configure IPX at the node level.

Use the following tables as worksheets for your port level configurations:

- Token-Ring Port - IPX on page 5-286
- Ethernet Port - IPX on page 5-287
- Serial Port - IPX over PPP on page 5-289
- Serial Port - IPX over Frame Relay on page 5-290
- SAP and RIP Options on page 5-290
- IPX Destination per DLCI - Detail on page 5-292
- X.25 Port - IPX on page 5-292
- X.25 Port - IPX on page 5-293
- SVC Options on page 5-294
- IPX Inbound Port Filters on page 5-296

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-14 on page D-13 for a mapping of parameter names and their associated labels.

Table 5-386 (Page 1 of 2). Configuration Worksheet - Token-Ring Port - IPX

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable IPX routing on this port Enable, Disable Disable This parameter enables or disables Internetwork Packet Exchange (IPX) routing on this port.	
Parameter **Valid Values** **Default** **Description**	IPX network number (required) X'0000 0001' to X'FFFF FFFE' None This parameter assigns an IPX network number to the physical network attached to this port.	
Parameter **Valid Values** **Default** **Description**	Encapsulation method Token-Ring 802.5 LLC, Token-Ring 802.5 SNAP Token-Ring 802.5 LLC This parameter determines the logical link control (LLC) encapsulation method used to transmit IPX packets. Only one value can be chosen.	
Parameter **Valid Values** **Default** **Description**	Tick override Enable, Disable Disable When this parameter is set to **Enable**, the 6611 uses the tick value specified in the Tick value parameter for this port. When this parameter is set to **Disable**, the 6611 uses a default tick value of 1 (1/18 of a second) for the attached LAN.	

Table 5-386 (Page 2 of 2). Configuration Worksheet - Token-Ring Port - IPX

Parameter Information	Your Value
Parameter Tick value **Valid Values** 1 to 65535, in 1/18 second intervals **Default** None **Description** This parameter specifies a tick value for the IPX port that overrides the default tick value used by the 6611 to make IPX routing decisions. You can specify this parameter only when the Tick override parameter is enabled. A tick is a rough estimate of the delay for a maximum-sized IPX packet to travel to any neighbor from this port. Each tick is 1/18 of a second. By overriding the default tick value, you can control the selection of IPX routes through the 6611. For example, if parallel routes exist to a neighbor router, you could increase the tick value on one of the parallel IPX ports. The route through the port with the increased tick value would be treated as a lower-priority route and the route through the other port would be learned. If the higher-priority route becomes unavailable, the 6611 must discover the lower-priority route again.	
Control SAP and RIP Broadcasting	
Parameter SAP update interval **Valid Values** 1 to 136 minutes **Default** 1 minute **Description** This parameter specifies how often the 6611 broadcasts server information table updates over the port.	
Parameter SAP age multiplier **Valid Values** 1 to 65535 **Default** 4 **Description** This parameter specifies the number of Service Access Protocol (SAP) update intervals that may elapse before unrefreshed SAP information is considered to have expired. The life span of SAP information is equal to the value of this parameter times the value of the SAP update interval parameter.	
Parameter RIP update interval **Valid Values** 1 to 136 minutes **Default** 1 minute **Description** This parameter specifies how often the 6611 router broadcasts routing table updates over the port.	
Parameter RIP age multiplier **Valid Values** 1 to 65535 **Default** 4 **Description** This parameter specifies the number of Routing Information Protocol (RIP) update intervals that may elapse before unrefreshed RIP information is considered to have expired. The life span of RIP information is equal to the value of this parameter times the value of the RIP update interval parameter.	

Table 5-387 (Page 1 of 3). Configuration Worksheet - Ethernet Port - IPX

Parameter Information	Your Value
Parameter Enable IPX routing on this port **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables IPX routing on this port.	

Table 5-387 (Page 2 of 3). Configuration Worksheet - Ethernet Port - IPX

Parameter Information		Your Value
Parameter	IPX network number (required)	
Valid Values	X'0000 0001' to X'FFFF FFFE'	
Default	None	
Description	This parameter assigns an IPX network number to the physical network attached to this port.	
Parameter	Encapsulation method	
Valid Values	Ethernet V2.0, Ethernet 802.3 SNAP, Ethernet 802.3, Ethernet 802.2	
Default	Ethernet 802.3	
Description	This parameter determines the encapsulation method used to transmit IPX packets on this Ethernet port. Only one value can be chosen.	
Parameter	Tick override	
Valid Values	Enable, Disable	
Default	Disable	
Description	When this parameter is set to **Enable**, the 6611 uses the tick value specified in the Tick value parameter for this port. When this parameter is set to **Disable**, the 6611 uses a default tick value of 1 (1/18 of a second) for the attached LAN.	
Parameter	Tick value	
Valid Values	1 to 65 535, in 1/18 second intervals	
Default	None	
Description	This parameter specifies a tick value for the IPX port that overrides the default tick value used by the 6611 to make IPX routing decisions. You can specify this parameter only when the Tick override parameter is enabled. A tick is a rough estimate of the delay for a maximum-sized IPX packet to travel to any neighbor from this port. Each tick is 1/18 of a second. By overriding the default tick value, you can control the selection of IPX routes through the 6611. For example, if parallel routes exist to a neighbor router, you could increase the tick value on one of the parallel IPX ports. The route through the port with the increased tick value would be treated as a lower-priority route and the route through the other port would be learned. If the higher-priority route becomes unavailable, the 6611 must discover the lower-priority route again.	
Control RIP and SAP Broadcasting		
Parameter	SAP update interval	
Valid Values	1 to 136 minutes	
Default	1 minute	
Description	This parameter specifies how often the 6611 broadcasts server information table updates over the port.	
Parameter	SAP age multiplier	
Valid Values	1 to 65 535	
Default	4	
Description	This parameter specifies the number of SAP update intervals that may elapse before unrefreshed SAP information is considered to have expired. The life span of SAP information is equal to the value of this parameter times the value of the SAP update interval parameter.	
Parameter	RIP update interval	
Valid Values	1 to 136 minutes	
Default	1 minute	
Description	This parameter specifies how often the 6611 router broadcasts routing table updates over the port.	

Table 5-387 (Page 3 of 3). Configuration Worksheet - Ethernet Port - IPX

Parameter Information		Your Value
Parameter	RIP age multiplier	
Valid Values	1 to 65 535	
Default	4	
Description	This parameter specifies the number of RIP update intervals that may elapse before unrefreshed RIP information is considered to have expired. The life span of RIP information is equal to the value of this parameter times the value of the RIP update interval parameter.	

Table 5-388 (Page 1 of 2). Configuration Worksheet - Serial Port - IPX over PPP

Parameter Information		Your Value
Parameter	Enable IPX routing on this port	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables IPX routing on this port.	
Parameter	IPX network number (required)	
Valid Values	X'0000 0001' to X'FFFF FFFE'	
Default	None	
Description	This parameter assigns an IPX network number to the physical network attached to this port.	
Parameter	Tick override	
Valid Values	Enable, Disable	
Default	Disable	
Description	When this parameter is set to **Enable**, the 6611 uses the tick value specified in the Tick value parameter for this port. When this parameter is set to **Disable**, the 6611 uses a default tick value of 1 (1/18 of a second) for the attached WAN.	
Parameter	Tick value	
Valid Values	1 to 65 535, in 1/18 second intervals	
Default	None	
Description	This parameter specifies a tick value for the IPX port that overrides the default tick value used by the 6611 to make IPX routing decisions. You can specify this parameter only when the Tick override parameter is enabled. A tick is a rough estimate of the delay for a maximum-sized IPX packet to travel to any neighbor from this port. Each tick is 1/18 of a second. By overriding the default tick value, you can control the selection of IPX routes through the 6611. For example, if parallel routes exist to a neighbor router, you could increase the tick value on one of the parallel IPX ports. The route through the port with the increased tick value would be treated as a lower-priority route and the route through the other port would be learned. If the higher-priority route becomes unavailable, the 6611 must discover the lower-priority route again.	
Control RIP and SAP Broadcasting		
Parameter	SAP update interval	
Valid Values	1 to 136 minutes	
Default	1 minute	
Description	This parameter specifies how often the 6611 broadcasts server information table updates over the port.	

Table 5-388 (Page 2 of 2). Configuration Worksheet - Serial Port - IPX over PPP

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	SAP age multiplier 1 to 65535 4 This parameter specifies the number of SAP update intervals that may elapse before unrefreshed SAP information is considered to have expired. The life span of SAP information is equal to the value of this parameter times the value of the SAP update interval parameter.	
Parameter **Valid Values** **Default** **Description**	RIP update interval 1 to 136 minutes 1 minute This parameter specifies how often the 6611 router broadcasts routing table updates over the port.	
Parameter **Valid Values** **Default** **Description**	RIP age multiplier 1 to 65535 4 This parameter specifies the number of RIP update intervals that may elapse before unrefreshed RIP information is considered to have expired. The life span of RIP information is equal to the value of this parameter times the value of the RIP update interval parameter.	

Table 5-389. Configuration Worksheet - Serial Port - IPX over Frame Relay

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable IPX routing on this port Enable, Disable Disable This parameter enables or disables IPX routing on this port.	
Parameter **Valid Values** **Default** **Description**	IPX network number (required) X'0000 0001' to X'FFFF FFFE' None This parameter assigns an IPX network number to the physical network attached to this port.	

Table 5-390 (Page 1 of 3). Configuration Worksheet - Serial Port - SAP and RIP Options (Frame Relay Ports)

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Tick override Enable, Disable Disable When this parameter is set to **Enable**, the 6611 uses the tick value specified in the Tick value parameter for this port. When this parameter is set to **Disable**, the 6611 uses a default tick value of 1 (1/18 of a second) for the attached WAN.	

Table 5-390 (Page 2 of 3). Configuration Worksheet - Serial Port - SAP and RIP Options (Frame Relay Ports)

Parameter Information		Your Value
Parameter	Tick value	
Valid Values	1 to 65 535, in 1/18 second intervals	
Default	None	
Description	This parameter specifies a tick value for the IPX port that overrides the default tick value used by the 6611 to make IPX routing decisions. You can specify this parameter only when the Tick override parameter is enabled. A tick is a rough estimate of the delay for a maximum-sized IPX packet to travel to any neighbor from this port. Each tick is 1/18 of a second. By overriding the default tick value, you can control the selection of IPX routes through the 6611. For example, if parallel routes exist to a neighbor router, you could increase the tick value on one of the parallel IPX ports. The route through the port with the increased tick value would be treated as a lower-priority route and the route through the other port would be learned. If the higher-priority route becomes unavailable, the 6611 must discover the lower-priority route again.	
Control RIP and SAP Broadcasting		
Parameter	Enable SAP and RIP pacing	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter specifies how the 6611 should handle the pacing of RIP and SAP broadcasts over frame-relay connections. Normally SAP and RIP broadcasts are sent out in periodic bursts, which can temporarily interrupt the flow of other traffic across the frame-relay DLCIs used by IPX. When this parameter is enabled, the 6611 staggers the transmission of individual RIP and SAP broadcasts. The broadcasts are transmitted at periodically throughout the update interval over the frame relay connection.	
Parameter	Split horizon for RIP and SAP updates	
Valid Values	On, Poison Reverse, Off	
Default	On	
Description	This parameter specifies how the 6611 should advertise Internetwork Protocol Exchange (IPX) Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) information.	
Parameter	SAP update interval	
Valid Values	1 to 136 minutes	
Default	1 minute	
Description	This parameter specifies how often the 6611 broadcasts server information table updates over the port.	
Parameter	SAP age multiplier	
Valid Values	1 to 65 535	
Default	4	
Description	This parameter specifies the number of SAP update intervals that may elapse before unrefreshed SAP information is considered to have expired. The life span of SAP information is equal to the value of this parameter times the value of the SAP update interval parameter.	
Parameter	RIP update interval	
Valid Values	1 to 136 minutes	
Default	1 minute	
Description	This parameter specifies how often the 6611 router broadcasts routing table updates over the port.	

Table 5-390 (Page 3 of 3). Configuration Worksheet - Serial Port - SAP and RIP Options (Frame Relay Ports)

Parameter Information		Your Value
Parameter	RIP age multiplier	
Valid Values	1 to 65 535	
Default	4	
Description	This parameter specifies the number of RIP update intervals that may elapse before unrefreshed RIP information is considered to have expired. The life span of RIP information is equal to the value of this parameter times the value of the RIP update interval parameter.	

Table 5-391. Configuration Worksheet - IPX Destination per DLCI - Detail

Parameter Information		Your Value
IPX Destination List - Parameters configured for each destination defined		
Parameter	Destination IPX address	
Valid Values	X'0000 0000 0000' to X'FFFF FFFF FFFE'	
Default	None	
Description	This parameter defines the IPX address for this DLCI connection on this serial port.	
Parameter	DLCI number (required for each DLCI pair defined)	
Valid Values	A selection from the drop-down list (if the list is empty, then no DLCIs have been configured)	
Default	None	
Description	This parameter defines the DLCI number that provides a logical connection to a router with an IPX address specified in the Destination IPX address parameter.	

Table 5-392 (Page 1 of 2). Configuration Worksheet - X.25 Port - IPX

Parameter Information		Your Value
Parameter	Enable IPX routing on this port	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables IPX routing on this port.	
Parameter	IPX network number (required)	
Valid Values	X'0000 0001' to X'FFFF FFFE'	
Default	None	
Description	This parameter assigns an IPX network number to the physical network attached to this port.	
Parameter	Tick override	
Valid Values	Enable, Disable	
Default	Disable	
Description	When this parameter is set to **Enable**, the 6611 uses the tick value specified in the Tick value parameter for this port. When this parameter is set to **Disable**, the 6611 uses a default tick value of 1 (1/18 of a second) for the attached WAN.	

Table 5-392 (Page 2 of 2). Configuration Worksheet - X.25 Port - IPX

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Tick value 1 to 65 535, in 1/18 second intervals None This parameter specifies a tick value for the IPX port that overrides the default tick value used by the 6611 to make IPX routing decisions. You can specify this parameter only when the Tick override parameter is enabled. A tick is a rough estimate of the delay for a maximum-sized IPX packet to travel to any neighbor from this port. Each tick is 1/18 of a second. By overriding the default tick value, you can control the selection of IPX routes through the 6611. For example, if parallel routes exist to a neighbor router, you could increase the tick value on one of the parallel IPX ports. The route through the port with the increased tick value would be treated as a lower-priority route and the route through the other port would be learned. If the higher-priority route becomes unavailable, the 6611 must discover the lower-priority route again.	
Parameter **Valid Values** **Default** **Description**	Split horizon for RIP and SAP updates On, Poison Reverse, Off On This parameter specifies how the 6611 should advertise Internetwork Protocol Exchange (IPX) Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) information.	
Parameter **Valid Values** **Default** **Description**	SAP update interval 1 to 136 minutes 1 minute This parameter specifies how often the 6611 broadcasts server information table updates over the port.	
Parameter **Valid Values** **Default** **Description**	SAP age multiplier 1 to 65 535 4 This parameter specifies the number of SAP update intervals that may elapse before unrefreshed SAP information is considered to have expired. The life span of SAP information is equal to the value of this parameter times the value of the SAP update interval parameter.	
Parameter **Valid Values** **Default** **Description**	RIP update interval 1 to 136 minutes 1 minute This parameter specifies how often the 6611 router broadcasts routing table updates over the port.	
Parameter **Valid Values** **Default** **Description**	RIP age multiplier 1 to 65 535 4 This parameter specifies the number of RIP update intervals that may elapse before unrefreshed RIP information is considered to have expired. The life span of RIP information is equal to the value of this parameter times the value of the RIP update interval parameter.	

Table 5-393 (Page 1 of 2). Configuration Worksheet - X.25 Remote Host - Detail

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Destination IPX address for X.25 A 12-byte address, X'0000 0000 0001' to X'FFFF FFFF FFFE' None This is the destination IPX host address to map to an X.25 virtual circuit.	

Table 5-393 (Page 2 of 2). Configuration Worksheet - X.25 Remote Host - Detail

Parameter Information		**Your Value**
Parameter	Virtual circuit type	
Valid Values	SVC, PVC	
Default Value	SVC	
Description	This parameter defines the type of virtual circuit to be associated with the Destination IPX address for X.25 parameter.	
SVC Only		
Parameter	Remote DTE address (required when the Virtual circuit type parameter is set to **SVC**)	
Valid Values	1 to 15 decimal digits	
Default Value	None	
Description	This parameter defines the X.25 address of the remote DTE.	
PVC Only		
Parameter	Logical channel number	
Valid Values	The range must lie between the value of the Lowest logical channel number for a PVC parameter and the value of the equation (from these parameters) [Lowest logical channel number for a PVC + Number of logical channels for PVCs - 1]	
Default Value	The value of the Lowest logical channel number for a PVC parameter.	
Description	Use this parameter to enter the logical channel number of the PVC that will be used to communicate with the remote host.	

Table 5-394 (Page 1 of 2). Configuration Worksheet - SVC Options

Parameter Information		**Your Value**
Parameter	Single LCN session	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter specifies the single logical channel number (LCN) session capability for the IPX protocol defined on this X.25 port.	
Parameter	Recall time	
Valid Values	0 to 254 seconds	
Default Value	60 seconds	
Description	This field defines the amount of time (in seconds) that will elapse before another Call Request is made by this port after a Clear is received for the previous Call attempt.	
Parameter	SVC inactivity timer	
Valid Values	0 to 65 535 seconds	
Default Value	0 seconds	
Description	This parameter specifies the amount of time (in seconds) that this virtual circuit remains idle or inactive before a Clear command is issued to close the circuit. A value of 0 implies an infinite timer.	
Parameter	Receive packet size	
Valid Values	64, 128, 256, 512, 1024, 2048, 4096, None (The values 2048 and 4096 are allowed only if the CCITT Support parameter is set to **1984**.)	
Default Value	None	
Description	This parameter defines the desired receive packet size to be used with this virtual circuit.	

Table 5-394 (Page 2 of 2). Configuration Worksheet - SVC Options

Parameter Information	Your Value
Parameter Transmit packet size **Valid Values** 64, 128, 256, 512, 1024, 2048, 4096, None (The values 2048 and 4096 are allowed only if the CCITT support parameter is set to **1984**.) **Default Value** None **Description** This parameter defines the desired transmit packet size to be used with this virtual circuit.	
Parameter Receive packet window size **Valid Values** If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31 **Default Value** None **Description** This parameter represents the desired receive packet window size for this SVC. Answer this parameter only if you are subscribed to the Flow control parameter negotiation facility.	
Parameter Transmit packet window size **Valid Values** If the Packet modulo parameter is set to 8: 1 to 7 If the Packet modulo parameter is set to 128: 1 to 31 **Default Value** None **Description** This parameter represents the desired transmit packet window size for this SVC. Answer this parameter only if you are subscribed to the Flow control parameter negotiation facility.	
Parameter Closed user group (CUG) index **Valid Values** 00 through 99, or 0000 through 9999 **Default Value** None **Description** This parameter defines the closed user group (CUG) index. The basic format of a CUG is 2 decimal digits. The extended format of a CUG is 4 decimal digits and is allowed only when the CCITT support parameter is set to **1984**.	
Parameter Closed user group (CUG) with outgoing access index **Valid Values** 00 through 99, or 0000 through 9999 **Default Value** None **Description** This parameter defines the index of the CUG with outgoing access. The basic format of a CUG is 2 decimal digits. The extended format of a CUG is 4 decimal digits and is allowed only when the CCITT support parameter is set to **1984**.	
Parameter RPOA indices **Valid Values** Up to 10 indexes, each index being 4 decimal digits (up to 40 characters can be entered) **Default Value** None **Description** This parameter defines the data network identification code or codes identifying the requested Recognized Private Operating Agency (RPOA) transit network.	
Parameter User-defined facilities **Valid Values** 0 to 16 hexadecimal digits **Default Value** None **Description** This parameter defines the optional user-defined facilities to be used in the call request packet. Facilities other than the listed parameters can be included in the call request packets by coding them in this parameter.	

Table 5-395 (Page 1 of 2). Configuration Worksheet - IPX Inbound Port Filters

Parameter Information		**Your Value**
Parameter	Enable inbound port filters	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all IPX filters defined on this port.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default	Deny	
Description	This parameter determines the filtering mode for all IPX inbound port filters defined on this port.	
IPX Port Filter List - Parameters configured for each port filter defined		
Parameter	Filter ID (required for each IPX port filter defined)	
Valid Values	1 to 10	
Default	None	
Description	This parameter uniquely defines this filter in a list of filters.	
Parameter	Filter based on hop count	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter allows IPX packets to be filtered based on hop count.	
Parameter	Relational compare operator	
Valid Values	equal to, less than, less than or equal to, greater than, greater than or equal to	
Default	equal to	
Description	This parameter is used as the relational operator when filtering is based on hop count.	
Parameter	Hop count value	
Valid Values	X'0' to X'F'	
Default	None	
Description	This parameter defines the hop count value used to filter IPX packets.	
Parameter	Filter on packet type	
Valid Values	Enable, Disable	
Default	None	
Description	This parameter allow IPX packets to be filtered based on the packet type.	
Parameter	Packet type value	
Valid Values	X'00' to X'FF'	
Default	None	
Description	This parameter defines the packet type value used to filter IPX packets.	
Parameter	Filter based on destination network	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter allows IPX packets to be filtered based on the destination network value.	
Parameter	Destination network value	
Valid Values	X'0000 0000' to X'FFFF FFFF'	
Default	None	
Description	This parameter defines the destination network value used to filter IPX packets.	
Parameter	Filter based on source network	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter allows IPX packets to be filtered on the source network.	

Table 5-395 (Page 2 of 2). Configuration Worksheet - IPX Inbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Source network value X'0000 0000' to X'FFFF FFFF' None This parameter defines the source network value used to filter IPX packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on destination host Enable, Disable Disable This parameter enables or disables the filtering of IPX packets based on the destination host value.	
Parameter **Valid Values** **Default** **Description**	Destination host value X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the destination host value used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on source host Enable, Disable Disable This parameter enables or disables the filtering of IPX packets based on the source host value.	
Parameter **Valid Values** **Default** **Description**	Source host value X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the source host value used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on destination socket Enable, Disable Disable This parameter enables or disables the filtering of IPX packets based on the destination socket value.	
Parameter **Valid Values** **Default** **Description**	Destination socket value X'0000' to X'FFFF' None This parameter defines the destination socket value used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on source socket Enable, Disable Disable This parameter enables or disables the filtering of IPX packets based on the source socket value.	
Parameter **Valid Values** **Default** **Description**	Source socket value X'0000' to X'FFFF' None This parameter defines the source socket value used for filtering packets.	

Note: A maximum of 10 IPX port filters can be configured for each port.

Node Level Worksheets

Figure 5-40 on page 5-298 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-40 on page 5-298.

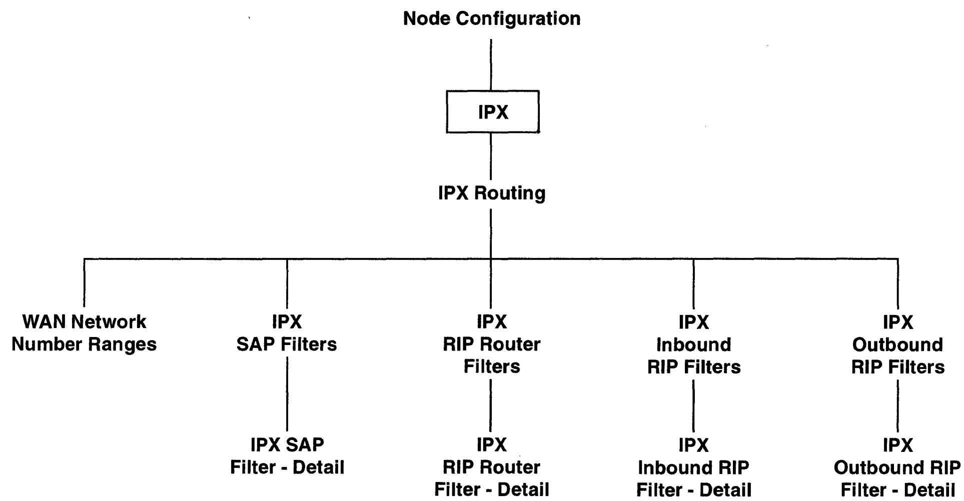


Figure 5-40. Flow of Node Level IPX Help Windows

To enable the 6611 to route IPX packets across network, you need to enable IPX routing at the node level. Use the following tables as worksheets for your node level configuration.

- IPX Routing on page 5-298
- IPX SAP Filter on page 5-298
- IPX RIP Router Filters on page 5-299
- IPX Inbound RIP Filters on page 5-300
- IPX Outbound RIP Filters on page 5-301

Table 5-396. Configuration Worksheet - IPX Routing

Parameter Information		Your Value
Parameter	Enable IPX router	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all ports configured for IPX.	

Table 5-397 (Page 1 of 2). Configuration Worksheet - IPX SAP Filter

Parameter Information		Your Value
Parameter	Enable SAP filters	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all IPX SAP filters defined on this 6611.	
Parameter	Filtering mode	
Valid Values	Permit, Deny	
Default	Deny	
Description	This parameter determines the filtering mode for all IPX SAP filters defined on this 6611.	
IPX SAP Filter List - Parameters configured for each filter defined		
Parameter	Filter ID (required for each SAP filter defined)	
Valid Values	1 to 128	
Default	None	
Description	This parameter specifies the ID of a system-level IPX SAP filter (an IPX filter that is applied to inbound SAP traffic received on the specified adapter ports).	

Table 5-397 (Page 2 of 2). Configuration Worksheet - IPX SAP Filter

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Local IPX network number to filter on All networks, Enter network number All networks This parameter determines if the specified SAP filter is applied on all adapter slots and ports or on a specified adapter slot and port.	
Parameter **Valid Values** **Default** **Description**	Network number X'0000 0001' to X'FFFF FFFE' None This parameter identifies the adapter slot and port on which the SAP filter is applied.	
Parameter **Valid Values** **Default** **Description**	Server type Enter server type, All server types All server types This parameter determines whether SAP information is filtered for all server types or for a specific server type.	
Parameter **Valid Values** **Default** **Description**	Type X'0001' to X'FFFE' (see Novell documentation for the type value) None This parameter defines the IPX server type whose SAP information is filtered.	
Parameter **Valid Values** **Default** **Description**	Server name All servers, Enter server name All servers This parameter determines whether SAP information is filtered for all servers, a subset of servers (using wildcard characters), or a specific server.	
Parameter **Valid Values** **Default** **Description**	Name A string of 1 to 47 ASCII characters (from X'20' through X'7E'), with exception of the following special characters: plus (+), comma (,), semicolon (;), colon (:), slash (/), and back slash (\). The question mark (?) and asterisk (*) characters serve as wildcard characters. The question mark may be used multiple times to represent any single character within the server name. The asterisk may be used multiple times to represent any portion of the server name. The question mark and asterisk may also be used together. None This parameter determines the name of the IPX server whose SAP information is filtered.	

Note: A maximum of 128 SAP filters can be configured for this 6611.

Table 5-398 (Page 1 of 2). Configuration Worksheet - IPX RIP Router Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable RIP router filters Enable, Disable Disable This parameter enables or disables all IPX RIP router filters defined on this 6611.	

Table 5-398 (Page 2 of 2). Configuration Worksheet - IPX RIP Router Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Filtering mode Permit, Deny Deny This parameter determines the filtering mode for all IPX RIP router filters defined on this 6611.	
IPX RIP Router Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required for each RIP router filter defined) 1 to 128 None This parameter specifies the ID of a node-level IPX RIP router filter (an IPX filter that is applied to inbound RIP traffic received on the specified adapter ports).	
Parameter **Valid Values** **Default** **Description**	Network numbers to filter on All networks, Enter network number All networks This parameter determines whether routing information is filtered for all networks, or for a specific network.	
Parameter **Valid Values** **Default** **Description**	Network number X'0000 0000' to X'FFFF FFFE' None This parameter defines the network number of the router whose routing information is filtered.	
Parameter **Valid Values** **Default** **Description**	Host addresses to filter on All hosts, Enter host address All hosts This parameter determines whether routing information is filtered for all hosts or for specific a host address.	
Parameter **Valid Values** **Default** **Description**	Host address X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the host address of the router whose routing information is filtered.	

Note: A maximum of 128 RIP router filters can be configured for this 6611.

Table 5-399 (Page 1 of 2). Configuration Worksheet - IPX Inbound RIP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable inbound RIP filters Enable, Disable Disable This parameter enables or disables all inbound RIP filters defined on this 6611.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Permit, Deny Deny This parameter determines the filtering mode for all inbound RIP filters defined on this 6611.	
IPX Inbound RIP Filter List - Parameters configured for each filter defined		

Table 5-399 (Page 2 of 2). Configuration Worksheet - IPX Inbound RIP Filters

Parameter Information		Your Value
Parameter	Filter ID (required for each inbound RIP filter defined)	
Valid Values	1 to 128	
Default	None	
Description	This parameter specifies the ID of a node-level IPX inbound RIP filter (an IPX filter that is applied to inbound RIP traffic received on the specified adapter ports).	
Parameter	Local IPX network to filter on (required for each inbound RIP router filter defined)	
Valid Values	A selection from the drop-down list (if the list is empty, no interface has been configured for IPX)	
Default	None	
Description	This parameter determines if routing information for a network is filtered on all local interfaces configured for IPX, or on an interface selected from the list displayed in the Configuration Program.	
Parameter	Network numbers to filter on	
Valid Values	All networks, Enter network number	
Default	All networks	
Description	This parameter determines if routing information in the RIP response packet is filtered for all networks or for specific networks.	
Parameter	Network number	
Valid Values	X'0000 0000' to X'FFFF FFFE'	
Default	None	
Description	This parameter identifies the specific IPX network number on which the routing information in the RIP response packet is filtered.	

Note: A maximum of 128 inbound RIP filters can be configured for this 6611.

Table 5-400 (Page 1 of 2). Configuration Worksheet - IPX Outbound RIP Filters

Parameter Information		Your Value
Parameter	Enable outbound RIP filters	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all outbound RIP filters defined on this 6611.	
Parameter	Filtering mode	
Valid Values	Permit, Deny	
Default	Deny	
Description	This parameter determines the filtering mode for all outbound RIP filters defined on this 6611.	
IPX Outbound RIP Filter List - Parameters configured for each filter defined		
Parameter	Filter ID (required for each outbound RIP filter defined)	
Valid Values	1 to 128	
Default	None	
Description	This parameter specifies the ID of a node-level IPX outbound RIP filter (an IPX filter that is applied to outbound RIP traffic received on the specified adapter ports).	

Table 5-400 (Page 2 of 2). Configuration Worksheet - IPX Outbound RIP Filters

Parameter Information		Your Value
Parameter	Local IPX network to filter on (required for each outbound RIP router filter defined)	
Valid Values	A selection from the drop-down list (if the list is empty, no interface has been configured for IPX)	
Default	None	
Description	This parameter determines if routing information for a network is filtered on all local interfaces configured for IPX, or on an interface selected from the list displayed in the Configuration Program.	
Parameter	Network numbers to filter on	
Valid Values	All networks, Enter network number	
Default	All networks	
Description	This parameter determines if the routing information in the RIP response packet is filtered for all networks or specified networks.	
Parameter	Network number	
Valid Values	X'0000 0000' to X'FFFF FFFE'	
Default	None	
Description	This parameter identifies th specific network on which the routing information in the RIP response packet is filtered.	

Note: A maximum of 128 outbound RIP filters can be configured for this 6611.

VIrtual NEtwork System (VINES)

Banyan VIrtual NEtwork System (VINES) is a network operating system provided by Banyan Systems, Inc. VINES provides transparent distributed computing to its users. It allows access to resources such as applications, disks, printers, minicomputers, and mainframes. Its strength is enterprise networking which is based on its support of distributed applications development, global directory services, WAN interconnection, and support of multiple communication protocol suites.

The 6611 will route native VINES traffic in a VINES internetwork. It will behave as a routing node and interoperate with VINES clients, VINES servers, and compatible original equipment manufacturer (OEM) router implementations.

To function as a VINES router, the 6611 implements the VINES network layer protocols. The 6611 does not provide application level VINES services. However, in order to interoperate in a VINES internetwork, the 6611 bridges selected zero and limited hop-count broadcast packets sent among VINES servers. It also responds to selected NetRPC calls initiated by clients and servers.

The 6611 provides several additional features such as

- VINES ARP (internet address assignments for clients)
- VINES RouTing update Protocol (RTP) packet filters
- VINES IP packet filters
- User-specified interface metrics
- Support for serverless LAN segments
- Support for VINES link level echo on token-ring and Ethernet networks
- Support for frame relay and PPP

For more information about the VINES protocol and filters, see the *Introduction and Planning Guide*.

Port Types Supported

Table 5-401. Port Types Supported for VINES Routing

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	

Restrictions

When you configure VINES on the Token-Ring Port and use Token-Ring 802.5 LLC encapsulation, you cannot use the SAP value X'BC' to route data link switching traffic.

When VINES is configured on a frame-relay port with either AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by VINES on the port.

Configuration Changes ...

That Require the VINES Function to Restart

None

That Require the 6611 to Restart

- Node-level parameters
  - Enable VINES router
  - VINES network number
- Port-level parameters
  - Enable VINES routing
  - DLCI number
  - VINES destination address

Configuration Options

Table 5-402 on page 5-305 summarizes the configuration options for each adapter type that supports the VINES protocol. After configuring VINES on specific ports, you need to enable VINES routing on the 6611.

Table 5-402. VINES Configuration Options

WHEN configuring VINES...	THEN optionally...
...on a token-ring port or an Ethernet port: • Enable VINES on the port. • Determine the encapsulation method.	• Define inbound and outbound filters for this port. For more information about VINES filters, read the *Introduction and Planning Guide*. • Determine whether to override the architected neighbor metric. • Determine whether to enable the Address Resolution Protocol (ARP). • Determine whether to enable serverless support.
...on a serial port using PPP: • Enable VINES on the port.	• Define inbound and outbound filters for this port. • Determine whether to override the architected neighbor metric. • Determine whether to enable periodic full routing updates.
...on a serial port using frame relay: • Enable VINES on the port. • Define DLCIs assigned to the frame relay port, and enable InARP *or* define VINES destinations for each DLCI to provide a logical mapping between the DLCI number and the destination VINES address. **Note:** When VINES is configured on a frame relay port with either AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by VINES on the port.	• Define inbound and outbound filters for this port. • Determine whether to override the architected neighbor metric. • Determine whether to enable periodic full routing updates.
...at the node level: • Enable the VINES router.	• Specify the VINES network number. • Specify the VINES routing server name. • Define RTP filters.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform VINES routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-403 (Page 1 of 2). VINES Configuration Verification Checklist

VINES Rule	Configuration Parameter	√
Node-Level Parameters:		
The Enable VINES router parameter must be enabled on all routers that transport VINES.	Enable VINES router	
When you enter VINES network numbers, they must be unique across the network. When you do not enter VINES network numbers, the 6611 generates unique network numbers.	VINES network number	

Table 5-403 (Page 2 of 2). VINES Configuration Verification Checklist

VINES Rule	Configuration Parameter	√
Unique VINES routing server names should be used across the network for ease of administration. This parameter does not affect routing of data in any way. However, administration will be more difficult if the names are not unique.	VINES routing server name	
Port-Level Parameters:		
The Enable VINES routing on this port parameter must be enabled on all 6611 ports that transport VINES. At least two ports on each 6611 must be enabled for VINES.	Enable VINES routing on this port	
Token-ring ports on the same LAN must have the same value for the Encapsulation method parameter. Ethernet ports on the same LAN must have the same value for the Encapsulation method parameter. Token-ring and Ethernet-connected VINES clients and servers on the same LAN must also have the same value for the Encapsulation method parameter.	Encapsulation method (token-ring Port)	
	Encapsulation method (Ethernet Port)	
The following parameters are applicable to Ethernet, token-ring and serial ports: If there are VINES clients on a LAN which does not have a VINES server, the Enable ARP parameter must be enabled on at least one port connected to the LAN. In addition, the Enable serverless support parameter must be enabled if the closest VINES server to the above VINES client is two or more hops away.	Enable ARP	
	Enable serverless support	
	Distance to server (1-15 hops)	
Interconnected serial ports configured for VINES must have the same value for the Enable periodic full routing updates parameter.	Enable periodic full routing updates	
For serial frame-relay port pairs: VINES destination address-DLCI number pairs must be configured if the Use InARP to resolve remote protocol addresses parameter is disabled on either end of the serial frame-relay port pair. The combination of the values of the DLCI number parameter and the VINES destination address parameter implies that there is a direct connection (physical link) between a 6611 and the destination. Therefore, there must be at least one match between the value of the VINES network address parameter on one port and the value of the VINES destination address parameter on ports on adjacent 6611s.	DLCI number	
	VINES destination address	
	VINES network number	
	Local Management Interface option	
	Use InARP to resolve remote protocol addresses	

Sample Network Graphic

Figure 5-41 on page 5-307 illustrates a network where VINES routing is enabled between a workstation and a file server over serial ports across a network.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and VINES over frame relay
  - A token-ring port running IP and VINES
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and VINES over frame relay
  - An Ethernet port running IP and VINES

The following information is shown in Figure 5-41:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*
- VINES network numbers

Note: The configuration of the IP protocol is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to route VINES.

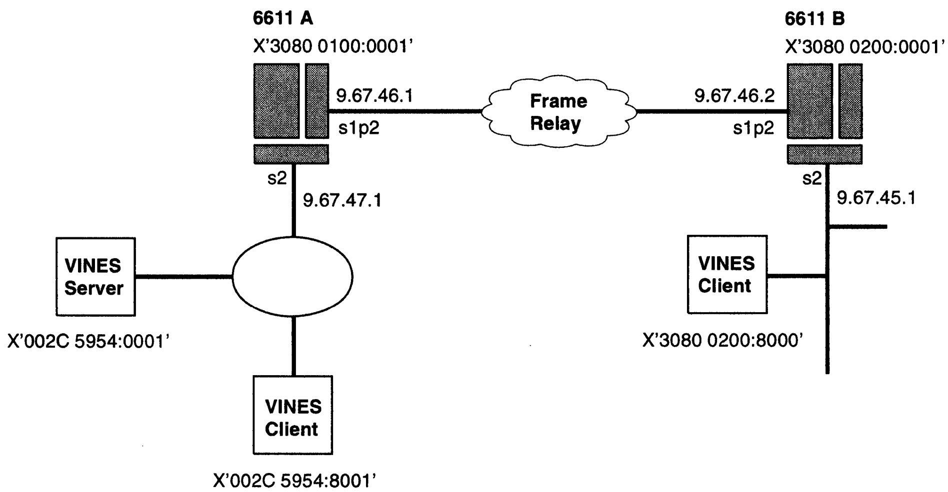


Figure 5-41. Sample Network for Routing VINES

This example shows the configuration for:

- VINES routing
- VINES serverless support
- Serial, Token-Ring, and Ethernet ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-41. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 5-404. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	Frame relay	Frame relay

Table 5-405. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56000	56000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table 5-406. Serial Port - Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Frame Relay on this port	Enable	Enable
Polling interval	10	10
Full inquiry interval	6	6
LMI option	ANSI T1.617 Annex D	ANSI T1.617 Annex D
Use InARP to resolve remote protocol addresses	Enable	Enable
DLCIs assigned to this port	20	30

Table 5-407. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.46.1	9.67.46.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Disable	Disable
Point-to-point only	Disable	Disable
Assignment for discovered DLCIs	Mesh	Mesh
IP Priority	Disable	Disable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-408. Serial Port - VINES over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable VINES routing on this port	Enable	Enable
Override architected neighbor metric	Disable	Disable
Neighbor metric override	NA	NA
Enable periodic full routing updates	Disable	Disable
Enable serverless support	Disable	Disable
Distance to server	NA	NA
Inbound Port Filters	Disable	Disable
Outbound port filters	Disable	Disable

Table 5-409. Serial Port - VINES Destinations per DLCI Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
DLCI number	20	30
VINES destination address (hex)	30800200	30800100

Token-Ring Port and Protocols Running on It

Table 5-410. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	NA
MAC address format	NA
Token ring data rate	4 Mbps
Broadcast type	Non-local

Table 5-411. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value
Enable IP routing on this port	Enable
IP address	9.67.47.1
Subnet mask	255.255.255.0
Max. transmission unit (octets)	1500
Enable ICMP address mask requests	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Table 5-412. Token-Ring Port - VINES Parameters Configured

Parameter	6611 A Slot 2 Value
Enable VINES routing on this port	Enable
Encapsulation method	Token-Ring 802.5 LLC
Override architected neighbor metric	Disable
Neighbor metric override	NA
Enable ARP	Disable
Enable serverless support	Disable
Distance to server	NA
Inbound Port Filters	Disable
Outbound port filters	Disable

Ethernet Port and Protocols Running on It

Table 5-413. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 2 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	None
Enable additional multicast addresses	Disable
Multicast MAC address	None

Table 5-414. Ethernet Port - IP Parameters Configured

Parameter	6611 B Slot 2 Value
Enable IP routing on this port	Enable
IP address	9.67.45.1
Subnet mask	255.255.255.0
Max. transmission unit (octets)	1500
Ethernet framing for IP	Ethernet V2.0
Enable ICMP address mask requests	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Table 5-415. Ethernet Port - VINES Parameters Configured

Parameter	**6611 B Slot 2 Value**
Enable VINES routing on this port	Enable
Encapsulation method	Ethernet V2.0
Override architected neighbor metric	Disable
Neighbor metric override	NA
Enable ARP	Enable
Enable serverless support	Enable
Distance to server	2
Inbound Port Filters	Disable
Outbound port filters	Disable

Node-Level Parameters

Table 5-416. Node Level - VINES Parameters Configured

Parameter	**6611 A Value**	**6611 B Value**
Enable VINES router	Enable	Enable
VINES network number	3080 0100	3080 0200
VINES routing server name	RouterA	RouterB
RTP router filters	Disable	Disable
Inbound RTP filters	Disable	Disable
Outbound RTP filters	Disable	Disable

Port Level Worksheets

Figure 5-42 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-42.

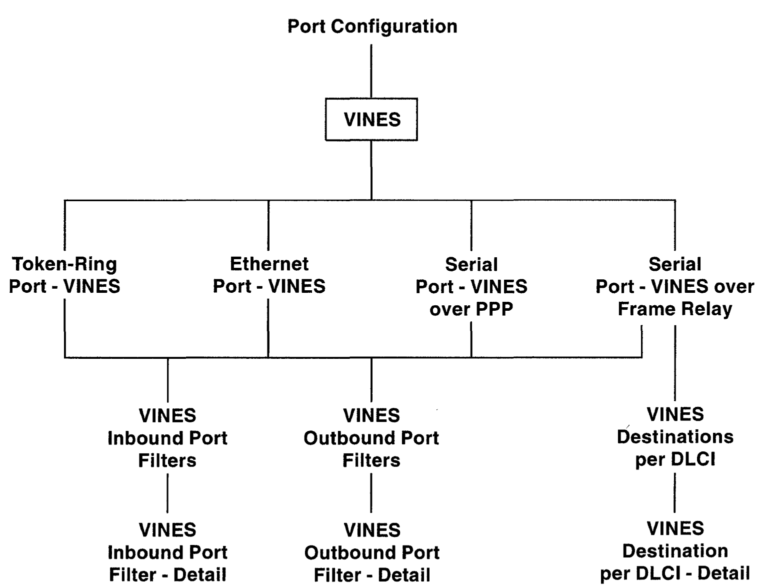


Figure 5-42. Flow of Port Level VINES Help Windows

To enable adapters to transmit and receive VINES packets, you need to enable VINES routing at the port level. Configure VINES on each port that will transmit and receive VINES packets. Then configure VINES at the node level.

Use the following tables as worksheets for your port level configurations.

- Token-Ring Port - VINES on page 5-312
- Ethernet Port - VINES on page 5-313
- Serial Port - VINES over PPP on page 5-314
- Serial Port - VINES over Frame Relay on page 5-314
- VINES Destination per DLCI - Detail on page 5-315
- VINES Inbound Port Filters on page 5-315
- VINES Outbound Port Filters on page 5-317

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-23 on page D-19 for a mapping of parameter names and their associated labels.

Table 5-417 (Page 1 of 2). Configuration Worksheet - Token-Ring Port - VINES

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable VINES routing on this port Enable, Disable Disable This parameter enables or disables VINES routing on this port.	
Parameter **Valid Values** **Default** **Description**	Encapsulation method Token-Ring 802.5 LLC, Token-Ring 802.5 SNAP Token-Ring 802.5 LLC This parameter determines the logical link control (LLC) encapsulation method used to transmit VINES packets.	
Parameter **Valid Values** **Default** **Description**	Override architected neighbor metric Enable, Disable Disable This parameter determines whether the 6611 uses the architected neighbor metric or uses the user-specified neighbor metric.	
Parameter **Valid Values** **Default** **Description**	Neighbor metric override 1 to 90 None This parameter defines the metric that the 6611 uses to make routing decisions. You can only answer this parameter when the override architected neighbor metric parameters is set to **Enable**.	
Parameter **Valid Values** **Default** **Description**	Enable ARP Enable, Disable Disable This parameter specifies whether the 6611 assigns addresses to clients that reside on the LAN attached to this port.	
Parameter **Valid Values** **Default** **Description**	Enable serverless support Enable, Disable Disable This parameter specifies whether the 6611 allows clients on a serverless LAN segment to access a VINES server that is more than one hop away.	

Table 5-417 (Page 2 of 2). Configuration Worksheet - Token-Ring Port - VINES

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Distance to server 2 to 15 hops 2 hops This parameter specifies the distance from the VINES client on the serverless LAN to the appropriate VINES server. You can only answer this parameter when the Enable serverless support parameter is set to **Enable**.	

Table 5-418. Configuration Worksheet - Ethernet Port - VINES

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable VINES routing on this port Enable, Disable Disable This parameter enables or disables VINES routing on this port.	
Parameter **Valid Values** **Default** **Description**	Encapsulation method Ethernet V2.0, Ethernet 802.3 SNAP Ethernet V2.0 This parameter determines the encapsulation method used to transmit VINES packets across this Ethernet port.	
Parameter **Valid Values** **Default** **Description**	Override architected neighbor metric Enable, Disable Disable This parameter determines whether the 6611 uses the architected neighbor metric or uses the user-specified neighbor metric.	
Parameter **Valid Values** **Default** **Description**	Neighbor metric override 1 to 90 None This parameter defines the metric that the 6611 uses to make routing decisions. You can only answer this parameter when the override architected neighbor metric parameters is set to **Enable**.	
Parameter **Valid Values** **Default** **Description**	Enable ARP Enable, Disable Disable This parameter specifies whether the 6611 assigns addresses to clients that reside on the LAN attached to this port.	
Parameter **Valid Values** **Default** **Description**	Enable serverless support Enable, Disable Disable This parameter specifies whether the 6611 allows clients on a serverless LAN segment to access a VINES server that is more than one hop away.	
Parameter **Valid Values** **Default** **Description**	Distance to server 2 to 15 hops 2 hops This parameter specifies the distance from the VINES client on the serverless LAN to the appropriate VINES server. You can only answer this parameter when the Enable serverless support parameter is set to **Enable**.	

Table 5-419. Configuration Worksheet - Serial Port - VINES over PPP

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable VINES routing on this port Enable, Disable Disable This parameter enables or disables VINES routing on this port.	
Parameter **Valid Values** **Default** **Description**	Override architected neighbor metric Enable, Disable Disable This parameter determines whether the 6611 uses the architected neighbor metric or uses the user-specified neighbor metric.	
Parameter **Valid Values** **Default** **Description**	Neighbor metric override 1 to 90 None This parameter defines the metric that the 6611 uses to make routing decisions. You can only answer this parameter when the override architected neighbor metric parameters is set to **Enable**.	
Parameter **Valid Values** **Default** **Description**	Enable periodic full routing updates Enable, Disable Disable This parameter specifies whether this 6611 sends routing updates continuously, or only when a link is opened or a network topology change is detected.	

Table 5-420. Configuration Worksheet - Serial Port - VINES over Frame Relay

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable VINES routing on this port Enable, Disable Disable This parameter enables or disables VINES routing on this port.	
Parameter **Valid Values** **Default** **Description**	Override architected neighbor metric Enable, Disable Disable This parameter determines whether the 6611 uses the architected neighbor metric or uses the user-specified neighbor metric.	
Parameter **Valid Values** **Default** **Description**	Neighbor metric override 1 to 90 None This parameter defines the metric that the 6611 uses to make routing decisions. You can only answer this parameter when the override architected neighbor metric parameters is set to **Enable**.	
Parameter **Valid Values** **Default** **Description**	Enable periodic full routing updates Enable, Disable Disable This parameter specifies whether this 6611 sends routing updates continuously, or only when a link is opened or a network topology change is detected.	

Table 5-421. Configuration Worksheet - VINES Destination per DLCI - Detail

Parameter Information		Your Value
VINES Destination List - Parameters configured for each destination defined		
Parameter **Valid Values** **Default** **Description**	DLCI number A selection from the drop-down list (if the list is empty, then no DLCIs have been configured) None This parameter defines the data link connection identifier (DLCI) number that provides a logical connection to a router with an VINES address specified in the Destination VINES address parameter.	
Parameter **Valid Values** **Default** **Description**	VINES destination network number X'0000 0000' to X'FFFF FFFE' None This parameter defines the VINES address for this data link connection identifier (DLCI) connection on this serial port.	

Table 5-422 (Page 1 of 3). Configuration Worksheet - VINES Inbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable inbound port filters Enable, Disable Disable This parameter enables or disables all VINES inbound port filters defined on this port.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter determines the filtering mode for all VINES inbound filters defined on this port.	
VINES Inbound Port Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required) 1 to 10 None This parameter uniquely defines this filter in a list of inbound port filters.	
Parameter **Valid Values** **Default** **Description**	Filter based on hop count Enable, Disable Disable This parameter allows VINES packets to be filtered based on hop count.	
Parameter **Valid Values** **Default** **Description**	Relational compare operator equal to, less than, less than or equal to, greater than, greater than or equal to equal to This parameter is used as the relational operator when filtering is based on hop count.	
Parameter **Valid Values** **Default** **Description**	Hop count value 0 to 15 None This parameter defines the hop count value used to filter VINES packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on protocol type Enable, Disable None This parameter allow VINES packets to be filtered based on the protocol type.	

Table 5-422 (Page 2 of 3). Configuration Worksheet - VINES Inbound Port Filters

Parameter Information	Your Value
Parameter Protocol type value **Valid Values** IPC, SPP, ARP, RTP, ICP **Default** None **Description** This parameter defines the protocol type value used to filter VINES packets.	
Parameter Filter based on destination network **Valid Values** Enable, Disable **Default** Disable **Description** This parameter allows VINES packets to be filtered based on the Destination network value parameter value specified.	
Parameter Destination network value **Valid Values** X'0000 0000' to X'FFFF FFFF' **Default** None **Description** This parameter defines the destination network value used to filter VINES packets.	
Parameter Filter based on source network **Valid Values** Enable, Disable **Default** Disable **Description** This parameter allows VINES packets to be filtered on the Source network value parameter value specified.	
Parameter Source network value **Valid Values** X'0000 0000' to X'FFFF FFFF' **Default** None **Description** This parameter defines the source network value used to filter VINES packets.	
Parameter Filter based on destination subnetwork **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables the filtering of VINES packets based on the Destination subnetwork value parameter value specified.	
Parameter Destination subnetwork value **Valid Values** X'0000' to X'FFFF' **Default** None **Description** This parameter defines the destination subnetwork value used for filtering packets.	
Parameter Filter based on source subnetwork **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables the filtering of VINES packets based on the Source subnetwork value parameter value specified.	
Parameter Source subnetwork value **Valid Values** X'0000' to X'FFFF' **Default** None **Description** This parameter defines the source subnetwork value used for filtering packets.	
Parameter Filter based on destination port **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables the filtering of VINES packets based on the Destination port value parameter value specified.	

Table 5-422 (Page 3 of 3). Configuration Worksheet - VINES Inbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Destination port value X'0000' to X'FFFF' None This parameter defines the destination port value used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on source port Enable, Disable Disable This parameter enables or disables the filtering of VINES packets based on the Source port value parameter value specified.	
Parameter **Valid Values** **Default** **Description**	Source port value X'0000' to X'FFFF' None This parameter defines the source port value used for filtering packets.	

Note: A maximum of 10 inbound filters can be configured for each port.

Table 5-423 (Page 1 of 3). Configuration Worksheet - VINES Outbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable outbound port filters Enable, Disable Disable This parameter enables or disables all VINES outbound port filters defined on this port.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter determines the filtering mode for all VINES outbound filters defined on this port.	
VINES Outbound Port Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required) 1 to 10 None This parameter uniquely defines this filter in a list of outbound port filters.	
Parameter **Valid Values** **Default** **Description**	Filter based on hop count Enable, Disable Disable This parameter allows VINES packets to be filtered based on hop count.	
Parameter **Valid Values** **Default** **Description**	Relational compare operator equal to, less than, less than or equal to, greater than, greater than or equal to equal to This parameter is used as the relational operator when filtering is based on hop count.	
Parameter **Valid Values** **Default** **Description**	Hop count value 0 to 15 None This parameter defines the hop count value used to filter VINES packets.	

Table 5-423 (Page 2 of 3). Configuration Worksheet - VINES Outbound Port Filters

Parameter Information	Your Value
Parameter Filter based on protocol type **Valid Values** Enable, Disable **Default** None **Description** This parameter allow VINES packets to be filtered based on the protocol type.	
Parameter Protocol type value **Valid Values** IPC, SPP, ARP, RTP, ICP **Default** None **Description** This parameter defines the protocol type value used to filter VINES packets.	
Parameter Filter based on destination network **Valid Values** Enable, Disable **Default** Disable **Description** This parameter allows VINES packets to be filtered based on the Destination network value parameter value specified.	
Parameter Destination network value **Valid Values** X'0000 0000' to X'FFFF FFFF' **Default** None **Description** This parameter defines the destination network value used to filter VINES packets.	
Parameter Filter based on source network **Valid Values** Enable, Disable **Default** Disable **Description** This parameter allows VINES packets to be filtered on the Source network value parameter value specified.	
Parameter Source network value **Valid Values** X'0000 0000' to X'FFFF FFFF' **Default** None **Description** This parameter defines the source network value used to filter VINES packets.	
Parameter Filter based on destination subnetwork **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables the filtering of VINES packets based on the Destination subnetwork value parameter value specified.	
Parameter Destination subnetwork value **Valid Values** X'0000' to X'FFFF' **Default** None **Description** This parameter defines the destination subnetwork value used for filtering packets.	
Parameter Filter based on source subnetwork **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables the filtering of VINES packets based on the Source subnetwork value parameter value specified.	
Parameter Source subnetwork value **Valid Values** X'0000' to X'FFFF' **Default** None **Description** This parameter defines the source subnetwork value used for filtering packets.	

Table 5-423 (Page 3 of 3). Configuration Worksheet - VINES Outbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Filter based on destination port Enable, Disable Disable This parameter enables or disables the filtering of VINES packets based on the Destination port value parameter value specified.	
Parameter **Valid Values** **Default** **Description**	Destination port value X'0000' to X'FFFF' None This parameter defines the destination port value used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on source port Enable, Disable Disable This parameter enables or disables the filtering of VINES packets based on the Source port value parameter value specified.	
Parameter **Valid Values** **Default** **Description**	Source port value X'0000' to X'FFFF' None This parameter defines the source port value used for filtering packets.	

Note: A maximum of 10 outbound filters can be configured for each port.

Node Level Worksheets

Figure 5-43 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-43.

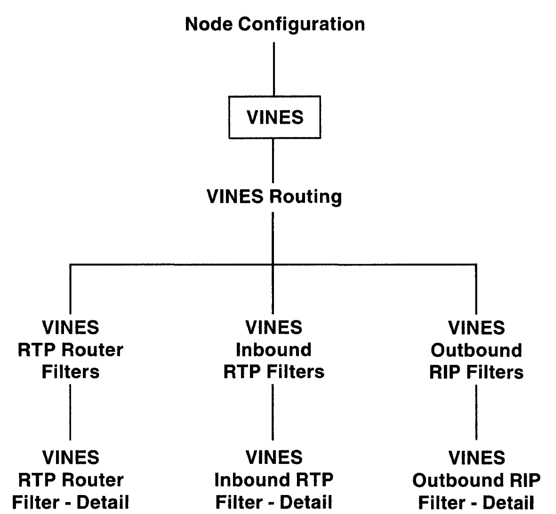


Figure 5-43. Flow of Node Level VINES Help Windows

To enable the 6611 to route VINES packets across network, you need to enable VINES routing at the node level. Use the following tables as worksheets for your node level configuration.

- VINES Routing on page 5-320
- VINES Inbound RTP Filters on page 5-321
- VINES Outbound RTP Filters on page 5-322

- VINES RTP Router Filters on page 5-320

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-23 on page D-19 for a mapping of parameter names and their associated labels.

Table 5-424. Configuration Worksheet - VINES Routing

Parameter Information		Your Value
Parameter	Enable VINES router	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all ports configured for VINES.	
Parameter	VINES network number	
Valid Values	For models 120, 125, 140, and 170, X'3080 0000' to X'3087 FFFF'. For models 145 and 175, X'3088 0000' to X'308F FFFF'.	
Default	An 6611-generated VINES network number that is based on this 6611's unique processor identification number	
Description	This parameter defines the VINES network number of this 6611.	
Parameter	VINES routing server name	
Valid Values	1 to 15 alphanumeric characters, periods, commas, dashes, and spaces	
Default	IBM*net#*, where *net#* is the ASCII equivalent of this 6611's VINES network number	
Description	This parameter specifies the name to be used by the 6611 when responding to client "WHATZ" requests.	

Table 5-425 (Page 1 of 2). Configuration Worksheet - VINES RTP Router Filters

Parameter Information		Your Value
Parameter	Enable RTP router filters	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all VINES RTP router filters defined on this 6611.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default	Deny	
Description	This parameter determines the filtering mode for all VINES RTP router filters defined on this 6611.	
VINES RTP Router Filter List - Parameters configured for each filter defined		
Parameter	Filter ID (required)	
Valid Values	1 to 128	
Default	None	
Description	This parameter uniquely identifies this filter within the list of VINES RTP routers displayed in the Configuration Program.	
Parameter	VINES networks to filter	
Valid Values	All networks, One network	
Default	All networks	
Description	This parameter determines whether routing information is filtered for all networks, or for a specific network.	

Table 5-425 (Page 2 of 2). Configuration Worksheet - VINES RTP Router Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	VINES network number X'0000 0000' to X'FFFF FFFE' None This parameter defines the number of the VINES network whose routing information is filtered. You can only answer this parameter when the VINES networks to filter parameter is set to **One network**.	

Note: A maximum of 128 VINES RTP router filters can be configured for this 6611.

Table 5-426. Configuration Worksheet - VINES Inbound RTP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable inbound RTP filters Enable, Disable Disable This parameter enables or disables all VINES inbound RTP filters defined on this 6611.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter determines the filtering mode for all VINES inbound RTP filters defined on this 6611.	
VINES Inbound RTP Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required) 1 to 128 None This parameter uniquely identifies this filter within the list of VINES inbound RTP filters displayed in the Configuration Program.	
Parameter **Valid Values** **Default** **Description**	Local port to filter on (required) A selection from the drop-down list (if the list is empty, no interface has been configured for VINES) None This parameter specifies the interface on which routing information is filtered.	
Parameter **Valid Values** **Default** **Description**	VINES networks to filter All networks, One network All networks This parameter determines whether routing information is filtered for all networks, or for a specific network.	
Parameter **Valid Values** **Default** **Description**	VINES network number X'0000 0000' to X'FFFF FFFE' None This parameter defines the number of the VINES network whose routing information is filtered.	

Note: A maximum of 128 VINES inbound RTP filters can be configured for this 6611.

Table 5-427. Configuration Worksheet - VINES Outbound RTP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable outbound RTP filters Enable, Disable Disable This parameter enables or disables all VINES outbound RTP filters defined on this 6611.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter determines the filtering mode for all VINES outbound RTP filters defined on this 6611.	
VINES Outbound Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required) 1 to 128 None This parameter uniquely identifies this filter within the list of VINES outbound RTP filters displayed in the Configuration Program.	
Parameter **Valid Values** **Default** **Description**	Local port to filter on (required) A selection from the drop-down list (if the list is empty, no interface has been configured for VINES) None This parameter specifies the interface on which routing information is filtered.	
Parameter **Valid Values** **Default** **Description**	VINES networks to filter All networks, One network All networks This parameter determines whether routing information is filtered for all networks, or for a specific network.	
Parameter **Valid Values** **Default** **Description**	VINES network number X'0000 0000' to X'FFFF FFFE' None This parameter defines the number of the VINES network whose routing information is filtered.	

Note: A maximum of 128 VINES outbound RTP filters can be configured for this 6611.

Xerox Network Systems** (XNS)

Released by Xerox** Corporation to integrate their computer systems, XNS is the predecessor for several important network protocols today. It defines these transport protocols: Echo, Error, Sequenced Packet (SPP), Packet Exchange (PEX), Routing Information (RIP), and Internet Datagram (IDP). These protocols provide data transfer service over LAN and WAN networks.

The 6611 implements Echo, Error, RIP, and IDP. SPP and PEX packets are routed using the best path. The 6611 learns the best path through RIP exchanges. The user can also define a best path by using static routes.

The 6611 provides several additional features such as:

- RIP packet filters
- IDP packet filters
- Static route configuration

For more information about the 6611 XNS functions, see the *Introduction and Planning Guide*.

Port Types Supported

Table 5-428. Port Types Supported for XNS Routing

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	√
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	

Restrictions

- When you configure XNS on the Token-Ring Port and use Token-Ring 802.5 LLC encapsulation, you cannot use the SAP X'80' to route data link switching traffic.
- The XNS host address is automatically set to the value of the MAC address of the Token-Ring Port and Ethernet Port on this port.
- When XNS is configured on a frame-relay port with either AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by XNS on the port.

Configuration Changes...

That Require the XNS Function to Restart

None

That Require the 6611 to Restart

- Port-level parameters
  - Enable XNS routing on this port
  - XNS network number
  - Destination XNS address
  - DLCI number
- Node-level parameters
  - Enable XNS router

Configuration Options

Table 5-429 summarizes the configuration options for each port type that supports the XNS protocol. After configuring XNS on specific ports, you need to enable XNS routing at the node level.

Table 5-429 (Page 1 of 2). XNS Configuration Options

WHEN configuring XNS...	THEN optionally...
...on a token-ring port or an Ethernet port: • Enable XNS on the port. • Enter the XNS network number. • Determine the encapsulation method.	• Define filters for this port. • Determine the error protocol packet size. • Determine whether to enable or disable the error protocol.
...on a serial port using PPP: • Enable XNS on the port. • Enter the XNS network number. • On the physical interface, enter the locally administered MAC address assigned to this port.	• Define filters for this port. • Determine the error protocol packet size. • Determine whether to enable or disable the error protocol.
...on a serial port using frame relay: • Enable XNS on the port. • Enter the XNS network number. • Define DLCIs assigned to the frame relay port, and enable InARP *or* define XNS destinations for each DLCI to provide a logical mapping between the DLCI number and the destination XNS address. **Note:** When XNS is configured on a frame relay port with either AppleTalk or a bridging protocol, you must explicitly define the data link connection identifiers (DLCIs) that will be used by XNS on the port. • On the physical interface, enter the locally administered MAC address assigned to this port.	• Define filters for this port. • Determine the error protocol packet size. • Determine whether to enable or disable the error protocol.

Table 5-429 (Page 2 of 2). XNS Configuration Options

WHEN configuring XNS...	THEN optionally...
...at the node level: • Enable the XNS router.	• Select the split horizon option. • Define RIP filters. • Define static routes.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform XNS routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-430. XNS Configuration Verification Checklist

XNS Rule	Configuration Parameter	√
Node-Level Parameters:		
Ensure that the Enable XNS router parameter is enabled.	Enable XNS router	
Port-Level Parameters:		
Ensure that the Enable XNS routing on this port parameter is enabled on at least 2 ports on each 6611.	Enable XNS routing on this port	
For a given XNS connection, ensure that the physical interfaces are enabled, media types are the same, framing methods are the same and are enabled, and line speeds are the same.	Enable physical interface on this port	
	Framing method	
	Token-ring data rate	
	Line speed	
For a given connection: When XNS is routed between two token-ring or two Ethernet segments, ensure that the encapsulation methods for token-ring and Ethernet segments are the same and the network numbers match.	Encapsulation method	
	XNS network number	
When the Use InARP to resolve remote protocol addresses parameter is disabled and the LNI option parameter is set to **None**, ensure that the values of the Host address parameters are the same and that the DLCI destinations are the same.	Use InARP to resolve remote protocol addresses	
	LMI option	
	Host address	
	DLCI number	

Sample Network Graphic

Figure 5-44 on page 5-326 illustrates a network where XNS routing is enabled between a workstation and a file server over serial ports across a network.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and XNS over PPP
  - A token-ring port running IP and XNS

- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and XNS over PPP
  - A token-ring port running IP and XNS

The following information is shown in Figure 5-41 on page 5-307:

- IP addresses
- XNS addresses
- Slot and port numbers, abbreviated *sx* p*y*
- Locally administered addresses

Note: The configuration of the IP protocol is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to route XNS.

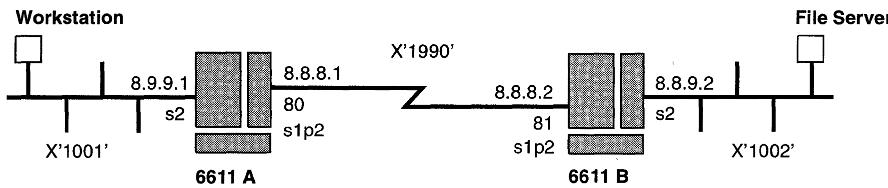


Figure 5-44. Sample Network for Routing XNS

This sample network shows the configuration for:

- XNS routing
- Serial and token-ring ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-44. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table 5-431. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-432. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	80	81
Enable port for transmission group	Disable	Disable
Transmission group name	None	None

Table 5-433. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-434. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-435. Serial Port - XNS over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable XNS routing on this port	Enable	Enable
XNS network number	1990	1990
Error protocol packet size	42	42
Error protocol active	Enable	Enable
Inbound Port Filters	Disable	Disable

Ethernet Ports and Protocols Running on Them

Table 5-436. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	None	None
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	None	None

Table 5-437. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.9.9.1	8.8.9.2
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-438. Ethernet Port - XNS Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable XNS routing on this port	Enable	Enable
XNS network number	1001	1002
Encapsulation method	Ethernet V2.0	Ethernet V2.0
Error protocol packet size	42	42
Error protocol active	Enable	Enable
Inbound Port Filters	Disable	Disable

Node-Level Parameters Configured

Table 5-439. Node Level - XNS Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable XNS router	Enable	Enable
Split horizon	On	On
Static Routes	Disable	Disable
RIP Router Filters	Disable	Disable
Inbound RIP Filters	Disable	Disable
Outbound RIP Filters	Disable	Disable

Port Level Worksheets

Figure 5-45 on page 5-329 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-45 on page 5-329.

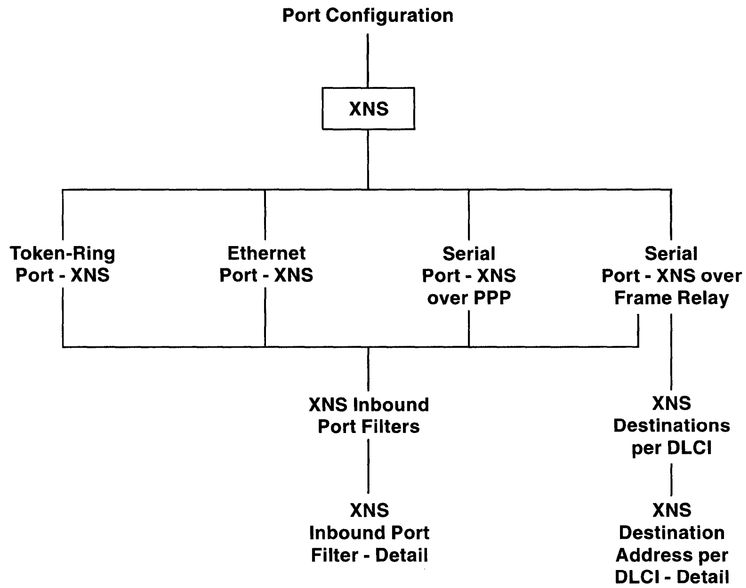


Figure 5-45. Flow of Port Level XNS Help Windows

To enable ports to transmit and receive XNS packets, you need to enable XNS routing at the port level. Configure XNS on each port that will transmit and receive XNS packets. Then configure XNS at the node level.

Use the following tables as worksheets for your port level configurations.

- Token-Ring Port - XNS on page 5-329
- Ethernet Port - XNS on page 5-330
- Serial Port - XNS over PPP on page 5-330
- Serial Port - XNS over Frame Relay on page 5-331
- XNS Destination Address per DLCI - Detail on page 5-331
- Define XNS Port Filters on page 5-332

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-24 on page D-20 for a mapping of parameter names and their associated labels.

Table 5-440 (Page 1 of 2). Configuration Worksheet - Token-Ring Port - XNS

Parameter Information		**Your Value**
Parameter	Enable XNS routing on this port	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables XNS routing on this port.	
Parameter	XNS network number (required)	
Valid Values	X'0000 0001' to X'FFFF FFFE'	
Default	None	
Description	This parameter assigns an XNS network number to the physical network attached to this port.	
Parameter	Encapsulation method	
Valid Values	Token-Ring 802.5 LLC, Token-Ring 802.5 SNAP	
Default	Token-Ring 802.5 SNAP	
Description	This parameter determines the LLC encapsulation method used to transmit XNS packets.	

Table 5-440 (Page 2 of 2). Configuration Worksheet - Token-Ring Port - XNS

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Error protocol packet size 42 to 542 42 This parameter determines the number of octets of the original packet returned in an error protocol packet used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Error protocol active Enable, Disable Enable This parameter enables or disables the generation of error protocol packets in response to invalid packets.	

Table 5-441. Configuration Worksheet - Ethernet Port - XNS

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable XNS routing on this port Enable, Disable Disable This parameter enables or disables XNS routing on this port.	
Parameter **Valid Values** **Default** **Description**	XNS network number (required) X'0000 0001' to X'FFFF FFFE' None This parameter assigns an XNS network number to the physical network attached to this port.	
Parameter **Valid Values** **Default** **Description**	Encapsulation method Ethernet V2.0, Ethernet 802.3 SNAP, Ethernet 802.3 LLC Ethernet V2.0 This parameter determines the logical link control (LLC) encapsulation method used to transmit XNS packets across this Ethernet port.	
Parameter **Valid Values** **Default** **Description**	Error protocol packet size 42 to 542 42 This parameter determines the number of octets of the original packet returned in an error protocol packet used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Error protocol active Enable, Disable Enable This parameter enables or disables the generation of error protocol packets in response to invalid packets.	

Table 5-442 (Page 1 of 2). Configuration Worksheet - Serial Port - XNS over PPP

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable XNS routing on this port Enable, Disable Disable This parameter enables or disables XNS routing on this port.	
Parameter **Valid Values** **Default** **Description**	XNS network number (required) X'0000 0001' to X'FFFF FFFE' None This parameter assigns an XNS network number to the physical network attached to this port.	

Table 5-442 (Page 2 of 2). Configuration Worksheet - Serial Port - XNS over PPP

Parameter Information		Your Value
Parameter	Error protocol packet size	
Valid Values	42 to 542	
Default	42	
Description	This parameter determines the number of octets of the original packet returned in an error protocol packet used for filtering packets.	
Parameter	Error protocol active	
Valid Values	Enable, Disable	
Default	Enable	
Description	This parameter enables or disables the generation of error protocol packets in response to invalid packets.	

Table 5-443. Configuration Worksheet - Serial Port - XNS over Frame Relay

Parameter Information		Your Value
Parameter	Enable XNS routing on this port	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables XNS routing on this port.	
Parameter	XNS network number (required)	
Valid Values	X'0000 0001' to X'FFFF FFFE'	
Default	None	
Description	This parameter assigns an XNS network number to the physical network attached to this port.	
Parameter	Error protocol packet size	
Valid Values	42 to 542	
Default	42	
Description	This parameter determines the number of octets of the original packet returned in an error protocol packet used for filtering packets.	
Parameter	Error protocol active	
Valid Values	Enable, Disable	
Default	Enable	
Description	This parameter enables or disables the generation of error protocol packets in response to invalid packets.	

Table 5-444. Configuration Worksheet - XNS Destination Address per DLCI - Detail

Parameter Information		Your Value
XNS Destination List - Parameters configured for each destination defined		
Parameter	Destination XNS address	
Valid Values	X'0000 0000 0000' to X'FFFF FFFF FFFE'	
Default	None	
Description	This parameter specifies an XNS router address that will be associated with a DLCI on this serial port.	
Parameter	DLCI number (required for each DLCI pair defined)	
Valid Values	A selection from the drop-down list (if the list is empty, then no DLCIs have been configured)	
Default	None	
Description	This parameter defines the DLCI number that provides a logical connection to a router with an XNS address specified in the Destination XNS address parameter.	

Table 5-445 (Page 1 of 3). Configuration Worksheet - XNS Inbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable inbound port filters Enable, Disable Disable This parameter enables or disables all XNS filters defined on this port.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter determines the filtering mode for all XNS filters defined on this port.	
XNS Port Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required for each XNS port filter defined) 1 to 10 None This parameter uniquely defines this filter in a list of filters.	
Parameter **Valid Values** **Default** **Description**	Filter based on hop count Enable, Disable Disable This parameter allows XNS packets to be filtered based on hop count.	
Parameter **Valid Values** **Default** **Description**	Relational compare operator equal to, less than, less than or equal to, greater than, greater than or equal to equal to This parameter is used as the relational operator when filtering is based on hop count.	
Parameter **Valid Values** **Default** **Description**	Hop count value X'0' to X'F' None This parameter defines the hop count value used to filter XNS packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on packet type Enable, Disable Disable This parameter allow XNS packets to be filtered based on the packet type.	
Parameter **Valid Values** **Default** **Description**	Packet type value X'00' to X'FF' None This parameter defines the packet type value used to filter XNS packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on checksum Enable, Disable Disable This parameter enables or disables the filtering of XNS packets based on checksum.	
Parameter **Valid Values** **Default** **Description**	Checksum value X'0000' to X'FFFF' None This parameter defines the checksum value used to filter XNS packets. The filtered values are found in the IDP header.	
Parameter **Valid Values** **Default** **Description**	Filter based on destination network Enable, Disable Disable This parameter allows XNS packets to be filtered based on the Destination network value parameter value specified.	

Table 5-445 (Page 2 of 3). Configuration Worksheet - XNS Inbound Port Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Destination network value X'0000 0000' to X'FFFF FFFF' None This parameter defines the destination network value used to filter XNS packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on source network Enable, Disable Disable This parameter allows XNS packets to be filtered on the Source network value parameter value specified.	
Parameter **Valid Values** **Default** **Description**	Source network value X'0000 0000' to X'FFFF FFFF' None This parameter defines the source network value used to filter XNS packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on destination host Enable, Disable Disable This parameter enables or disables the filtering of XNS packets based on the Destination host value parameter value specified.	
Parameter **Valid Values** **Default** **Description**	Destination host value X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the destination network value used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on source host Enable, Disable Disable This parameter enables or disables the filtering of XNS packets based on the Source host value parameter value specified.	
Parameter **Valid Values** **Default** **Description**	Source host value X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the source host value used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on destination socket Enable, Disable Disable This parameter enables or disables the filtering of XNS packets based on the Destination socket value parameter value specified.	
Parameter **Valid Values** **Default** **Description**	Destination socket value X'0000' to X'FFFF' None This parameter defines the destination socket value used for filtering packets.	
Parameter **Valid Values** **Default** **Description**	Filter based on source socket Enable, Disable Disable This parameter enables or disables the filtering of XNS packets based on the Source socket value parameter value specified.	

Table 5-445 (Page 3 of 3). Configuration Worksheet - XNS Inbound Port Filters

Parameter Information		Your Value
Parameter	Source socket value	
Valid Values	X'0000' to X'FFFF'	
Default	None	
Description	This parameter defines the source socket value used for filtering packets.	

Note: A maximum of 10 XNS port filters can be configured for each port.

Node Level Worksheets

Figure 5-46 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-46.

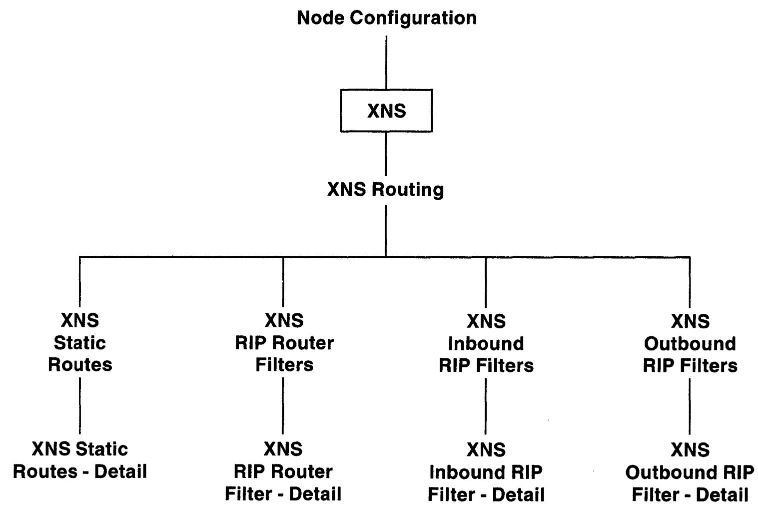


Figure 5-46. Flow of Node Level XNS Help Windows

To enable the 6611 to route XNS packets across a network, you need to enable XNS routing at the node level. Use the following tables as worksheets for your node level configuration.

- XNS Routing on page 5-334
- XNS Inbound RIP Filters on page 5-336
- XNS Outbound RIP Filters on page 5-337
- XNS RIP Router Filters on page 5-335
- XNS Static Routes on page 5-335

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-24 on page D-20 for a mapping of parameter names and their associated labels.

Table 5-446 (Page 1 of 2). Configuration Worksheet - XNS Routing

Parameter Information		Your Value
Parameter	Enable XNS router	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all ports configured for XNS.	

Table 5-446 (Page 2 of 2). Configuration Worksheet - XNS Routing

Parameter Information		Your Value
Parameter	Split horizon	
Valid Values	On, Poison Reverse, Off	
Default	On	
Description	This parameter determines if the XNS route process should use the split horizon technique of handling RIP information.	

| *Table 5-447. Configuration Worksheet - XNS Static Routes*

Parameter Information		Your Value
Parameter	Enable XNS static routes	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all defined static routes for XNS.	
XNS Static Route List - Parameter configured for each static route defined		
Destination		
Parameter	Destination network number (required for each static route defined)	
Valid Values	X'0000 0001' to X'FFFF FFFE'	
Default	None	
Description	This parameter defines the destination network for this static route.	
Parameter	Destination network number mask	
Valid Values	X'0000 0001' to X'FFFF FFFE'	
Default	X'FFFF FFFE'	
Description	This parameter defines the mask that is applied to the network number to define a range of network numbers that match this destination.	
Next hop		
Parameter	Network number of next hop router (required for each static route defined)	
Valid Values	X'0000 0001' to X'FFFF FFFE'	
Default	None	
Description	This parameter defines the network number of a router on an attached network that is the next hop router.	
Parameter	Next hop router host address (required for each static route defined)	
Valid Values	12 hexadecimal digits	
Default	None	
Description	This parameter defines the host address of a router on an attached network that is the next hop router.	

Table 5-448 (Page 1 of 2). Configuration Worksheet - XNS RIP Router Filters

Parameter Information		Your Value
Parameter	Status of all RIP router filters	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables all XNS RIP router filters defined on this 6611.	
Parameter	Filtering mode	
Valid Values	Deny, Permit	
Default	Deny	
Description	This parameter determines the filtering mode for all XNS RIP router filters defined on this 6611.	

Table 5-448 (Page 2 of 2). Configuration Worksheet - XNS RIP Router Filters

Parameter Information		Your Value
RIP Router Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required for each RIP router filter defined) 1 to 128 None This parameter uniquely identifies this filter within the list displayed in the Configuration Program.	
Parameter **Valid Values** **Default** **Description**	Network numbers to filter on All networks, Enter network number All networks This parameter defines routing information about the XNS network number. The network number is filtered on the interface on the interface identified in the Local XNS network to filter on parameter.	
Parameter **Valid Values** **Default** **Description**	Network number X'0000 0000' to X'FFFF FFFE' None This parameter defines the number of the XNS network whose routing information is filtered.	
Parameter **Valid Values** **Default** **Description**	Host address to filter on All hosts, Enter host address All hosts This parameter determines whether routing information is filtered for all hosts or for specific a host.	
Parameter **Valid Values** **Default** **Description**	Host address X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the address of the host whose routing information is filtered.	

Note: A maximum of 128 RIP router filters can be configured for this 6611.

Table 5-449 (Page 1 of 2). Configuration Worksheet - XNS Inbound RIP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable inbound RIP filters Enable, Disable Disable This parameter enables or disables all inbound RIP filters defined on this 6611.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter determines the filtering mode for all inbound RIP filters defined on this 6611.	
Inbound RIP Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required for each inbound RIP filter defined) 1 to 128 None This parameter uniquely identifies this filter within the list displayed in the Configuration Program.	

Table 5-449 (Page 2 of 2). Configuration Worksheet - XNS Inbound RIP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Local network to filter on (required for each inbound RIP filter defined) A selection from the drop-down list (if the list is empty, no interface has been configured for XNS) None This parameter determines if routing information for a network is filtered on all local interfaces configured for XNS, or on an interface selected from the list displayed in the Configuration Program.	
Parameter **Valid Values** **Default** **Description**	Network numbers to filter on All networks, Enter network number All networks This parameter defines routing information about the XNS network number. The network number is filtered on the interface on the interface identified in the Local XNS network to filter on parameter.	
Parameter **Valid Values** **Default** **Description**	Network number X'0000 0000' to X'FFFF FFFE' None This parameter defines the number of the XNS network whose routing information is filtered.	

Note: A maximum of 128 inbound RIP filters can be configured for this 6611.

Table 5-450 (Page 1 of 2). Configuration Worksheet - XNS Outbound RIP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable outbound RIP filters Enable, Disable Disable This parameter enables or disables all outbound RIP filters defined on this 6611.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter determines the filtering mode for all outbound RIP filters defined on this 6611.	
Outbound RIP Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Filter ID (required for each outbound RIP filter defined) 1 to 128 None This parameter uniquely identifies this filter within the list displayed in the Configuration Program.	
Parameter **Valid Values** **Default** **Description**	Local network to filter on (required for each outbound RIP filter defined) A selection from the drop-down list (if the list is empty, no interface has been configured for XNS) None This parameter determines if routing information for a network is filtered on all local interfaces configured for XNS, or on an interface selected from the list displayed in the Configuration Program.	

Table 5-450 (Page 2 of 2). Configuration Worksheet - XNS Outbound RIP Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Network numbers to filter on All networks, Enter network number All networks This parameter defines routing information about the XNS network number. The network number is filtered on the interface on the interface identified in the Local XNS network to filter on parameter.	
Parameter **Valid Values** **Default** **Description**	Network number X'0000 0000' to X'FFFF FFFE' None This parameter defines the number of the XNS network whose routing information is filtered.	

Note: A maximum of 128 outbound RIP filters can be configured for this 6611.

Data Link Switching (DLSw)

DLSw enables SNA devices or NetBIOS stations to communicate with each other across an intervening IP network. The end station must rely on a 6611 attached to its network to provide a connection across the IP network to the remote station. DLSw uses TCP/IP transport and local acknowledgement to reliably transmit SNA and NetBIOS traffic from one end station to another. DLSw can either be:

- Remote (between two or more 6611s)

  Remote DLSw is used for SNA and NetBIOS transport. SNA and NetBIOS workstations attached to a 6611 use remote DLSw to communicate with SNA or NetBIOS workstations attached to another 6611. The 6611s are DLSw partners, which communicate across an intervening IP network.

- Local (one 6611 which performs SLDC to LLC conversion)

  Local DLSw is used for SNA transport only and can be provided for stations attached to a 6611 by an SDLC adapter when the destination host is attached to a LAN segment that is attached to a single 6611. During configuration, SDLC devices that are link-attached to the 6611 are assigned MAC sublayer addresses so that they appear to be on a LAN segment. When the 6611 is configured for DLSw at the system level, it will automatically use DLSw on its SDLC Adapter ports. Those ports must also be configured for SNA.

- Combination of local and remote

DLSw has the effect of making all end stations appear to be attached to a token-ring. Therefore, to the source station, the destination station appears to be attached to the ring.

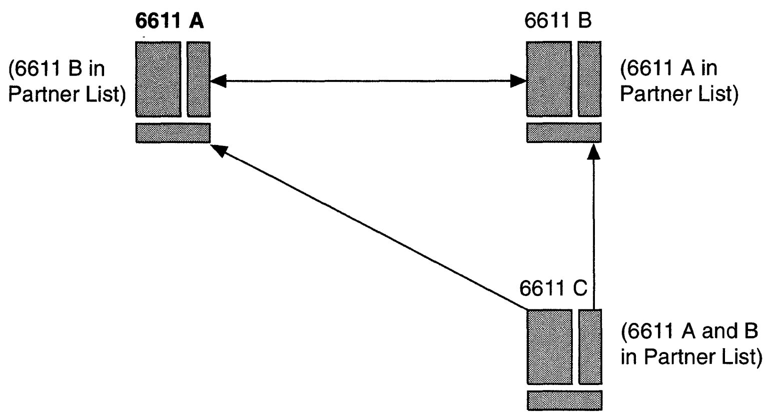
Notes:

1. In the Configuration Program, DLSw is configured with port parameters (see Table 5-452 on page 5-341) and with Node Configuration parameters.
2. To run DLSw, bridging must be configured at the port and node levels.
3. DLSw must be configured in order to run the APPN protocol.

Understanding DLSw Partner Configuration

DLSw encapsulation in IP frames occurs only between two DLSw partners. When you configure an 6611 for DLSw, you can configure so that it is authorized to communicate with some or all of its partners. If a 6611 specifies a device in its partner list, the 6611 will initiate a connection or call to that device, as shown in Figure 5-47 on page 5-340.

6611 A Partner List	6611 B Partner List	Accept Specific Connections Only	Call	Result
B	None	Disable on A and B	A→B	Accept
None	A	Disable on A and B	B→A	Accept
B	A	Disable A and B	A←→B	Accept
B	None	Enable on B	A→B	Reject; A not in B partner list
None	A	Enable on A	B→A	Reject; B not in A partner list
B	A	Enable on B	A←→B	Accept; A in B partner list
B	A	Enable on A	A←→B	Accept; B in A partner list
B	A	Enable on A and B	A←→B	Accept; A and B in each other's partner list



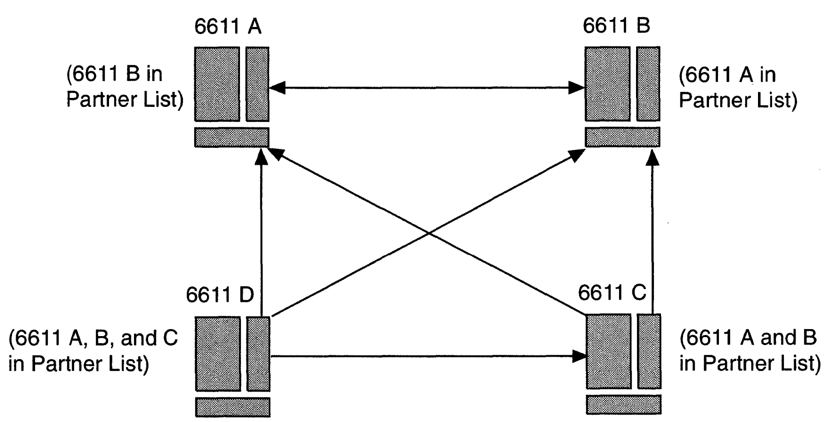


Figure 5-47. Sample Partner Connectivity Options

Port Types Supported

Table 5-451. Port Types Supported for SNA Transport via DLSw

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	√
X.25	CCITT X.25	X.25	√

Restrictions

You must configure the following functions when you want this 6611 to provide DLSw function:

Table 5-452 (Page 1 of 2). SNA and NetBIOS Configuration Requirements

Protocol	Adapter	Configuration Requirements
NetBIOS	Token-Ring or Ethernet	Token-ring ports must be configured for source route bridging and NetBIOS. Ethernet ports must be configured for transparent bridging and NetBIOS. Data link switching must be configured (NetBIOS enabled). NetBIOS must be configured on a token-ring port or Ethernet port. At least one data link switching partner must be defined and IP must be configured on some port.
SNA	Token-Ring or Ethernet	Token-ring ports must be configured for source route bridging and SNA. Ethernet ports must be configured for transparent bridging and SNA. Data link switching must be configured (SNA enabled). SNA must be configured on a token-ring port or Ethernet port. If there is no SDLC Adapter installed, then at least one data link switching partner must be defined and IP must be configured on some port. With an SDLC Adapter adapter installed, local DLSw can be performed; the configuration of IP and DLSw partners is not required for local DLSw.
SNA NetBIOS	Serial Port or V.35/V.36 Serial Port	Serial ports that handle encapsulated DLSw traffic must be configured for routing IP. If the serial port is also configured for bridging (Transparent or Source Route Bridging), then the appropriate outbound bridge filters must be established as Outbound Deny SAP *xx*, where *xx* corresponds to the protocol or protocols being data link switched. These bridge filters will prevent bridged sessions from being established when the DLSw function is desired for that traffic.

Table 5-452 (Page 2 of 2). SNA and NetBIOS Configuration Requirements

Protocol	Adapter	Configuration Requirements
SNA	SDLC	SDLC Adapter parameters must be configured. Each SNA station must be configured. Data link switching must be enabled (SNA enabled).

- Refer to "Advanced Peer-to-Peer Networking (APPN)" for APPN configuration requirements.
- You cannot use the following SAPs to route DLSw traffic:
  - X'E0' (reserved for IPX)
  - X'80' (reserved for XNS)
  - X'BC' (reserved for VINES)
- Do not configure more than 100 DLSw partners. If you specify more than 100 DLSw partners, the 6611 might not operate properly.

Configuration Changes...

That Require the Data Link Switching Function to Restart

- Node-level parameters
  - Protocols Forwarded by DLSw
    - SNA
    - NetBIOS
  - Virtual ring segment number
  - Destination cache timeout
  - Default DLSw IP Address for this 6611
  - Accept connections from specific 6611s only
  - IP address of remote 6611 router
- Port-level parameters
  - Enable LNM communication through this port

That Require the 6611 to Restart

None

Configuration Options

Table 5-453 on page 5-343 summarizes the configuration options for each adapter type that supports DLSw for LAN connections and for WAN connections. After configuring the appropriate bridging method and DLSw parameters on specific ports, you need to enable DLSw at the node level.

Table 5-453 (Page 1 of 2). DLSw Configuration Options

<table>
<tr><th>WHEN configuring local DLSw...</th><th>THEN optionally...</th></tr>
<tr><td>At the port level, configure at least one LAN port and one SDLC port whose information is data link switched:
• Token-ring port
– Enable source route bridging on this port.
– Specify the ring number of the LAN to which the port is attached.
• Ethernet port
– Enable transparent bridging on this port.
• SDLC port
– Configure SNA stations.</td><td>• If this port communicates with APPN or SNA end stations, enable SNA.
• Configure IP on this port.
Note: Local DLSw does not require the configuration of IP.</td></tr>
<tr><td>At the node level:
• Enable the appropriate bridging protocols.
– If this 6611 enables SDLC-attached SNA stations to communicate with a token-ring attached SNA device, enable source route bridging and specify the bridge number and designated ring number.
– If this 6611 enables SDLC-attached SNA stations to communicate with an Ethernet attached SNA device, enable translational bridging and specify the bridge number and designated ring number.
• Enable SNA DLSw.
• Specify the Virtual ring segment number.
• On the DLSw Partners window, set the Accept connections from specific IBM 6611s only parameter to Enable.</td><td>• Define SNA source and destination frame filters.</td></tr>
<tr><th>WHEN configuring remote DLSw...</th><th>THEN optionally...</th></tr>
<tr><td>At the port level, configure at least one LAN port whose information is data link switched:
• Token-ring port
– Enable source route bridging on this port.
– Specify the ring number of the LAN to which the port is attached.
– Enable SNA and/or NetBIOS, as appropriate.
• Ethernet port
– Enable transparent bridging on this port.
– Enable SNA and/or NetBIOS, as appropriate.
• SDLC port
– Configure SNA stations.
– Enable SNA.
Configure at least one WAN port for IP and ensure that it is attached to the network over which this 6611 communicates with its DLSw partners.
Note: IP must be enabled on each port that communicates with this 6611's DLSw partners.</td><td>• Adjust the Priority parameter on page 5-123 for TCP to suit your network's DLSw requirements. DLSw uses TCP ports 2065 and 2067. The Priority parameter is set by default to medium.</td></tr>
</table>

Table 5-453 (Page 2 of 2). DLSw Configuration Options

At the node level:

- Configure an IP router-to-router protocol (for example, OSPF) *or* static routes.
- Enable the source route bridging protocol.
  - Enable source route bridging and specify the bridge number and designated ring number when this 6611 enables devices on a token-ring LAN to communicate with devices on a remote LAN.
  - Enable transparent bridging when this 6611 enables devices on an Ethernet LAN to communicate with devices on a remote LAN.
- Enable SNA DLSw or NetBIOS DLSw, as appropriate.
- Specify the virtual ring segment number and the default DLSw address for this 6611.
- Specify the DLSw partners. Read "Understanding DLSw Partner Configuration" on page 5-339 for more information.
- Specify the destination cache timeout, SNA transmission bias, and maximum NetBIOS frame size.
- Configure default destinations for SNA and NetBIOS to eliminate extraneous searching when explorer frames are received.
- Define filters.

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform DLSw. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-454 (Page 1 of 2). DLSw Configuration Verification Checklist

DLSw Rule	**Configuration Parameter**	√
Node-Level Parameters:		
If SNA traffic is to be routed using DLSw, both 6611s must have the Enable SNA DLSw parameter enabled.	Enable SNA DLSw	
If NetBIOS traffic is to be routed using DLSw, then both 6611s must have the Enable NetBIOS DLSw parameter enabled.	Enable NetBIOS DLSw	
Ensure that the value of the Default DLSw IP address for this 6611 parameter is included in the DLSw partner list of the remote 6611.	IP address of remote router	
	Default DLSw IP address for this 6611	

Table 5-454 (Page 2 of 2). DLSw Configuration Verification Checklist		
DLSw Rule	**Configuration Parameter**	√
If the Enable SNA DLSw parameter is enabled and SNA source or destination frame filters are set to **Deny**, the list of filters must not contain any of the MAC addresses of the DLSw SNA devices.	Enable SNA DLSw	
	Source address (source) or Destination address (destination)	
	Enable SNA source frame filters (source) Enable SNA destination frame filters (destination)	
	Filtering mode	
	Destination MAC address	
For a given serial DLSw connection, the following parameters must have the same values on both 6611s at either end of the connection: • Data encoding • Framing method	Data encoding	
	Framing method	
For an X.25 DLSw connection, the value of the DTE address parameter on the local and remote 6611 must be the same.	DTE address	
For an X.25, serial PPP, or serial frame-relay connection when the Use InARP to resolve remote protocol addresses parameter is set to **Disable**, the local and destination IP addresses must match.	IP address	
	Use InARP to resolve remote protocol addresses	
Ensure that the Virtual ring number parameters have the same value on all 6611s that are DLSw partners.	Virtual ring number	
Port-Level Parameters:		
For all ports that connect each 6611 to the LAN or the WAN, the Enable interface parameter must be enabled.	Enable physical interface on this port	
When 2 6611s are connected by a token-ring LAN, the ports that connect each 6611 to the LAN must have the following values: • The ports on each 6611 must be of the same adapter type. • The Enable Source Route Bridging on this port parameter must be enabled. • The Enable SNA frame forwarding on this port parameter and/or the Forward NetBIOS frames on this port parameter must be enabled.	Enable Source Route Bridging on this port	
	Enable SNA frame forwarding on this port	
	Forward NetBIOS frames on this port	
When 2 6611s are connected by an Ethernet LAN, the ports that connect each 6611 to the LAN must have the following values: • The ports on each 6611 must be of the same adapter type. • The Enable transparent bridging on this port parameter must be enabled. • The Enable SNA frame forwarding on this port parameter and/or the Forward NetBIOS frames on this port parameter must be enabled.	Enable transparent on this port	
	Enable SNA frame forwarding on this port	
	Forward NetBIOS frames on this port	
When 2 6611s are connected by a WAN, the ports that connect each 6611 to the WAN must have the following values: • The Enable IP routing on this port parameter must be enabled • The IP address parameter must be configured.	Enable IP routing on this port	
	IP address	

Estimating DLSw Storage Requirements

Developing an DLSw configuration requires careful design and planning for efficient utilization of available system resources. To assist you in planning your configuration and determining your 6611 memory needs, IBM provides a storage estimating tool called the IBM 6611 Storage Estimate EXEC. For information on this tool, contact your IBM marketing representative and ask for the Internetworking Marketing Specialist for your trading area.

Sample Network Graphic

Figure 5-48 shows a sample network in which the 6611s are configured for data link switching. The 3745 is token-ring attached. 6611 A is connected to Ring 2 via a token-ring port and to the telecommunications link via a serial port. 6611 B is connected to Ring 5 via a token-ring port and to the telecommunications link via a serial port.

For additional local and remote DLSw configuration examples, see Appendix A on page A-1.

The following information is shown in Figure 5-48:

- IP addresses
- Slot and port numbers, abbreviated s*x* p*y*
- Ring numbers and ring speeds

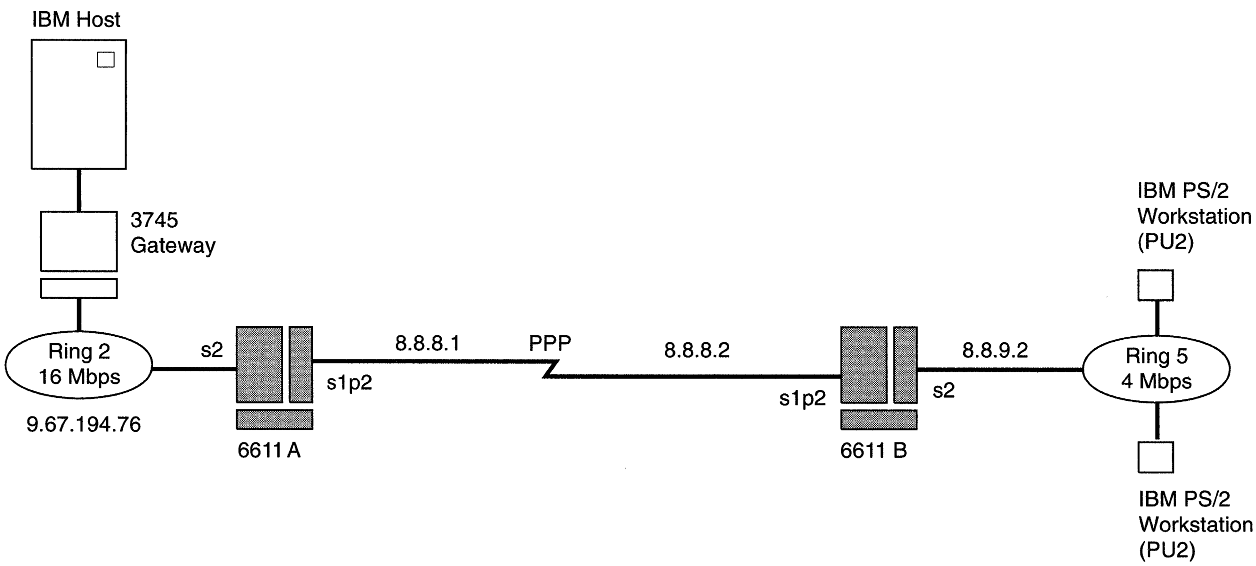


Figure 5-48. Sample Network Using Data Link Switching

The sample network shows the configuration of:

- DLSw between routers 6611 A and 6611 B
- SNA on the attached token-rings

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-48 on page 5-346. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and the Protocols Running on Them

Table 5-455. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-456. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Cylink serial number	None	None
Serial line speed	19200	19200
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table 5-457. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-458. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.1	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.2	8.8.8.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	Disable	Disable
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table 5-459. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	16 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-460. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable Source Route Bridging on this port	Enable	Enable
Spanning tree mode	Automatic	Automatic
Path cost	0	0
Port priority for Translational Bridging	80	80
Port state	NA	NA
Ring number	2	5
Max. transmission unit (octets)	2052	2052

Table 5-461. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.194.76	8.8.9.2
Subnet mask	255.255.240.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Table 5-462. Token-Ring Port - SNA Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable SNA frame forwarding on this port	Enable	Enable
SAP value	00, 04	00, 04

Node-Level Parameters Configured

Table 5-463. Node Level - Source Route Bridging Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Source Route Bridging	Enable	Enable
Bridge number	4	4
Enable LAN Bridging Protocol	Enable	Enable
Designated ring number	2	5
Spanning tree parameters		
Bridge priority	8000	8000
Hello time	2	2
Forward delay time	15	15
Max age	20	20

Node-Level Parameters Configured - Area 0.0.0.0

Table 5-464. Node Level - OSPF Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable OSPF	Enable	Enable
Router ID	8.8.8.1	8.8.8.2

Table 5-465. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 A Value	6611 B Value
Area ID	0.0.0.0	0.0.0.0
Area type	NA	NA
Stub cost	NA	NA
Authentication type	None	None

Table 5-466. Node Level - OSPF Interface Detail Parameters Configured

Parameter	6611 A Value 1	6611 A Value 2	6611 B Value 1	6611 B Value 2
Interface IP address	8.8.8.2	9.67.194.76	8.8.8.1	8.8.9.2
Interface type	NA	Broadcast	NA	Broadcast
Authorization key	NA	NA	NA	NA
Retransmit interval	5	5	5	5
Router priority	1	1	1	1
Interface transit delay	1	1	1	1
Cost	65	6	65	6
Router dead interval	40	40	40	40
Poll interval	NA	NA	NA	NA
Hello interval	10	10	10	10

Table 5-467. Node Level - DLSw Parameters Configured

Parameter	6611 A Value	6611 B Value
Protocols forwarded by DLSw		
SNA	Enable	Enable
NetBIOS	Disable	Disable
SNA transmission bias	NA	NA
Maximum NetBIOS frame size	2052	2052
DLSw parameters		
Virtual ring segment number	FAB	FAB
Destination cache timeout	8	8
Default DLSw IP address for this 6611	9.67.194.76	8.8.9.2

Table 5-468. Node Level - DLSw Partners Parameters Configured

Parameter	6611 A Value	6611 B Value
Accept connections from specific 6611s only	Disable	Disable
IP address of remote 6611 router	8.8.9.2	9.67.194.76

Node Level Worksheets

Figure 5-49 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-49.

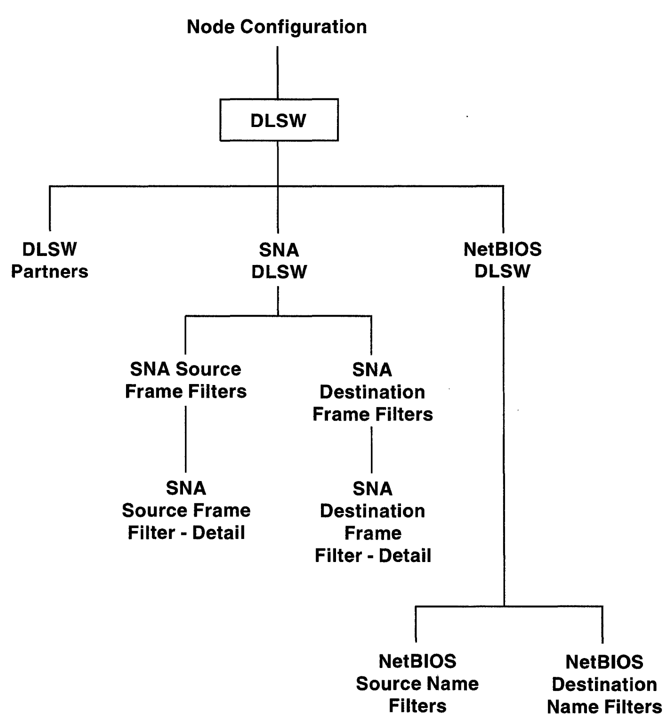


Figure 5-49. Flow of Node Level Data Link Switching Help Windows

Use the following tables as worksheets for your node level configurations.

- DLSw on page 5-351
- DLSw Partners on page 5-352

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-9 on page D-11 for a mapping of parameter names and their associated labels.

Table 5-469 (Page 1 of 2). Configuration Worksheet - DLSw

Parameter Information		Your Value
Parameter	SNA	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables the forwarding of SNA frames.	
Parameter	NetBIOS	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables the forwarding of NetBIOS frames.	
Parameter	SNA transmission bias	
Valid Values	0 to 9	
Default	0	
Description	This parameter specifies the ratio of SNA to NetBIOS frames to be transmitted across a WAN connection by DLSw. A value of 0 means that there is no bias for SNA traffic. SNA and NetBIOS frames are sent over the TCP/IP connection in the same order in which they are received. A value of 1 to 9 represents the number of SNA frames that should be sent after each NetBIOS frame is sent (assuming that there are at least that number of SNA frames waiting to be sent).	
Parameter	Maximum NetBIOS frame size	
Valid Values	516, 1500, or 2052 octets	
Default	2052 octets	
Description	This parameter specifies the maximum size of NetBIOS frames that will be passed through this 6611 by DLSw. When used with the SNA transmission bias parameter, this parameter also enables you to better control the flow of SNA frames across the WAN.	
Parameter	Virtual ring segment number (required when forwarding SNA or NetBIOS frames)	
Valid Values	X'0' to X'FFF'	
Default	None	
Description	This parameter specifies the virtual token-ring network segment number that is used in all frames passed to or from the 6611 data link switching function. It also represents the value that is assigned to the segment number that is placed in the token-ring routing information (RI) field to address frames to the data link switching function.	

Table 5-469 (Page 2 of 2). Configuration Worksheet - DLSw

Parameter Information		Your Value
Parameter	Destination cache timeout	
Valid Values	1 to 20 minutes	
Default	8 minutes	
Description	This parameter defines how long a MAC address or NetBIOS name will remain in cache memory without active communications. DLSw creates an entry in cache memory at the beginning of an SNA or NetBIOS session. The entry contains a MAC address or NetBIOS name and the destination IP address . If no frames flow over that session for the time alloted by this parameter, DLSw purges the entry from the cache. **For NetBIOS Only:** This parameter also defines the length of time that a NetBIOS name that is marked as unreachable remains unreachable. When a NetBIOS name is marked as unreachable, the 6611 does not send queries to attempt to locate it in the network. **Note:** The feature of the Destination cache timeout parameter that enables you to control NetBIOS negative caching can be disabled separately using the System Manager. For more information, read the *MPNP Operations and Problem Management Guide.*	
Parameter	Default DLSw IP address for this 6611 (required when forwarding SNA or NetBIOS frames)	
Valid Values	A valid IP address	
Default	None	
Description	This parameter defines the IP address that DLSw partners use when sending SNA or NetBIOS frames to this IBM 6611 across an IP network. If a valid IP address is not given, the DLSw function chooses an IP address which corresponds to the interface over which the initial connection to a remote IBM 6611 is made.	

Table 5-470 (Page 1 of 2). Configuration Worksheet - DLSw Partners

Parameter Information		Your Value
Parameter	Accept connections from specific IBM 6611s only	
Valid Values	Enable, Disable	
Default	Disable	
Description	When this parameter is set to **Enable**, this 6611 accepts a request to establish a DLSw connection (to become a DLSw partner) from other 6611s that appear in the set defined by the responses to the IP address of remote 6611 parameter. When this parameter is set to **disable**, this 6611 accepts a DLSw connection request from any 6611. **Note:** If you enable this parameter, you must define at least one DLSw partner.	

Table 5-470 (Page 2 of 2). Configuration Worksheet - DLSw Partners

Parameter Information		Your Value
DLSw Partner List - Parameter configured for each partner defined		
Parameter	IP address of remote 6611 router (required for each DLSw partner defined)	
Valid Values	A valid IP address	
Default Value	None	
Description	This parameter specifies the IP address for each 6611 with which this 6611 may establish a data link switching (DLSw) connection. The DLSw function will reject or accept connection requests from 6611s whose IP addresses have not been configured for this parameter. This rejection or acceptance is based on the value established in the Accept connections only from specific 6611s parameter. Configure this parameter for each remote 6611 to which this 6611 communicates with DLSw. **Note:** This parameter is required when the Accept connections only from DLSw partners parameter is enabled.	

Network Basic Input/Output System (NetBIOS)

NetBIOS is a LAN protocol used to communicate between two stations on a LAN. The user must assign each station a NetBIOS name. NetBIOS establishes a connection-oriented session between two NetBIOS names.

Port Types Supported

Table 5-471. Port Types Supported for NetBIOS Transport via DLSw

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	√

Restrictions

- The following protocols must be configured before you can route NetBIOS using DLSw:
  - DLSw
  - Source route bridging (on a token-ring port or a serial adapter)
  - Transparent bridging (on an Ethernet port)
  - IP (for remote DLSw)
- The SAP X'F0' is reserved for NetBIOS.

Configuration Changes ...

That Require the NetBIOS Function to Restart

Port-level parameters

- Forward NetBIOS frames on this port
- Forward NetBIOS datagram and datagram broadcast message on this port

Node-level parameters

- Default destination parameters
  - Destination name
  - IP address of destination router
- Destination name filter parameters
  - Enable NetBIOS destination name filters
  - Filtering mode
  - Destination name

- Source name

- Source name filter parameters
  - Enable NetBIOS source name filters
  - Filtering mode
  - Destination name
  - Source name

That Require the 6611 to Restart

None

Before You Configure...

This section contains additional information to assist you in configuring NetBIOS.

- Default Destinations

  The 6611 allows you to define default destinations for NetBIOS. A default destination is composed of a NetBIOS name, representing an end station, and an IP address, representing a router. The 6611 uses default destinations to route address resolution frames destined for the specified NetBIOS end station to a router without performing a broadcast search on the network. Refer to the *Introduction and Planning Guide* for more information about default destinations.

- Name Filters

  NetBIOS allows you to define a set of filters which are applied to frames transported using DLSw. The purpose of filtering is to allow or disallow connection establishment between NetBIOS stations. Each filter is composed of a source name and a destination name. The filter compares the source name and destination name of each NetBIOS explorer frame with the configured list, then either forwards or discards the frame based on the comparison. Source name filters are applied on traffic travelling from a LAN connection to a WAN connection. Destination name filters are applied on traffic travelling from a WAN connection to a LAN connection. Refer to the *Introduction and Planning Guide* for more information about NetBIOS name filters.

  Note: When defining the NetBIOS names on your LANs, it is recommended that you use all upper or all lower case letters in NetBIOS names. By using names with only one case, you limit the number of filters you need to specify for bridging and data link switching. When you specify less NetBIOS filters in your 6611 configuration, the 6611's performance improves significantly.

- Destination cache timeout

  The Destination cache timeout parameter for DLSw determines how long a NetBIOS name will remain in the cache. DLSw learns about the reachability of NetBIOS names by examining NetBIOS broadcast frames. When the 6611 discovers that a name is reachable, the name is put in the name cache and is marked as reachable and as local or remote. If the name is marked as remote, the address of the router where the name is located is also put in the cache. The name remains in the cache as long as broadcast frames are received for that name. If no broadcast frames are received for a name for the duration of the specified cache timeout period, the name is deleted from the cache.

  If a NetBIOS Name_Query for a name is not answered, the name is put in the cache and marked as not reachable. The name remains marked as not reachable for the cache timeout period. When the cache timeout period expires and a broadcast frame is not received from that name, the name is deleted from the cache. When a broadcast frame is received before the cache timeout period expires, the name is marked as reachable and is retained in the cache.

Broadcast frames destined for a name that is marked as not reachable in the cache are dropped. Broadcast frames destined for a name that is marked as reachable are sent only to the router where the name is known to be. Broadcast frames destined for names that are not in the cache are broadcast to all DLSw partners.

Configuration Options

Table 5-472 summarizes the configuration options for each adapter type that supports NetBIOS. After configuring NetBIOS on specific ports, you need to enable DLSw at the node level.

Table 5-472. NetBIOS Configuration Options

WHEN configuring NetBIOS...	THEN optionally...
...on the node level: • Enable NetBIOS frame forwarding. • Create a list of default destinations.	• Define source name filters. • Define destination name filters.
...on the port level: • Enable NetBIOS frame forwarding. • Enable NetBIOS datagram and datagram broadcast message.	

Port Level Worksheet

Use the following table as a worksheet for your port level configurations.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-16 on page D-15 for a mapping of parameter names and their associated labels.

Table 5-473. Configuration Worksheet - Port Parameters - NetBIOS

Parameter Information	Your Value
Forward on this port	
Parameter NetBIOS frames **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables NetBIOS frame forwarding on this port.	
Parameter NetBIOS datagram and datagram broadcast message **Valid Values** Enable, Disable **Default** Enable **Description** This parameter enables or disables the forwarding of NetBIOS datagram and datagram broadcast messages on this port.	

Node Level Worksheets

Use the following tables as worksheets for your node level configurations.

- NetBIOS DLSw on page 5-357
- NetBIOS Source Name Filters on page 5-357
- NetBIOS Destination Name Filters on page 5-358

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-16 on page D-15 for a mapping of parameter names and their associated labels.

Table 5-474. Configuration Worksheet - NetBIOS DLSw

Parameter Information	Your Value
NetBIOS Default Destination List - Parameters configured for each default desintation defined	
Parameter Destination name (required) **Valid Values** Any valid NetBIOS name **Default** None **Description** This parameter defines the NetBIOS destination name of the NetBIOS station serviced by this 6611. The 6611 is specified in the IP address of destination router parameter. Together, a destination name and an IP address (of the destination router) form a default destination.	
Parameter IP address of destination router (required) **Valid Values** Any IP address **Default** None **Description** This parameter defines the IP address of the router which acts as the default destination.	

Note: You can configure up to 100 default destinations.

Table 5-475 (Page 1 of 2). Configuration Worksheet - NetBIOS Source Name Filters

Parameter Information	Your Value
Parameter Enable source name filters **Valid Values** Enable, Disable **Default** Disable **Description** This parameter enables or disables the use of source name filters.	
Parameter Filtering mode **Valid Values** Deny, Permit **Default** Deny **Description** This parameter defines the type of source name filter. If you choose **Deny**, all frames that match the filter will not be forwarded. If you choose **Permit**, all frames that match the filter will be forwarded.	
Source Name Filter List - Parameters configured for each filter defined	
Parameter Source name (required) **Valid Values** Any valid NetBIOS name **Default** None **Description** This parameter defines a source name for a NetBIOS source name filter. Source name filters are applied to NetBIOS explorer frames received from the local area network (LAN) and transferred via the wide area network (WAN) to the destination.	

Table 5-475 (Page 2 of 2). Configuration Worksheet - NetBIOS Source Name Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Destination name (required) Any valid NetBIOS name None This parameter defines the destination name used in NetBIOS source name filters. Source name filters are applied to NetBIOS explorer frames received from the local area network (LAN) and transferred via the wide area network (WAN) to the destination.	

Table 5-476. Configuration Worksheet - NetBIOS Destination Name Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable destination name filters Enable, Disable Disable This parameter enables or disables the use of destination name filters.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter defines the type of destination name filter. If you choose **Deny**, all frames that match the filter will not be forwarded. If you choose **Permit**, all frames that match the filter will be forwarded.	
Destination Name Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Destination name (required) Any valid NetBIOS name None This parameter specifies a destination name used in NetBIOS destination name filters. Destination name filters are applied to NetBIOS frames received off the wide area network (WAN) and destined for the local area network (LAN).	
Parameter **Valid Values** **Default** **Description**	Source name (required) Any valid NetBIOS name None This parameter specifies a source name used in NetBIOS destination name filters. Destination name filters are applied to NetBIOS frames received off the wide area network (WAN) and destined for the local area network (LAN).	

Systems Network Architecture (SNA)

Developed by IBM in the early 1970s, SNA is a seven-layer architecture that was designed to distribute computing functions usually performed by a centralized host computer to other specializing communications processors in the network. Typically, SNA routes data over SDLC switched or unswitched communications lines and token-ring LAN segments. SNA networks range from very small networks to extremely large networks consisting of hundreds of thousands of users.

Enhancements to SNA, such as Advanced-Peer-to-Peer Networking (APPN), have moved SNA from a hierarchical network architecture to an architecture supporting both older, non-APPN equipment, as well as newer peer-to-peer and client/server networks.

The 6611 uses a technique of tranporting SNA data called data link switching (DLSw). APPN Network Node server functions are optional and are described in "Advanced Peer-to-Peer Networking (APPN)" on page 5-364.

Port Types Supported

Table 5-477. Port Types Supported for SNA Transport via DLSw

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	√
X.25	CCITT X.25	X.25	√

Restrictions

- The following protocols must be configured before you can route SNA traffic using DLSw:
  - DLSw
  - Source route bridging (for a Token-Ring Port or a serial adapter)
  - Transparent bridging (for an Ethernet port)
  - IP (for remote DLSw)
- You cannot use the following SAPs to route SNA using DLSw:
  - X'E0' (reserved for IPX)
  - X'80' (reserved for XNS)
  - X'BC' (reserved for VINES)
  - X'F0' (reserved for NetBIOS)

  The SAPs X'04' and X'08' are reserved for SNA.

Configuration Changes...

That Require the SNA Function to Restart

Node-level parameters

- Default destination parameters
  - MAC address
  - IP address
- Destination frame filter parameters
  - Enable SNA destination frame filters
  - Filtering mode
  - Destination address
  - Destination address mask
  - Source address
  - Source address mask
- Source name filter parameters
  - Enable SNA source frame filters
  - Filtering mode
  - Destination address
  - Destination address mask
  - Source address
  - Source address mask

Port-level parameters

- Enable SNA frame forwarding on this port
- SAP value

That Require the 6611 to Restart

None

Configuration Options

Table 5-478 summarizes the configuration options for each adapter type that supports SNA. After configuring SNA on specific ports, you need to enable DLSw at the node level.

Table 5-478. SNA Configuration Options

WHEN configuring SNA...	THEN optionally...
...on the node level: • Enable the forwarding of SNA traffic.	• Create a list of default destinations. • Define source frame filters. • Define destination frame filters.
...on the port level: • Enable SNA frame forwarding on the port. • Define SAP values.	

Before You Configure...

This section contains additional information to assist you in configuring SNA.

- Default Destinations

  The 6611 allows you to define default destinations for SNA. A default destination is composed of a MAC address, representing an SNA station, and an IP address, representing a router. The 6611 uses default destinations to route explorer frames destined for specified SNA station to a router without performing a search on the network. Refer to the *Introduction and Planning Guide* for more information about default destinations.

- Frame Filters

  SNA allows you to define a set of filters which are applied to frames transported using DLSw. The purpose of filtering is to allow or disallow connection establishment between SNA stations. Each filter is composed of a source MAC address and a destination MAC address. The filter compares the source MAC address and destination MAC address of each SNA explorer frame with the configured list, then either forwards or discards the frame based on the comparison. Source frame filters are applied to frames travelling from a LAN connection to a WAN connection. Destination frame filters are applied to frames travelling from a WAN connection to a LAN connection. Refer to the *Introduction and Planning Guide* for more detailed information about frame filters.

Port Level Worksheets

Use the following table as a worksheet for your port level configurations.

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-19 on page D-16 for a mapping of parameter names and their associated labels.

Table 5-479. Configuration Worksheet - Port Parameters - SNA

Parameter Information		Your Value
Parameter	Enable SNA frame forwarding on this port	
Valid Values	Enable, Disable	
Default	Disable	
Description	This parameter enables or disables SNA frame forwarding on this port.	
Parameter	SAP value (required for each unique SAP value defined)	
Valid Values	X'00' to X'EC', in increments of 2	
Default	X'00', X'04'	
Description	This parameter defines a SAP value which will be forwarded by DLSw.	

Node Level Worksheets

Use the following tables as worksheets for your node level configurations.

- SNA DLSw on page 5-362
- SNA Source Frame Filters on page 5-362
- SNA Destination Frame Filters on page 5-363

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter.

If you are working with an ASCII-formatted configuration file, refer to Table D-19 on page D-16 for a mapping of parameter names and their associated labels.

Table 5-480. Configuration Worksheet - SNA DLSw

Parameter Information		Your Value
Default Destination List - Parameters configured for each default destination defined		
Parameter **Valid Values** **Default** **Description**	IP address of destination router (required) Any IP address None This parameter defines the IP address of the router which acts as the default destination.	
Parameter **Valid Values** **Default** **Description**	Destination MAC address (required) 12 hex digits None This parameter represents a token-ring destination medium-access control (MAC) address. The default destination is configured based on this address (the default destination router is determined in the IP address of designated router parameter).	

Note: You can configure up to 100 default destinations.

Table 5-481. Configuration Worksheet - SNA Source Frame Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable SNA source frame filters Enable, Disable Disable This parameter enables or disables the use of source frame filters.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter defines the type of source frame filter. If you choose **Deny**, all frames that match the filter will not be forwarded. If you choose **Permit**, all frames that match the filter will be forwarded.	
SNA Source Frame Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Source address (required) X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the source MAC address used in this filter.	
Parameter **Valid Values** **Default** **Description**	Source address mask X'0000 0000 0000' to X'FFFF FFFF FFFF' X'FFFF FFFF FFFF' This parameter defines the mask used with the Source address parameter.	
Parameter **Valid Values** **Default** **Description**	Destination address X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the destination MAC address used in this filter.	
Parameter **Valid Values** **Default** **Description**	Destination address mask X'0000 0000 0000' to X'FFFF FFFF FFFF' X'FFFF FFFF FFFF' This parameter defines the mask used with the Destination address parameter.	

Note: A maximum of 100 source frame filters may be configured.

Table 5-482. Configuration Worksheet - SNA Destination Frame Filters

Parameter Information		Your Value
Parameter **Valid Values** **Default** **Description**	Enable SNA destination frame filters Enable, Disable Disable This parameter enables or disables the use of destination frame filters.	
Parameter **Valid Values** **Default** **Description**	Filtering mode Deny, Permit Deny This parameter defines the type of destination frame filter. If you choose **Deny**, all frames that match the filter will not be forwarded. If you choose **Permit**, all frames that match the filter will be forwarded.	
SNA Destination Frame Filter List - Parameters configured for each filter defined		
Parameter **Valid Values** **Default** **Description**	Source address (required) X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the source MAC address used in this filter.	
Parameter **Valid Values** **Default** **Description**	Source address mask X'0000 0000 0000' to X'FFFF FFFF FFFF' X'FFFF FFFF FFFF' This parameter defines the mask used with the Source address parameter.	
Parameter **Valid Values** **Default** **Description**	Destination address X'0000 0000 0000' to X'FFFF FFFF FFFF' None This parameter defines the destination MAC address used in this filter.	
Parameter **Valid Values** **Default** **Description**	Destination address mask X'0000 0000 0000' to X'FFFF FFFF FFFF' X'FFFF FFFF FFFF' This parameter defines the mask used with the Destination address parameter.	

Note: A maximum of 100 destination frame filters may be configured.

Advanced Peer-to-Peer Networking (APPN)

APPN is an enhancement to IBM's SNA architecture and allows nodes to communicate as peers without requiring the services of an SNA host computer. APPN nodes are classified as type 2.1 (T2.1) nodes and extend the capabilities of T2.1 low-entry networking (LEN) nodes. Like LEN nodes, each APPN node contains a *control point* (CP) that is responsible for managing the resources of the node. Unlike LEN nodes, APPN nodes can share information about resources through CP-CP sessions, reducing the need to define the location of resources in the network.

The APPN architecture defines two types of APPN nodes: *network nodes* and *end nodes*. Network nodes provide directory, route selection, and management services for attached end nodes. End nodes provide limited directory, route selection, and management services for logical units (LUs) associated with the end node.

The 6611 functions as a network node within an APPN network. As a network node, the 6611 can provide services to attached APPN end nodes and act as an intermediate node that routes data between adjacent network nodes. The 6611 network node also supports connections to LEN end nodes. Such connections can serve as entry points into an SNA subarea network.

For more information about how APPN is implemented on the 6611, refer to the *Introduction and Planning Guide*.

Port Types Supported

APPN is not configured on individual adapters, but supports definitions for SNA, Data link switching (DLSw), and IP. (See "Before You Configure..." on page 5-365 for information about configuring the protocols that support APPN routing on the 6611.)

Table 5-483. Port Types Supported for APPN Routing

Port Type	Standard	Framing	Supported?
Ethernet	Version 2	Type	√
	IEEE 802.3	LLC	√
		SNAP	√
Token-Ring Network	IEEE 802.5	LLC	√
		SNAP	√
EIA 422/449 Serial and V.35/V.36 Serial		PPP	√
		Frame Relay	√
		LAN Bridging Protocol	NA
4-Port SDLC		SDLC	
X.25	CCITT X.25	X.25	√

Restrictions

The 6611 does not provide transmission priority based on class of service (COS). As a result, care must be taken to ensure that when SNA traffic is routed over an intervening telecommunication link, the link data rate is adequate to support the traffic volume. In addition, the 6611 does not provide a method for defining new classes of service. The 6611 does, however:

- Service session requests for mode names that map to the architected classes of service.
- Calculate least-weight routes based on COS and transmission group (TG) characteristics in accordance with the APPN architecture.
- Enable you to use the Configuration Program to modify TG characteristics for APPN link stations. The TG characteristics you specify can influence the selection of routes through the APPN network node.
- Enable you to use the System Manager to view an APPN COS file, add a mode name to the file, or modify user-defined TG characteristics within the file.
- Enable you to retrieve and modify an APPN COS file.

Configuration Changes...

That Require the APPN Function to Restart

- Network ID
- Control point name
- XID ID number (of network node)
- Locally administered MAC address (of network node)
- SAP address (of network node)
- Accept connection requests from any node
- Adjacent node type
- The following Node Tuning parameters:
  - Max. number of APPN network nodes
  - Max. number of serviced end and LEN nodes
  - Avg. number of LUs for serviced nodes
  - Maximum shared memory
  - Maximum cached directory entries

That Require the 6611 to Restart

None

Before You Configure...

This section contains additional information to assist you in configuring the APPN protocol.

Configuration Requirements for APPN

To use APPN to route SNA traffic, the following protocols must be configured and enabled.

- At the port level:
  - SNA and source route bridging on ports for token-ring LANs that contain APPN nodes and LEN end nodes that are part of the APPN network.

- SNA and transparent bridging on ports for Ethernet LANs that contain APPN nodes and LEN end nodes that are part of the APPN network.
- IP over PPP or IP over frame relay on serial adapter ports that provide serial links between 6611 network nodes across a WAN.

- At the node level:
  - Source route bridging for token-ring connections and transparent bridging for Ethernet connections, or translational bridging for both types of connections.
  - DLSw, including the enabling of SNA as the protocol to be forwarded by DLSw.
  - APPN routing.

APPN's Utilization of Data Link Switching and IP

This section describes how APPN uses DLSw to communicate with adjacent nodes on a LAN, and either DLSw or IP to communicate with 6611 network nodes across a WAN.

Connectivity to Adjacent Nodes on a LAN: APPN, as implemented on the 6611, relies on DLSw to provide a connection-oriented interface (802.2 LLC type 2) between the 6611 network node and LAN-attached APPN nodes and LEN end nodes. The DLSw function uses bridging to transport SNA frames encapsulated in a MAC sublayer frame to and from LAN-attached nodes served by the 6611 network node. During configuration, the 6611 network node is assigned a unique MAC and SAP address pair that enables it to communicate with DLSw. The MAC address for the network node is locally administered and must not correspond to any physical MAC address in the DLSw network.

Because APPN nodes can initiate CP-CP sessions with the 6611 network node, these nodes do not need to be defined to the 6611. In general, when configuring APPN on the 6611, you can simplify the task considerably by allowing the 6611 network node to accept connection requests from any node. Configuring the network node in this manner eliminates the need to define information about adjacent nodes, except in the following cases:

- The adjacent node is a LEN end node. LEN end nodes do not support CP-CP sessions, so information about such nodes and their LU resources must be configured on the 6611 network node.
- You want the 6611 network node to be able to initiate a CP-CP session with an adjacent APPN node.

In these cases, you must specify information about the adjacent node when configuring the 6611 network node. Because the adjacent node is reached through a DLSw connection, the node is referred to as a *DLSw adjacent node* for configuration purposes.[3]

If you want to control which APPN nodes can initiate CP-CP sessions with the 6611 network node, you can configure the network node to accept connection requests from explicitly defined nodes only. When you configure the 6611 network node in

3 This term is used only within the Configuration Program to identify how an adjacent node communicates with the 6611 network node.

this manner, you must specify information about each adjacent node that is allowed to communicate with the network node.

Table 5-484 summarizes the connection options available for the 6611 network node and adjacent nodes connected to a LAN. Normally, end nodes serviced by the 6611 network node are connected to a LAN that is locally attached to the 6611. However, the 6611 network node can service an end node that is connected to a LAN on another 6611 network node. In either case, the end nodes are defined as shown in Table 5-484.

Table 5-484 (Page 1 of 2). Connection Options for 6611 Network Node and Adjacent Nodes on a LAN

WHEN Adjacent Node Type Is...	**AND this 6611 Is Configured to Accept Connection Requests...**	**THEN These Connection Options Are Available...**
APPN node	From any node	• Adjacent node initiates connection with this 6611 network node: – Adjacent node specifies MAC/SAP address used by this 6611 to communicate with DLSw – No adjacent node definition required on this 6611 *or* • This 6611 network node initiates connection: – 6611 specifies adjacent node's physical MAC address and its SAP address – 6611 activates link to adjacent node automatically (Activate link automatically parameter is enabled)
APPN node	From explicitly defined nodes only	• Adjacent node initiates connection with this 6611 network node: – Adjacent node specifies MAC/SAP address used by this 6611 to communicate with DLSw – This 6611 specifies adjacent node's physical MAC address, SAP address, and fully qualified control point name. This 6611 does not activate link to adjacent node (Activate link automatically parameter is disabled) *or* • This 6611 network node initiates connection: – 6611 specifies adjacent node's physical MAC address, SAP address, and fully qualified control point name. – 6611 activates link to adjacent node automatically (Activate link automatically parameter is enabled)

Table 5-484 (Page 2 of 2). Connection Options for 6611 Network Node and Adjacent Nodes on a LAN

WHEN Adjacent Node Type Is...	AND this 6611 Is Configured to Accept Connection Requests...	THEN These Connection Options Are Available...
LEN end node	Either from any node or from explicitly defined nodes only	• LEN end node initiates connection with this 6611 network node: – LEN end node specifies MAC/SAP address used by this 6611 to communicate with DLSw – This 6611 specifies LEN end node's physical MAC address, SAP address, and fully qualified control point name, and any LU resources on the LEN end node that this 6611 may need to locate. This 6611 does not activate link to LEN end node (Activate link automatically parameter is disabled) *or* • This 6611 network node initiates connection: – 6611 specifies LEN end node's physical MAC address, SAP address, and fully qualified control point name, and any LU resources on the LEN end node that the 6611 may need to locate. – 6611 activates link to LEN end node automatically (Activate link automatically parameter is enabled)

Notes:

- Because LEN end nodes do not support CP-CP sessions, they cannot register their LU resources with the 6611 network node. For the 6611 to locate an LU on a LEN end node, the LU must be defined on the 6611 (unless the LU name is the same as the CP name of the LEN node).
- A single transmission group, or link, can be defined between the 6611 network node and any specific adjacent node. APPN, as implemented on the 6611, does not support parallel connections to the same adjacent node (control point).

Connectivity to 6611 Network Nodes across a WAN: Across a WAN (using a serial link), the 6611 network node can communicate with other 6611 network nodes in one of two ways:

- Directly, using IP.
- Through the remote DLSw function.

Figure 5-50 on page 5-369 illustrates the two ways in which CP-CP sessions can flow through the 6611 network node. Sample network A shows a CP-CP session between two 6611 network nodes using a direct IP connection. In this example, DLSw transfers frames to the APPN component in the 6611 network node and APPN hands off the frames to the Transmission Control Protocol (TCP). TCP, which ensures that the session between the 6611 nodes on the WAN is reliable (connection-oriented), passes the frames to the IP protocol for transport across the WAN.

Sample network B shows a CP-CP session between two 6611 network nodes using the remote DLSw function. In this example, the frames flow through the APPN component but DLSw is responsible for handing off the frames to TCP, which passes the frames to the IP protocol.

Note: As shown in Figure 5-50 on page 5-369, all CP-CP sessions are routed through the APPN component in the 6611. When APPN calculates a route for an LU-LU session, however, the session flows through the APPN component in the

6611 only if the end nodes in the session do *not* belong to the same connection network or are not part of a connection network. (Refer to the *Introduction and Planning Guide* for a complete discussion of how the 6611 network node routes LU-LU sessions).

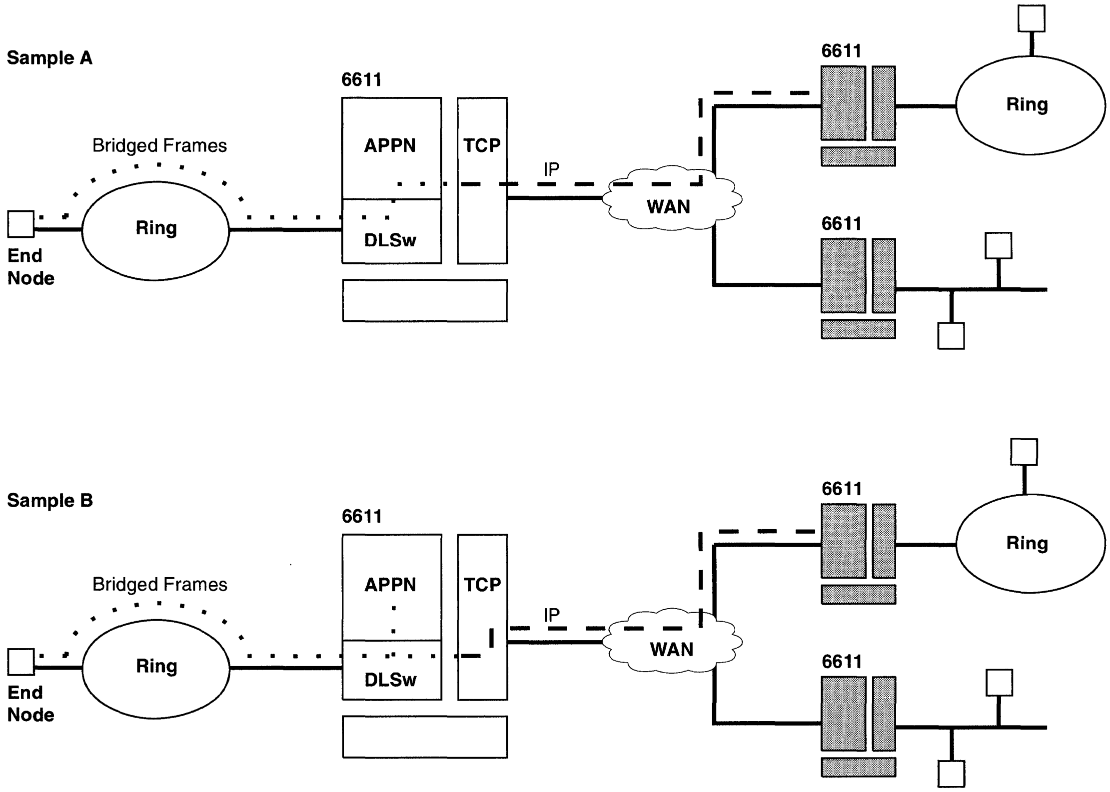


Figure 5-50. Configuration Options for CP-CP Sessions

If the 6611 network node is configured to accept connection requests from any node, then you do not need to define information about other 6611 network nodes on the WAN. You must ensure, however, that adjacent network nodes on the WAN are able to initiate a connection with this node. To allow this network node to initiate a connection with another network node on the WAN, you must define information about the adjacent node when configuring this node. For configuration purposes, adjacent nodes on a WAN are identified by their connection to the 6611 network node: adjacent nodes reached through a remote DLSw connection are referred to as *DLSw adjacent nodes*; adjacent nodes reached through a direct IP connection are referred to as *IP adjacent nodes*.[4]

If you want to control which 6611 network nodes on the WAN can initiate CP-CP sessions with this network node, you can configure this node to accept connection requests from explicitly defined nodes only. When you configure the node in this manner, you must specify information about each adjacent network node that is allowed to communicate with this node.

Table 5-485 on page 5-370 summarizes the connection options available for the 6611 network node and adjacent 6611 nodes on a WAN.

4 This term is used only within the Configuration Program to identify how an adjacent node communicates with the 6611 network node.

Table 5-485 (Page 1 of 2). Connection Options for 6611 Network Node and Adjacent 6611 Nodes on a WAN

WHEN Adjacent Node Type Is...	AND This 6611 Is Configured to Accept Connection Requests...	THEN These Connection Options Are Available...
APPN node (6611)	From any node	**Using IP Only** • Adjacent network node initiates connection with this 6611 network node: – Adjacent node specifies IP address of this 6611 – No adjacent node definition required on this 6611 *or* • This 6611 network node initiates connection with adjacent network node: – 6611 specifies IP address of adjacent node – 6611 activates link to adjacent node automatically (Activate link automatically parameter is enabled) **Using Remote DLSw** • Adjacent network node initiates connection with this 6611 network node: – Adjacent node specifies MAC/SAP address used by this 6611 to communicate with DLSw – No adjacent node definition required on this 6611 *or* • This 6611 network node initiates connection with adjacent network node: – 6611 specifies MAC/SAP address used by adjacent node to communicate with DLSw – 6611 activates link to adjacent node automatically (Activate link automatically parameter is enabled)

Table 5-485 (Page 2 of 2). Connection Options for 6611 Network Node and Adjacent 6611 Nodes on a WAN

WHEN Adjacent Node Type Is...	AND This 6611 Is Configured to Accept Connection Requests...	THEN These Connection Options Are Available...
APPN node (6611)	From explicitly defined nodes only	**Using IP Only** • Adjacent network node initiates connection with this 6611 network node: – Adjacent network node specifies IP address of this 6611 – This 6611 specifies adjacent node's IP address and fully qualified control point name. – This 6611 does not activate link to adjacent node (Activate link automatically parameter is disabled) *or* • This 6611 network node initiates connection with adjacent network node: – 6611 specifies adjacent node's IP address and fully qualified control point name. – 6611 activates link to adjacent node automatically (Activate link automatically parameter is enabled) **Using Remote DLSw** • Adjacent network node initiates connection with this 6611 network node: – Adjacent node specifies MAC/SAP address used by this 6611 to communicate with DLSw – This 6611 specifies adjacent node's fully qualified control point name and MAC/SAP address used by adjacent node to communicate with DLSw. – This 6611 does not activate link to adjacent node (Activate link automatically parameter is disabled) *or* • This 6611 network node initiates connection with adjacent network node: – 6611 specifies adjacent node's fully qualified control point name and MAC/SAP address used by adjacent node to communicate with DLSw. – 6611 activates link to adjacent node automatically (Activate link automatically parameter is enabled)

Note: A single transmission group, or link, can be defined between the 6611 network node and any specific adjacent node. APPN, as implemented on the 6611, does not support parallel connections to the same adjacent node (control point).

Estimating APPN Storage Requirements

Developing an APPN configuration requires careful design and planning for efficient utilization of available system resources. To assist you in planning your configuration and determining your 6611 memory needs, IBM provides a storage estimating tool called the IBM 6611 Storage Estimate EXEC. For information on this tool, contact your IBM marketing representative and ask for the Internetworking Marketing Specialist for your trading area.

Note: The 6611 Storage Estimate EXEC replaces the APPN Planning Worksheet provided in a previous version of this book.

It is recommended that you use the System Manager to monitor paging space usage on the 6611 and APPN shared memory usage.

- To monitor paging space usage:
  1. Log in to the System Manager on the 6611
  2. Press **F3** on the main menu to enter the fast-path command environment
  3. Enter the following command to determine the amount of paging space in use by the 6611:

     system statistics view -paging_space

- To monitor APPN shared memory usage, use SNMP to check the following APPN MIB variables:

  ibmappnMemorySize
  ibmappnMemoryUsed

Tuning the APPN Network Node

You can use the APPN Node Tuning window to tune the performance of the APPN network node. Node performance can be tuned in two ways:

- By manually setting the values of the Maximum shared memory and the Maximum cached directory entries parameters.
- By selecting values for the Maximum shared memory and Maximum cached directory entries parameters from the Node Tuning table.

The Maximum shared memory parameter affects the amount of storage available to the APPN network node for network operations. The Maximum cached directory entries parameter affects the amount of directory information that will be stored or *cached* to reduce the time it takes to locate a resource in the network. To simplify the task of selecting the proper values for these parameters, the Configuration Program generates a table of values for the parameters based on your responses to (or the default values of) the following parameters on the Node Tuning window:

- Max. number of APPN network nodes
- Max. number of serviced end and LEN nodes
- Avg. number of LUs for serviced nodes

Each row of the table contains a different set of values for the Maximum shared memory and Maximum cached directory entries parameters. Each row also corresponds to one of five tuning options that you can select. The first tuning option, **Best performance**, requires the most storage. The last tuning option, **Minimum storage used** uses the least amount of storage. The default tuning option, **Balanced adjustment**, is a balance between best performance and minimum storage usage. The other tuning options represent more gradual steps within the range of options.

The tuning window was designed to enable you to experiment with the different options for tuning the network node. In general, tuning the APPN node involves a trade-off between node performance and storage usage. The better the performance, the more storage required. If you prefer, you can tune the performance of the 6611 network node manually by enabling the Manual tuning parameter on the window and entering your own values for the Maximum shared memory and Maximum cached directory entries parameters.

Tuning Notes:

1. If you define connection networks within your APPN network and you anticipate that most end nodes will initiate LU-LU sessions with other end nodes on the same connection network, you should set the Avg. number of LUs for serviced nodes parameter to the minimum value (1). Using connection networks in this manner reduces the shared memory requirements of the 6611 network node because most LU-LU sessions will not need to flow through the APPN component in the 6611.
2. Because the Maximum shared memory parameter affects storage allocation within the 6611, you should use care when explicitly defining this parameter. Use the values generated by the Configuration program as a guide when increasing or reducing maximum shared memory or select one of the tuning options provided by the Node Tuning window.

APPN Trace Options

The APPN Trace Options window enables you to start one or more APPN traces through the Configuration Program. The traces are activated when the configuration file is applied on the 6611. The traces will continue to be active until they are stopped through the System Manager or until a new configuration that stops the traces is applied on the 6611.

Note: Running traces on the 6611 can affect its performance. Traces should be started only when needed and should be stopped as soon as the required amount of trace information is gathered.

Intermediate Session Accounting

You can use options on the APPN Node Management window to collect information about intermediate sessions. Intermediate sessions are LU-LU sessions that pass through the APPN network node, but whose endpoints (origin and destination) lie outside of the network node.

Information on intermediate sessions is generated by the intermediate session routing (ISR) component in the network node and falls into two categories:

- Intermediate session names and counters
- Route Selection control vector (RSCV) data for intermediate sessions

Enabling the Collect intermediate session information parameter instructs the 6611 to collect session names and counters for active intermediate sessions. Enabling the Save RSCV information for intermediate sessions parameter instructs the 6611 to collect RSCV data for active intermediate sessions. The RSCV data is useful for monitoring session routes. In both cases, you can retrieve data on active sessions by issuing SNMP **get** and **get-next** commands for variables in the APPN

Management Information Base (MIB). Refer to the *Network Management Reference* for information on using SNMP.

For accounting purposes, you also can maintain records of intermediate sessions passing through the network node. The data records can be created and stored on the 6611's hard disk (DASD) or in router memory. To capture this information on the 6611, select the **Intermediate Session Records** push button on the APPN Node Management window, enable the creation of records, and define how the records should be collected and stored. Each record provides a snapshot of intermediate session activity on the node during a specific period of time. In addition, when the Save RSCV information for intermediate sessions parameter is enabled, RSCV data also is recorded in each data record.

The Record creation threshold parameter specifies how often intermediate session records are generated. Each time the total number of bytes recorded by the session counters exceeds the value of this parameter (by an even multiple), a new record is created. For example, when the Record creation threshold (which is defined in 1000-byte increments) is set to 500, a new record is created each time the total number of bytes recorded by the session counters exceeds 500 000.

Intermediate session records stored in the memory buffer can be accessed only through SNMP. You must issue SNMP **get** or **get-next** commands to retrieve the APPN MIB variables that correspond to fields in the records. Records stored on the 6611's hard disk can be retrieved through SNMP or by using the File Transfer Protocol (FTP) to retrieve the contents of an entire buffer. "Retrieving Data Records from a DASD Buffer" on page 5-383 describes the procedure for retrieving intermediate session records from a DASD buffer.

Notes:

1. When you enable the creation of intermediate session records on the 6611, data on active intermediate sessions also is collected, by default. The data is collected whether or not the Collect intermediate session information parameter has been enabled or disabled for this configuration.
2. Configuration changes to the APPN accounting parameters will not take effect until the 6611 or the APPN function on the 6611 is restarted. You can make changes interactively, however, by issuing SNMP **set** commands to modify the APPN MIB variables associated with the configuration parameters. (See "MIB Variables for APPN Accounting Parameters" on page 5-382.)
3. Data on intermediate sessions and RSCVs is obtained by examining the BIND request used to activate a session between two LUs. Consequently, when the data collection options on this window are activated on the 6611, no data is collected for sessions that have already been established because the BIND information for those sessions is not available.
4. Unless disk space is limited, it is recommended that intermediate session records be stored on the 6611's hard disk so that you can retrieve the records more easily using FTP.

The following sections provide additional information on intermediate session accounting.

Session Names and Counters: When you enable the Collect intermediate session information parameter or enable the creation of intermediate session records, the session names and counters described in this section are collected for active intermediate sessions. The SNMP variables that correspond to these session names and counters are located in the "Intermediate Session Information Table" in the APPN MIB. All MIB variables in the "Intermediate Session Information Table" begin with the prefix *ibmappnIsIn*.

When you enable the creation of intermediate session records, the 6611 also stores the session names and counters in accounting records. The SNMP variables that correspond to the accounting records are located in the "Intermediate Session Accounting Data Table" in the APPN MIB. All MIB variables in this table begin with the prefix *ibmappnIsAc*.

Notes:

1. Session names and counters in the "Intermediate Session Information Table" are indexed by the following MIB variables:
   - ibmappnIsInFqLuName (the fully-qualified LU name of a session partner)
   - ibmappnIsPcid (the path control identifier that identifies an intermediate session)

   When specific data for these variables is used as a suffix on an SNMP **get** or **get-next** command for a session name or counter variable, the suffix serves as a pointer or *index* to the names or counter data for a specific active session. A **get** command, for example, takes the form:

   get *mib_variable.FQLUname_length.FQLUname.path_control_ID*

2. Session names and counters in the "Intermediate Session Accounting Table" are indexed by the accounting record number. Record numbers are identified by the MIB variable ibmappnIsAcIndex.

Table 5-486. APPN Intermediate Session Names

Session Name	Associated MIB Variable	Description
Primary LU name	ibmappnIsInPriLUName ibmappnIsAcPriLUName	The name of the LU that sent the BIND request to activate the LU-LU session.
Secondary LU name	ibmappnIsInSecLUName ibmappnIsAcSecLUName	The name of the primary LU's session partner.
Mode name	ibmappnIsIsModeName ibmappnIsAcModeName	The mode name for the session.
COS name	ibmappnIsInCosName ibmappnIsAcCosName	The class of service (COS) name for the session.

Table 5-487 (Page 1 of 2). APPN Intermediate Session Counters

Session Counter	Associated MIB Variable	Description
Primary to secondary FMD PIUs	ibmappnIsInP2SFmdPius ibmappnIsAcP2SFmdPius	The number of FMD PIUs (packets of user data) transmitted from the primary LU during the session.
Secondary to primary FMD PIUs	ibmappnIsInS2PFmdPius ibmappnIsAcS2PFmdPius	The number of FMD PIUs transmitted by the secondary LU during the session.

Table 5-487 (Page 2 of 2). APPN Intermediate Session Counters

Session Counter	Associated MIB Variable	Description
Primary to secondary non-FMD PIUs	ibmappnIsInP2SNonFmdPius ibmappnIsAcP2SNonFmdPius	The number of non-FMD PIUs (packets of system data) transmitted from the primary LU during the session.
Secondary to primary non-FMD PIUs	ibmappnIsInS2PNonFmdPius ibmappnIsAcS2PNonFmdPius	The number of non-FMD PIUs transmitted from the secondary LU during the session.
Primary to secondary FMD bytes	ibmappnIsInP2SFmdBytes ibmappnIsAcP2SFmdBytes	The number of bytes of FMD (user) data transmitted from the primary LU during the session.
Secondary to primary FMD bytes	ibmappnIsInS2PFmdBytes ibmappnIsAcS2PFmdBytes	The number of bytes of FMD data transmitted from the secondary LU during the session.
Primary to secondary non-FMD bytes	ibmappnIsInP2SNonFmdBytes ibmappnIsAcP2SNonFmdBytes	The number of bytes of non-FMD (system) data transmitted from the primary LU during the session.
Secondary to primary non-FMD bytes	ibmappnIsInS2PNonFmdBytes ibmappnIsAcS2PNonFmdBytes	The number of bytes of non-FMD data transmitted from the secondary LU during the session.

RSCV Information: When you enable the Save RSCV information for intermediate sessions parameter, RSCV information is collected for each active intermediate session. The RSCV data for an active session can be retrieved by accessing the APPN MIB variable ibmappnIsInRouteInfo. This variable is located in the "Intermediate Session Information Table" in the MIB.

When you enable the creation of intermediate session records, the 6611 also stores the RSCV data in accounting records. The RSCV data in an accounting record can be retrieved by accessing the APPN MIB variable ibmappnIsAcRouteInfo. This variable is located in the "Intermediate Session Accounting Data Table" in the MIB.

Notes:

1. The ibmappnIsInRouteInfo variable in the "Intermediate Session Information Table" is indexed by the following MIB variables:

   - ibmappnIsInFqLuName (the fully-qualified LU name of a session partner)
   - ibmappnIsPcid (the path control identifier that identifies the intermediate session)

   When specific data for these variables is used as a suffix on an SNMP **get** or **get-next** command for ibmappnIsInRouteInfo, the suffix serves as a pointer or *index* to the RSCV for a specific active session. A **get** command, for example, takes the form:

   get ibmappnIsInRouteInfo.*FQLUname_length.FQLUname.path_control_ID*

2. The ibmappnIsAcRouteInfo variable in the "Intermediate Session Accounting Table" is indexed by the accounting record number. Record numbers are identified by the MIB variable ibmappnIsAcIndex.

The session RSCV is carried in the BIND request used to activate a session between two LUs. It describes the optimum route through an APPN network for a particular LU-LU session. The session RSCV contains the CP names and TG associated with each pair of adjacent nodes along the route from a source node to a destination node. Table 5-488 on page 5-377 shows the format of the RSCV.

Table 5-488. RSCV Format

Octet	Description
Octet 0 to 1	Vector header (X'2B')
Octet 2	Maximum hop count. The number (in binary) of TG descriptor control vectors in the RSCV.
Octet 3	Current hop count. The index (in binary) of the last TG descriptor control vector processed.
Octets 4 to n	Control vectors that include TG descriptors. TG descriptors are identified by a vector header of X'46'. Each descriptor contains data that identifies a TG in the route.

Accounting Records Buffer: Accounting records generated by the 6611 can be stored in a single buffer in router memory or in a set of buffers on the 6611's hard disk. This section describes the APPN MIB variables associated with an accounting records buffer on the 6611.

The APPN MIB contains two buffer tables for accounting records:

- The "Intermediate Session Accounting Buffer Type Table" contains MIB variables that report status for each *type* of 6611 accounting buffer. Specific variables in the table are indexed by media type (memory or DASD). A **get** command, for example, takes the form:

  get *ibmappnIsAcBtypexxx*.**1** (for the memory buffer)
  get *ibmappnIsAcBtypexxx*.**2** (for the DASD buffers)

  where *ibmappnISAcBtypexxx* is a MIB variable in the buffer type table.

  Table 5-492 on page 5-382 describes the MIB variables in this buffer table that correspond to the configuration parameters for intermediate session accounting.

- The "Intermediate Session Accounting Buffer Table" contains MIB variables that point to specific accounting buffers. Specific variables in the table are indexed by media type and buffer number. A **get** command, for example, takes the form:

  get *ibmappnIsAcBufxxx*.**1**.*n* (for the memory buffer)
  get *ibmappnIsAcBufxxx*.**2**.*n* (for a DASD buffer)

  where *ibmappnIsAcBufxxx* is a MIB variable in the buffer table and *n* is the number of the buffer.

  Table 5-489 on page 5-378 shows the contents of the "Intermediate Session Accounting Buffer Table."

Table 5-489. Accounting Buffer Table (APPN MIB Variables)

Description	APPN MIB Variable	SNMP Set?	Notes
Recording media	ibmappnIsAcBufMedia	No	An index for MIB variables in the buffer table, which associates a variable with the memory buffer or one of the DASD buffers. MIB value: 1 - Memory 2 - DASD
Buffer number	ibmappnIsAcBufNumber	No	An index for MIB variables in the buffer table, which associates a variable with a specific buffer number.
Buffer state	ibmappnIsAcBufState	Yes	MIB value: 1 - Complete 2 - Active 3 - Delete buffer (DASD only)
Record format	ibmappnIsAcBtypeRecFormat	Yes	MIB value: 1 - ASCII 2 - Binary
Maximum records per buffer	ibmappnIsAcBufMaxRecords	Yes	The maximum number of records that can be stored in a buffer.
First (oldest) buffer record	ibmappnIsAcBufOldestIndex	Yes	When you set this pointer to a newer record in the buffer, all records logged prior to that record are deleted. This is the method by which sequential records in memory can be deleted.
Last (newest) buffer record	ibmappnIsAcBufNewestIndex	No	The last buffer record created.
Buffer name	ibmappnIsAcBufName	Yes	The file name of a DASD buffer. You can use FTP to retrieve records from this file. See "Retrieving Data Records from a DASD Buffer" on page 5-383 for more information.

The 6611 logs two types of accounting records in the accounting records buffer.

- *Time records*, which identify specific events that occurred while the intermediate session records were being collected
- *Data records*, which contain the actual data collected for intermediate sessions

Time records are created and logged for the following events:

- The collection of accounting records is started or stopped
- A new recording medium is created (memory buffer or DASD buffers)
- Buffer data is overwritten (wrapped)
- The time is changed on the 6611, through the System Manager or SNMP
- The format of the buffer records is changed (to ASCII or binary)

A buffer always contains at least one time record. If one of the previous events has not occurred, the 6611 creates a time record and stores it in the buffer as a time reference. Table 5-490 on page 5-379 shows the format of a binary time record.

Table 5-490 (Page 1 of 2). Intermediate Source Routing (ISR) Time Record - Binary Format

Bytes	Type	Contents	APPN MIB Variable
1	Character	Record format ASCII *B* - binary format	NA
1	Character	Record level 1 - 6611 Release 3	NA
4	Signed integer	Record type 1 - Intermediate session record	NA
4	Signed integer	Record sub-type 1 - Time record	NA
2	Signed integer	Record length	NA
4	Signed integer	Record number	ibmappnIsAcTimeIndex (table index)
4	Signed integer	Type of time record • 1 - Start collection • 2 - End collection • 3 - Media created • 4 - Media wrapped • 5 - Time change • 6 - Manager set time • 7 - Record format changed • 8 - Time reference	ibmappnIsAcTimeEntryType
4	Signed integer	Type of media event • 1 - Memory medium • 2 - DASD medium • 99 - All media	ibmappnIsAcTimeForMedia
4	Unsigned integer	Record time (in hundredths of seconds since APPN started)	ibmappnIsAcTimeRecTime
4	Unsigned integer	Agent seconds (0-59)	ibmappnIsAcAgtUtcSecs
4	Unsigned integer	Agent minutes (0-59)	ibmappnIsAcAgtUtcMins
4	Unsigned integer	Agent hours (0-23)	ibmappnIsAcAgtUtcHours
4	Unsigned integer	Agent month days (1-31)	ibmappnIsAcAgtUtcMdays
4	Unsigned integer	Agent months (0-11)	ibmappnIsAcAgtUtcMonths
4	Unsigned integer	Agent years	ibmappnIsAcAgtUtcYears
4	Unsigned integer	Agent week days (0-6)	ibmappnIsAcAgtUtcWdays
4	Unsigned integer	Agent year days (0-365)	ibmappnIsAcAgtUtcYdays
4	Unsigned integer	Agent Isdst (positive if daylight savings time is in effect)	ibmappnIsAcAgtUtcIsdst
18	Unsigned integer	Agent name (null terminated)	ibmappnIsAcAgtName
4	Unsigned integer	Manager seconds (0-59)	ibmappnIsAcMgrUtcSecs
4	Unsigned integer	Manager minutes (0-59)	ibmappnIsAcMgrUtcMins
4	Unsigned integer	Manager hours (0-23)	ibmappnIsAcMgrUtcHours
4	Unsigned integer	Manager month days (0-31)	ibmappnIsAcMgrUtcMdays
4	Unsigned integer	Manager months (0-11)	ibmappnIsAcMgrUtcMonths
4	Unsigned integer	Manager years	ibmappnIsAcMgrUtcYears
4	Unsigned integer	Manager week days (0-6)	ibmappnIsAcMgrUtcWdays

Table 5-490 (Page 2 of 2). Intermediate Source Routing (ISR) Time Record - Binary Format

Bytes	Type	Contents	APPN MIB Variable
4	Unsigned integer	Manager year days	ibmappnIsAcMgrUtcYdays
4	Unsigned integer	Manager Isdst (positive if daylight savings time is in effect)	ibmappnIsAcMgrUtcIsdst
18	Unsigned integer	Manager name (null terminated)	ibmappnIsAcMgrName
4	Signed integer	Manager times/name valid • 1 - Not valid • 2 - Valid	ibmappnIsAcMgrTimeValid
4	Unsigned integer	Reserved	NA

Note: The MIB variables shown in this table are located in the "Intermediate Session Accounting Time Table" in the APPN MIB.

When saved in ASCII format, the time record appears as a text string. The following example shows a portion of the record:

```
A1=1,1,n,4,1,2...(and so on)
││ │ │ │ │ │
││ │ │ │ │ └──────── Type of media event (DASD)
││ │ │ │ └────────── Type of time record (start collection)
││ │ │ └──────────── Record number
││ │ └────────────── Record length (n bytes)
││ └──────────────── Record sub-type (time record)
│└────────────────── Record type (intermediate session record)
└─────────────────── Record level (6611 Release 3)
──────────────────── Record format (ASCII)
```

Note: The contents of the ASCII version of the time record appear in the same order as the contents of the binary version of the record shown in Table 5-490.

Data records are created and logged after the following events:

- The collection of accounting records is started or stopped
- The total number of bytes recorded by the intermediate session counters exceeds (by an even multiple) the value set by the Record creation threshold parameter or the MIB variable ibmappnIsAcGlobeByteThresh.
- You set the ibmappnIsAcGlobeCheckpt MIB variable. When you set this variable, the 6611 generates data records for all currently active sessions.

Data records contain the following information:

- The reason the record was created
- Session names and counters
- RSCV information (if requested)

Table 5-491 shows the format of a binary data record.

Table 5-491 (Page 1 of 3). Intermediate Source Routing (ISR) Data Record - Binary Format

Bytes	Type	Contents	APPN MIB Variable
1	Character	Record format ASCII *B* - binary format	NA

Table 5-491 (Page 2 of 3). Intermediate Source Routing (ISR) Data Record - Binary Format

Bytes	Type	Contents	APPN MIB Variable
1	Character	Record level 1 - 6611 Release 3	NA
4	Signed integer	Record type 1 - Intermediate session record	NA
4	Signed integer	Record sub-type 2 - Data record	NA
2	Signed integer	Record length	NA
4	Signed integer	Record number	ibmappnIsAcIndex (table index)
4	Unsigned integer	Entry type • 1 - Session started • 2 - Session ended • 3 - Session threshold reached • 4 - Session checkpoint record	ibmappnIsAcEntryType
4	Unsigned integer	Record time	ibmappnIsAcRecTime
18	Character string	Network qualified CP name (null terminated)	ibmappnIsAcFqLuName
8	Unsigned character	PCID	ibmappnIsAcPcid
18	Character string	Primary LU name (null terminated)	ibmappnIsAcPriLuName
18	Character string	Secondary LU name (null terminated)	ibmappnIsAcSecLuName
9	Character string	Class of service name (null terminated)	ibmappnIsAcCosName
9	Character string	Mode name (null terminated)	ibmappnIsAcModeName
4	Unsigned integer	Transmission priority	ibmappnIsAcTransPriority
4	Unsigned integer	Session type	ibmappnIsAcSessType
4	Unsigned integer	Session state	ibmappnIsAcSessState
4	Unsigned integer	Session start time (in hundredths of seconds since APPN started)	ibmappnIsAcSessStartTime
4	Unsigned integer	Session up time (in hundredths of seconds since APPN started)	ibmappnIsAcSessUpTime
4	Unsigned integer	Counter up time (in hundredths of seconds since APPN started)	ibmappnIsAcCtrUpTime
4	Unsigned integer	Session end reason	ibmappnIsAcEndReason
4	Unsigned integer	Primary to secondary FMD PIUs	ibmappnIsAcP2SFmdPius
4	Unsigned integer	Secondary to primary FMD PIUs	ibmappnIsAcS2PFmdPius
4	Unsigned integer	Primary to secondary non-FMD PIUs	ibmappnIsAcP2SNonFmdPius
4	Unsigned integer	Secondary to primary non-FMD PIUs	ibmappnIsAcS2PNonFmdPius
4	Unsigned integer	Primary to secondary FMD bytes	ibmappnIsAcP2SFmdBytes
4	Unsigned integer	Secondary to primary FMD bytes	ibmappnIsAcS2PFmdBytes
4	Unsigned integer	Primary to secondary non-FMD bytes	ibmappnIsAcP2SNonFmdBytes

Table 5-491 (Page 3 of 3). Intermediate Source Routing (ISR) Data Record - Binary Format

Bytes	Type	Contents	APPN MIB Variable
4	Unsigned integer	Secondary to primary non-FMD bytes	ibmappnIsAcS2PNonFmdBytes
4	Signed integer	RSCV length	NA
0-255	Unsigned character	RSCV	ibmappnIsAcRouteInfo

Note: The MIB variables shown in this table are located in the "Intermediate Session Accounting Data Table" in the APPN MIB.

When saved in ASCII format, the data record appears as a text string. The following example shows a portion of the record:

```
A1=1,2,n,5,1,...(and so on)
|||  | | | |
|||  | | | └────────── Entry type (session started)
|||  | | └──────────── Record number
|||  | └────────────── Record length (n bytes)
|||  └──────────────── Record sub-type (data record)
||└─────────────────── Record type (intermediate session record)
|└──────────────────── Record level (6611 Release 3)
└───────────────────── Record format (ASCII)
```

Note: The contents of the ASCII version of the data record appear in the same order as the contents of the binary version of the record shown in Table 5-491.

MIB Variables for APPN Accounting Parameters: The configuration parameters that you can specify for intermediate session accounting correspond to the APPN MIB variables shown in Table 5-492.

Table 5-492 (Page 1 of 2). Accounting Parameters (Associated MIB Variables)

Accounting Parameter	Associated MIB Variable	SNMP Set?
Collect intermediate session information	ibmappnIsInGlobeStatus (1 - Disable; 2 - Enabled)	Yes
Save RSCV information for intermediate sessions	ibmappnIsInGlobeRscv (1 - Disable; 2 - Enabled)	Yes
Create intermediate session records	None	NA
Record creation threshold	ibmappnIsAcGlobeByteThresh	Yes
Recording media (see table note)	ibmappnIsAcBtypeMedia (1 - Memory; 2 - DASD)	No
Memory	ibmappnIsAcBtypeActive (1 - Disable; 2 - Enabled)	Yes
Maximum buffers	ibmappnIsAcBtypeMaxBufs	
Maximum records per buffer	ibmappnIsAcBtypeRecPerBuf	
Buffers full	ibmappnIsAcBtypeFullAction	
Record format	ibmappnIsAcBtypeRecFormat	

Table 5-492 (Page 2 of 2). Accounting Parameters (Associated MIB Variables)

Accounting Parameter	Associated MIB Variable	SNMP Set?
DASD	ibmappnIsAcBtypeActive (1 - Disable; 2 - Enabled)	Yes
Maximum buffers	ibmappnIsAcBtypeMaxBufs	
Maximum records per buffer	ibmappnIsAcBtypeRecPerBuf	
Buffers full	ibmappnIsAcBtypeFullAction	
Record format	ibmappnIsAcBtypeRecFormat	

Note: The MIB variable ibmappnIsAcBtypeMedia (recording media) is an index for other variables in the "Intermediate Session Accounting Buffer Type Table" (prefix *ibmappnIsAcBtype*). The index associates other variables in the table with the memory buffer or DASD buffers on the 6611.

Retrieving Data Records from a DASD Buffer: To retrieve intermediate session records from a DASD buffer on the 6611, perform the following steps.

1. From an SNMP workstation, issue the SNMP command:

   get-next ibmappnIsAcBufState.2

   where *2* specifies a media type of DASD. Because a buffer number has not been specified as an index on the command, this command returns the state of the first DASD buffer. If a value of 1 is returned, the buffer is full (complete). When the buffer is still active, a value of 2 is returned.

2. To retrieve the file name of a complete buffer, issue the SNMP command:

   get ibmappnIsAcBufName.2.n

   where *2* specifies a media type of DASD and *n* is the number of the buffer (determined in step 1). This command returns the name of the file on the 6611 hard disk that contains the contents of the buffer. The file is located in the transfer directory on the 6611.

3. Use the File Transfer Protocol (FTP) to retrieve the file:

   ftp *router_ip_address*

   Enter a user ID and password and issue the following command:

   get *file_name*

   The file is placed in the home directory of the user ID that initiated the FTP commands.

4. To delete the contents of a complete DASD buffer on the 6611, issue an SNMP **set** command to set the ibmappnIsAcBufState variable to purge (3). The format of the command is:

   ibmappnIsAcBufState.2.n=3

   where *2* specifies a media type of DASD and *n* is the number of the buffer (determined in step 1).

Defining Transmission Group Characteristics

When configuring APPN on a 6611, you have the option of modifying the TG characteristics that define a connection between the 6611 and an adjacent node. These characteristics, such as the security of a link or its effective capacity, are used by APPN when calculating an optimum or "least-weight" route between nodes in the APPN network.

Note: The TG characteristics you define affect only the selection of routes between APPN nodes. These characteristics have no direct affect on any intermediate routing performed by DLSw or IP on APPN's behalf.

The APPN function on the 6611 provides two sets of default TG characteristics. One set applies to all DLSw connections to adjacent nodes; the other set applies to all IP connections to adjacent nodes. The Configuration Program enables you to:

- Modify the default TG characteristics for all DLSw connections
- Modify the default TG characteristics for all IP connections
- Override the default TG characteristics when defining a specific connection between the 6611 network node and an adjacent node (link station definition)

The default TG characteristics used for the configuration also apply to adjacent nodes that are not defined to the 6611 network node but that request service.

As an example of how TG characteristics could be used to influence the selection of a route through an APPN network node, suppose that a route from network node 6611 A to network node 6611 D can pass through either network node 6611 B or 6611 C. In this example, 6611 A defines an IP connection to both 6611 B and 6611 C. However, the connection from 6611 A to 6611 B is a high-speed link, while the connection from 6611 A to 6611 C is a slower-speed link.

To ensure that the high-speed connection from 6611 A to 6611 B is viewed as the more desirable path for routing APPN interactive traffic, you could modify the effective capacity TG characteristic for the link station associated with this path. In this case, the default value for effective capacity is X'38', which represents a link speed of approximately 20 Kbps. Higher effective capacities represent higher-speed links. By changing the effective capacity value for the path to X'69', the path is assigned a lower weight in the COS file for interactive traffic (#INTER). Consequently, the connection from 6611 A to 6611 B is represented as more desirable (lower weight) than the connection from 6611 A to 6611 C.

COS Options: The 6611 also enables you to modify the architected COS files provided for APPN routing. Each COS file contains a range of acceptable TG characteristics that APPN compares against actual TG and node characteristics to determine the best route for the session. Using System Manager fast-path commands, you can:

- View an entire COS file or a specific TG row in the file.
- Set the minimum and maximum ranges for the user-defined TG characteristics within a COS file.
- Add a mode name to a COS file. The mode name is used by the LU initiating a session to specify the characteristics desired for the session, including the class of service.

In addition, you can retrieve an APPN COS file from the 6611 and use a standard text editor to modify it. Refer to *Operations and Problem Management* for a description of how to retrieve the file, and for information on the System Manager fast-path commands for APPN.

Configuration Options

Table 5-493 summarizes the options you have when configuring the 6611 as an APPN network node. To access the APPN configuration parameters, select the **Node Configuration** push button on the main menu of the Configuration Program. APPN is one of the Node Configuration options.

Table 5-493 (Page 1 of 2). APPN Configuration Options

IF you want...	THEN...
Minimum Configuration: • Allow this network node to accept any request it receives from another node to establish a connection. • Restrict this network node from initiating connections with other nodes. **Note:** If you choose the minimum configuration, adjacent nodes must define connections to this 6611 network node to ensure connectivity.	• Enable the APPN protocol. • Configure the following parameters for this node: – Network ID – Control point name – Locally administered MAC address (for DLSw) • Accept all other defaults.
To Initiate Connections: • Allow this network node to accept any request it receives from another node to establish a connection. • Enable this network node to initiate connections with other nodes that you specify, including LEN end nodes.	• Enable the APPN protocol. • Configure the following parameters for this node: – Network ID – Control point name – Locally administered MAC address (for DLSw) • Specify the LAN-attached adjacent nodes with which this network node may initiate a connection by defining those nodes under the DLSw Adjacent Nodes push button. • Specify the 6611 network nodes on a WAN with which this network node may initiate a connection by defining those nodes under the DLSw Adjacent Nodes or IP Adjacent Nodes push buttons. • Additionally, you can: – Tune this network node – Activate APPN traces on this 6611 – Collect accounting and node statistics for this network node (Node Management)

Table 5-493 (Page 2 of 2). APPN Configuration Options

IF you want...	THEN...
To Completely Control Connections: • Allow this network node to accept connection requests *only* from nodes that you specify. • Enable this network node to initiate connections with the nodes that you specify, including LEN end nodes. **Note:** This option provides a higher level of security because you explicitly define the APPN nodes that may communicate with this 6611 network node. A connection request from an adjacent node will be accepted only if the node's MAC/SAP address or IP address has been configured on this network node. In addition, you can ensure that you have a secure link with each adjacent node by configuring the session level security feature for each link.	• Enable the APPN protocol. • Configure the following parameters for this node: – Network ID – Control point name – Locally administered MAC address (for DLSw) • Disable the parameter: Accept connection requests from any node. • Select the DLSw Adjacent Nodes push button and define those LAN-attached adjacent nodes that may communicate with this network node. • Specify the 6611 network nodes on a WAN that may communicate with this network node by defining those nodes under the DLSw Adjacent Nodes or IP Adjacent Nodes push buttons. • Additionally, you can: – Tune this network node – Activate APPN traces on this 6611 – Collect accounting and node statistics for this network node (Node Management)

Configuration Verification Checklist

Use the following checklist to help you verify that two or more 6611s are correctly configured to perform APPN routing. The first column lists rules to which the configurations must adhere; the second column lists the affected configuration parameter in the Configuration Program.

Table 5-494 (Page 1 of 2). APPN Configuration Verification Checklist

APPN Rule	Configuration Parameter	√
Node-Level Parameters:		
The Enable APPN parameter must be enabled on all 6611s that communicate using APPN.	Enable APPN	
For 6611s in the same APPN network, the following values must be the same: • Network ID • Key	Network ID	
	Key	
For 6611s in the same APPN network, the following values must must be different: • Control point name • XID ID	Control point name	
	XID ID	
Every 6611 must have unique values for: • MAC address of this node • MAC address of this node-SAP address of this node pair	MAC address of this node	
	SAP address of this node	

Table 5-494 (Page 2 of 2). APPN Configuration Verification Checklist

APPN Rule	Configuration Parameter	√
Every 6611 must have unique values for these adjacent node parameters: • MAC address • MAC address-SAP address pair	MAC address	
	SAP address	
If the 6611s are on adjacent nodes, the Activate link automatically parameter must be enabled on at least one 6611.	Activate link automatically	
If 6611 B is an IP adjacent node of 6611 A, and if 6611 A's configuration includes 6611 B's fully-qualified control point name, then that fully-qualified control point name must match the string equal to 6611 B's network ID.control point name.	Fully-qualified control point name	
	Network ID	
	Control point name	

Sample Network Graphic

Figure 5-51 on page 5-388 shows a sample APPN network containing two 6611s configured as adjacent network nodes. The sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP over PPP
  - A token-ring port configured to data link switch SNA frames and to run IP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP over PPP
  - A token-ring port configured to data link switch SNA frames and to run IP
  - An Ethernet port configured to data link switch SNA frames and to run IP

Slot and port numbers in Figure 5-51 on page 5-388 are abbreviated S*x* P*y*

Note: The IP protocol has been configured on the token-ring and Ethernet LANs to enable you to test your connectivity using the IP ping protocol. IP is not required on the LANs for APPN routing.

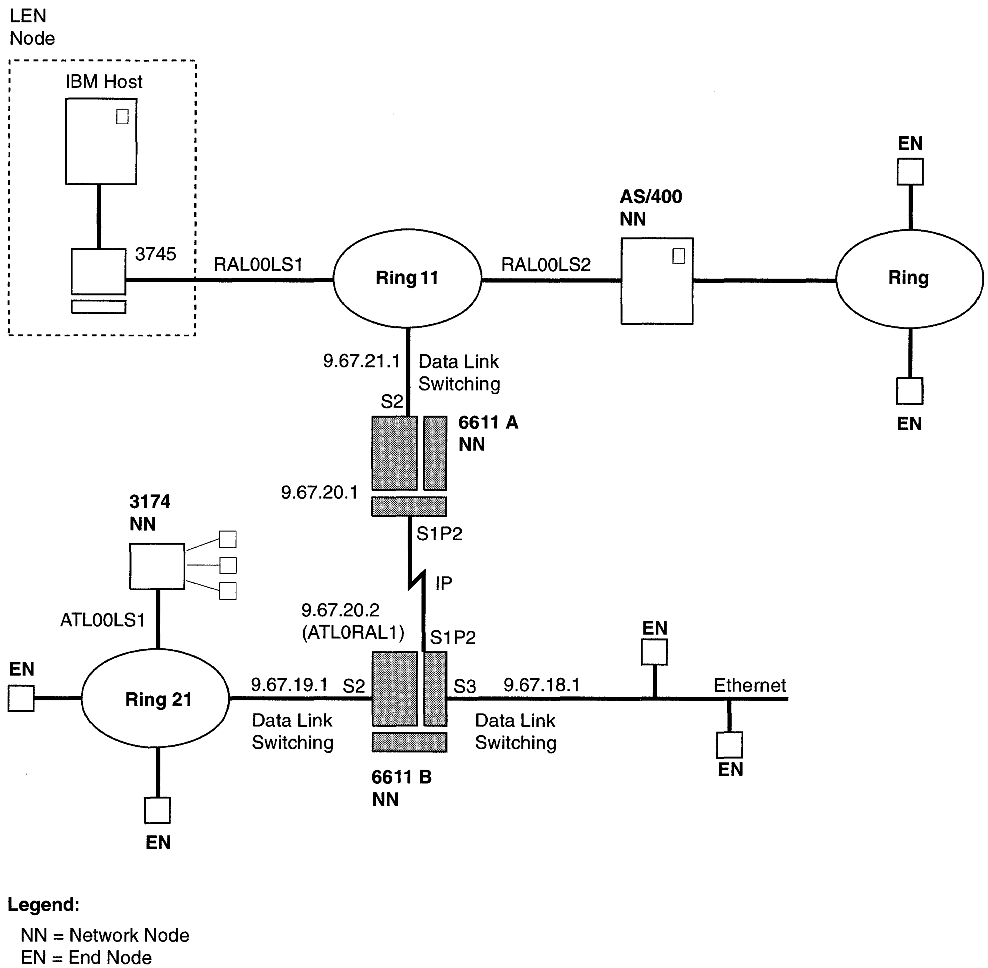


Figure 5-51. Sample APPN Network

Network nodes 6611 A and 6611 B are part of the **EASTERN** APPN network, and are configured to accept connection requests from any node. In addition, 6611 A has been configured so that it can initiate data link switched connections with two adjacent nodes through link stations RAL00LS1 and RAL00LS2. 6611 A also can initiate a connection with 6611 B (link station ATL0RAL1) using IP only. 6611 B has been configured so that it can initiate a data link switched connection with an adjacent node through link station ATL00LS1.

Notes:

1. DLSw is *not* being used in this sample network to establish a CP-CP session across the serial link. The APPN component in 6611 A and 6611 B can establish a direct CP-CP session through IP.
2. In Figure 5-51, 6611 B is attached to an Ethernet LAN. The remote DLSw function will handle frame conversion for frames sent between the Ethernet LAN and Token Ring 11 across the serial link. DLSw does not provide frame conversion between locally attached LANs, such as the Ethernet LAN and Token Ring 21. This function could be provided, however, by configuring 6611 B as a translational bridge.

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure 5-51 on page 5-388. The following tables list the configuration parameters for the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Port and Protocols Running on It

Table 5-495. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Data link protocol	PPP	PPP

Table 5-496. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	56 000	56 000
Data encoding	NRZI	NRZI
Locally administered MAC address	None	None
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table 5-497. Serial Port - PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable
Maximum receive unit size (octets)	1500	1500
Use magic-number for loopback detection	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table 5-498. Serial Port - IP over PPP Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.20.1	9.67.20.2
Subnet mask	255.255.255.255	255.255.255.255
Destination IP address	9.67.20.2	9.67.20.1
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Enable transmission group for IP on this port	NA	NA
Inbound Port Filters	Disable	Disable
IP Priority	Disable	Disable
UDP Broadcasts	Disable	Disable

Token-Ring Ports and Protocols Running on Them

Table 5-499. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table 5-500. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable Source Route Bridging on this port	Enable	Enable
Spanning tree mode	Automatic	Automatic
Path cost	0	0
Port priority for Translational Bridging	80	80
Port state	NA	NA
Ring number	011	021
Max. transmission unit (octets)	2052	2052

Table 5-501. Token-Ring Port - SNA Parameters Configured (for DLSw)

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable SNA frame forwarding on this port	Enable	Enable
SAP value	00, 04	00, 04

Table 5-502. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	9.67.21.1	9.67.19.1
Subnet mask	None	None
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Ethernet Port and Protocols Running on It

Table 5-503. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 3 Value
Enable physical interface on this port	Enable
MAC address	Universally administered address
Locally administered address	NA
Enable additional multicast addresses	Disable
Multicast MAC address	NA

Table 5-504. Ethernet Port - Transparent Bridging Parameters Configured

Parameter	6611 B Slot 3 Value
Enable Transparent Bridging on this port	Enable
Maximum transmission unit size	1500
Spanning tree mode	Automatic
Port priority	80
Path cost	0
Port state	NA
Emulated ring number (for translational bridging only)	None

Table 5-505. Ethernet Port - SNA Parameters Configured (for DLSw)

Parameter	6611 B Slot 3 Value
Enable SNA frame forwarding on this port	Enable
SAP value	Default values

Table 5-506. Ethernet Port - IP Parameters Configured

Parameter	6611 B Slot 3 Value
Enable IP routing on this port	Enable
IP address	9.67.18.1
Subnet mask	None
Max. transmission unit (octets)	1500
Ethernet framing for IP	Ethernet V2.0
Enable ICMP address mask requests	Enable
Inbound Port Filters	Disable
UDP Broadcasts	Disable

Node-Level Parameters - APPN

Table 5-507. Node Level - APPN Routing Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable APPN	Enable	Enable
Network ID	EASTERN	EASTERN
Control point name	RALNN001	ATLNN002
XID ID number for subarea connection	00000	00000
Locally administered MAC address (for DLSw)	4103000FFFFF	5F02002FFFFF
SAP address (for DLSw)	04	04
Accept connection requests from any node	Enable	Enable

Table 5-508. Node Level - APPN DLSw Adjacent Node Parameters Configured

Parameter	6611 A Value	6611 A Value	6611 B Value
Link station name	RAL00LS1	RAL00LS2	ATL00LS1
MAC address	4103000A5231	4103000A5202	5F020024F301
SAP address	04	04	04
Activate link automatically	Enable	Enable	Enable
Enable session level security	Disable	Disable	Disable
Key	NA	NA	NA
Adjacent node type	LEN node	APPN node	APPN node
Fully qualified control point name	EASTERN.RALLEN01	NA	NA
XID block number	000	NA	NA
XID ID number	00000	NA	NA

Table 5-509. Node Level - LEN Node LU Names Parameter Configured

Parameter	6611 A Value (RAL00LS1)	6611 A Value (RAL00LS2)	6611 B Values (ATL00LS1)
Fully qualified LU name	EASTERN.RALLU*	NA	NA

Table 5-510. Node Level - APPN IP Adjacent Node Parameters Configured

Parameter	6611 A Value
Link station name	ATL0RAL1
IP address	9.67.20.2
Activate link automatically	Enable
Enable session level security	Disable
Key	NA
Fully qualified control point name	None

Table 5-511. Node Level - APPN Node Tuning Parameters Configured

Parameter	6611 A Value	6611 B Value
Max. number of APPN network nodes	10	10
Max. number of serviced end and LEN nodes	3	50
Avg. number of LUs for serviced nodes	90	1
Maximum shared memory (using Balanced adjustment tuning option)	6	4
Maximum cached directory entries (using Balanced adjustment tuning option)	1080	200
Manual tuning	Disable	Disable

Node-Level Parameters - Source Route Bridging

Table 5-512. Node Level - Source Route Bridging Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Source Route Bridging	Enable	Enable
Bridge number	1	2
Enable LAN Bridging Protocol	Enable	Enable
Designated ring number	11	21
Spanning tree parameters		
Bridge priority	8000	8000
Hello time	2	2
Forward delay	15	15
Max age	20	20

Node-Level Parameters - Transparent Bridging

Table 5-513. Node Level - Transparent Bridging Parameters Configured

Parameter	6611 B Value
Enable Transparent Bridging	Enable
Duplicate address check	Filter
overflow policy	Learn
Aging time	300
Spanning tree parameters	
Bridge priority	8000
Hello time	2
Forward delay	15
Max age	20

Node-Level Parameters - DLSw

Table 5-514. Node Level - DLSw Parameters Configured

Parameter	6611 A Value	6611 B Value
Protocols forwarded by DLSw		
SNA	Enable	Enable
NetBIOS	Disable	Disable
SNA transmission bias	NA	NA
Maximum NetBIOS frame size	2052	2052
DLSw parameters		
Virtual ring segment number	F01	F01
Destination cache timeout	8	8
Default DLSw IP address for this 6611	9.67.21.1	9.67.19.1

Node Level Worksheets

Figure 5-50 on page 5-369 shows the configuration paths through the Configuration Program. The titles of the worksheets in this section correspond to the window titles shown in Figure 5-52.

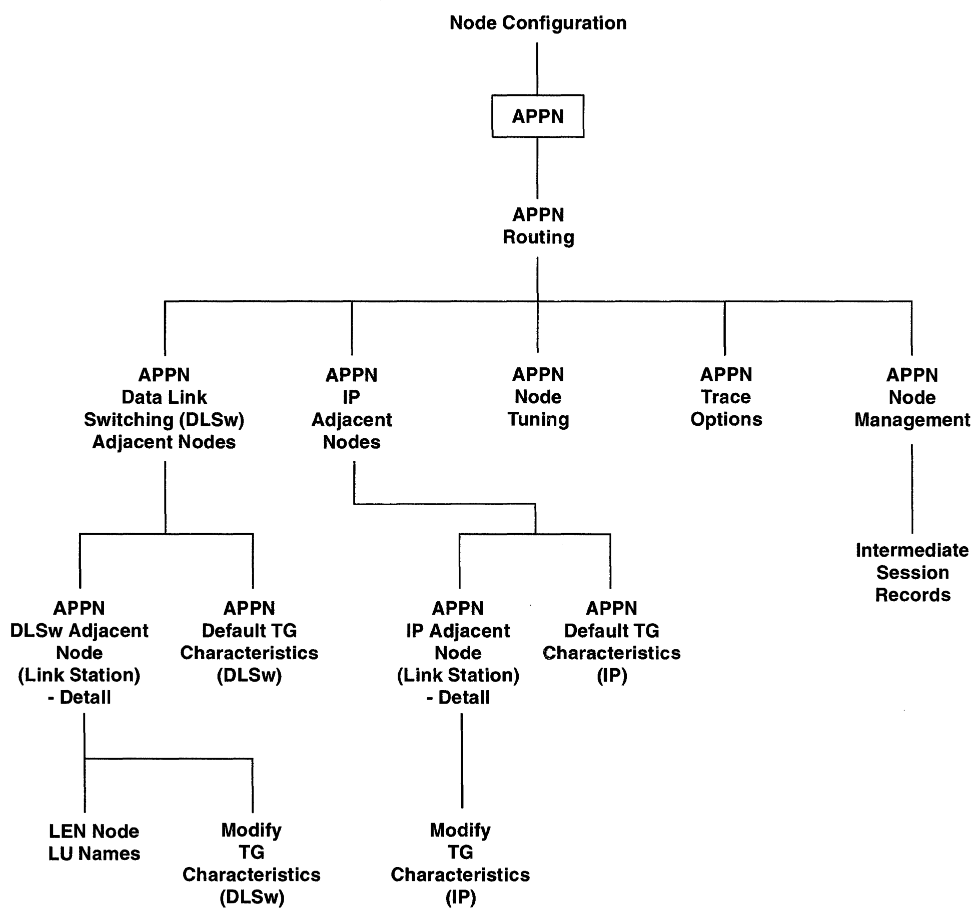


Figure 5-52. Flow of Node Level APPN Help Windows

Use the following tables as worksheets to configure APPN:

- APPN Routing on page 5-395
- APPN Default TG Characteristics (DLSw) on page 5-396

For additional information on any parameter, including any configuration dependencies, refer to the Configuration Program Help window for the parameter. If you are working with an ASCII-formatted configuration file, refer to Table D-3 on page D-5 for a mapping of parameter names and their associated labels.

Table 5-515 (Page 1 of 2). Configuration Worksheet - APPN Routing

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable APPN Enable, Disable Disable This parameter enables or disables the 6611 as an APPN network node.	
Parameter **Valid Values** **Default Value** **Description**	Network ID (required) A string of 1 to 8 characters: • First character: A to Z, @, or $ • Second to eighth characters: A to Z, 0 to 9, @, or $ **Note:** IBM recommends that the special characters @ and $ not be used in the network ID unless they are part of an existing network ID that will be used by this node. None This parameter specifies the name of the APPN network to which this network node belongs.	
Parameter **Valid Values** **Default** **Description**	Control point name (required) A string of 1 to 8 characters, • First character: A to Z, @, or $ • Second to eighth characters: A to Z, 0 to 9, @, or $ None This parameter specifies the name of the control point for this APPN network node. The CP name is the logical name of the APPN network node in the network. The CP name must be unique within the APPN network identified by the Network ID parameter.	
Parameter **Valid Values** **Default** **Description**	XID ID number for subarea connection (see table notes) A string of 5 hexadecimal digits (0 to 9, A, B, C, D, E, F) X'00000' This parameter specifies a unique ID number (identifier) for the network node. The XID ID number is combined with an XID block number (which identifies a specific IBM product) to form an *XID node identification.* Node identifications are exchanged between adjacent nodes when the nodes are establishing a connection. The 6611 network node automatically appends an XID block number to this parameter during the XID exchange to create an XID node identification.	

Table 5-515 (Page 2 of 2). Configuration Worksheet - APPN Routing

Parameter Information	Your Value
Parameter Locally administered MAC address (required) **Valid Values** X'4000 0000 0000' to X'7FFF FFFF FFFF' **Default Value** None **Description** This parameter specifies an address, in the form of a medium access control (MAC) address, for the 6611 network node. This address, combined with the SAP address for the network node, uniquely identifies the node to the DLSw function. The address you assign is locally administered and must not correspond to any physical MAC address.	
Parameter SAP address **Valid Values** X'04' to X'EC', in increments of 4 **Default Value** X'04' **Description** This parameter specifies the service access point (SAP) address to be used by the APPN component in the 6611 network node. The SAP address represents the logical interface that the APPN component uses to acquire LLC services from the DLSw function. X'04' is the default SAP used by SNA nodes.	
Parameter Accept connection requests from any node **Valid Values** Enable, Disable **Default Value** Enable **Description** This parameter controls how the 6611 network node responds to a request from another node to establish a connection. Connection requests may be received from APPN network nodes, APPN end nodes, and LEN end nodes. When this parameter is set to **Disable,** the network node accepts connection requests *only* from nodes that you explicitly define through the network node.	

Note: Node identifications are normally exchanged between T2.1 nodes during a CP-CP session. If the network node is communicating with the IBM Virtual Telecommunications Access Method (VTAM*) product through a T2.1 LEN node and the LEN node has a CP name defined for it, the XID ID number parameter is not required. If the adjacent LEN node is not a T2.1 node or does not have an explicitly defined CP name, the XID ID number parameter must be specified to establish a connection with the LEN node. VTAM versions prior to Version 3 Release 2 do not allow CP names to be defined for LEN nodes.

Table 5-516 (Page 1 of 2). Configuration Worksheet - APPN Default TG Characteristics (DLSw) (See table note)

Parameter Information	Your Value
Parameter Cost per connect time **Valid Values** 0 to 255 **Default Value** 0 **Description** This parameter specifies the default cost per connect time for all DLSw connections (TGs). The cost per connect time expresses the relative cost of maintaining a connection over this type of TG. The units (0 to 255) are user-defined and are typically based on the applicable tariffs for the transmission facilities used by this type of TG. A value of zero means that connections over these TGs can be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.	

Table 5-516 (Page 2 of 2). Configuration Worksheet - APPN Default TG Characteristics (DLSw) (See table note)

Parameter Information		Your Value
Parameter	Cost per byte	
Valid Values	0 to 255	
Default Value	0	
Description	This parameter specifies the default cost per byte for all DLSw connections (TGs). The cost per byte is the relative cost of transmitting a byte over this type of TG. The units (0 to 255) are user-defined. A value of zero means that bytes can be transmitted over these TGs at no additional cost. Higher values represent higher costs.	
Parameter	Security	
Valid Values	Nonsecure (X'01'), Public switched network (X'20'), Underground (X'40'), Secure (X'60'), Guarded conduit (X'80'), Encrypted (X'A0'), Guarded radiation (X'C0')	
Default Value	Nonsecure (X'01')	
Description	This parameter specifies the default level of security protection for all DLSw connections (TGs). The security values are architecturally defined.	
Parameter	Propagation delay	
Valid Values	Terrestrial (X'71'), Negligible (X'4C'), Packet switched (X'91'), Long (X'99')	
Default Value	Terrestrial (X'71')	
Description	This parameter specifies the default propagation delay for all DLSw connections (TGs). The propagation delay is the length of time it takes for a signal to propagate, or travel, from one end of a TG to the other end.	
Parameter	Effective capacity	
Valid Values	X'00' to X'FF'	
Default Value	X'75' (represents approximately 4 Mbps)	
Description	This parameter specifies the default effective capacity for all DLSw connections (TGs). Effective capacity represents the highest bit transmission rate that TGs are allowed to obtain before being considered overloaded. The computed effective capacity approximates the bits per second that a link can transmit (the transmission rate of the link, times a maximum load factor expressed as a percentage). The Configuration Program help for this parameter contains a table that maps effective capacities to link speeds.	
Parameter	First user-defined TG characteristic	
Valid Values	0 to 255	
Default Value	128	
Description	This parameter specifies the default value for the first user-defined TG characteristic. The default applies to all DLSw connections (TGs). In addition to the architected TG characteristics, you can define up to three user-defined characteristics to describe TGs in a network. User-defined TG characteristics are represented as integers in the range of 0 to 255.	
Parameter	Second user-defined TG characteristic	
Valid Values	0 to 255	
Default Value	128	
Description	This parameter specifies the default value for the second user-defined TG characteristic. The default applies to all DLSw connections (TGs).	
Parameter	Third user-defined TG characteristic	
Valid Values	0 to 255	
Default Value	128	
Description	This parameter specifies the default value for the third user-defined TG characteristic. The default applies to all DLSw connections (TGs).	

Note: You can modify any of the default TG characteristics when defining specific DLSw connections to adjacent APPN nodes. See Table 5-519 on page 5-401 (Modify TG Characteristics).

Table 5-517 (Page 1 of 3). Configuration Worksheet - APPN DLSw Adjacent Nodes (Link Station) - Detail

<table>
<tr><th colspan="2">Parameter Information</th><th>Your Value</th></tr>
<tr><td colspan="3">Adjacent Node List - Parameters configured for each node defined</td></tr>
<tr><td>Parameter
Valid Values

Default Value
Description</td><td>Link station name (required for each adjacent node defined)
A string of 1 to 8 characters,
• First character: A to Z, @, or $
• Second to eighth characters: A to Z, 0 to 9, @, or $
None
This parameter specifies a name that represents the link between the 6611 network node and the adjacent node. You can define only one link station for each adjacent node, but each link station supports multiple sessions. The link station name must be unique within this network node.</td><td></td></tr>
<tr><td>Parameter
Valid Values

Default Value
Description</td><td>MAC address (required for each adjacent node defined)
For an address in noncanonical format, the valid range is,
X'4000 0000 0000' to X'7FFF FFFF FFFF'

For an address in canonical format, the valid ranges are,
X'x2 xx xx xx xx xx'
X'x6 xx xx xx xx xx'
X'xA xx xx xx xx xx'
X'xE xx xx xx xx xx'

where x is any hexadecimal digit.
None
This parameter specifies the MAC address of the adjacent node. When the adjacent node is attached to a LAN, this is the physical address of the node on the LAN. (For nodes attached to an Ethernet LAN, this address must be in canonical format.) When the adjacent node is connected to the 6611 network node across a WAN, this is the address the adjacent node uses to communicate with the DLSw function. The adjacent node, in this case, must be another 6611 network node.

The MAC address, combined with the adjacent node's SAP address, uniquely identifies the adjacent node.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>SAP address
X'04' to X'EC', in increments of 4
X'04'
This parameter specifies the SAP address to be used by the APPN component in the adjacent node.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Activate link automatically
Enable, Disable
Enable
When this parameter is enabled, the 6611 network node automatically activates the link to the adjacent node and initiates a connection.</td><td></td></tr>
<tr><td>Parameter
Valid Values
Default Value
Description</td><td>Enable session level security
Enable, Disable
Disable
This parameter enables or disables the session level security feature for connections between the 6611 network node and the adjacent node. When the feature is enabled, the 6611 network node will establish a connection with a control point on this link only if the control point has the same hexadecimal key as the one specified for the Key parameter.</td><td></td></tr>
</table>

Table 5-517 (Page 2 of 3). Configuration Worksheet - APPN DLSw Adjacent Nodes (Link Station) - Detail

Parameter Information	Your Value
Parameter Key (required when session level security is enabled) **Valid Values** A string of up to 16 hexadecimal digits (0 to 9, A, B, C, D, E, F). If fewer than 16 digits are specified, the value is padded on the right with zeros. **Default Value** None **Description** This parameter specifies a hexadecimal *key* that the 6611 network node uses to verify its connection partner. The connection partner must specify an identical key. The 6611 network node and the adjacent node compare data encrypted using their respective keys before establishing a connection. If the data does not match, the 6611 does not establish the connection. It is recommended that the chosen key uniquely identify the link between the 6611 network node and the adjacent node associated with the link station.	
Parameter Adjacent node type **Valid Values** APPN node, LEN node **Default Value** APPN node **Description** This parameter identifies whether the adjacent node is an APPN node or a LEN end node.	
Parameter Fully qualified control point name (see table notes) **Valid Values** A string of up to 17 characters in the form *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a control point name from 1 to 8 characters. Each name must conform to the following rules: • First character: A to Z, @, or $ • Second to eighth characters: A to Z, 0 to 9, @, or $ **Default Value** None **Description** This parameter specifies the adjacent node's fully qualified CP name, which consists of the node's network ID and CP name. The network ID is the name of the network that contains the adjacent node. The CP name is the logical name of the adjacent node and must be unique within the network specified by the network ID.	
Parameter XID block number (see table notes) **Valid Values** A string of 3 hexadecimal digits, with the following values: • X'01D', if the adjacent LEN node provides a direct connection to VTAM • X'01E', if the adjacent LEN node provides a connection to VTAM through the IBM Network Control Program (NCP) **Default Value** X'000' **Description** If the adjacent node is a LEN end node, this parameter specifies the XID block number associated with the adjacent node. The XID block number identifies the specific IBM product in the adjacent node that will communicate with this APPN network node.	

Table 5-517 (Page 3 of 3). Configuration Worksheet - APPN DLSw Adjacent Nodes (Link Station) - Detail

Parameter Information		Your Value
Parameter	XID ID number	
Valid Values	A string of 5 hexadecimal digits (0 to 9, A, B, C, D, E, F)	
Default Value	X'00000'	
Description	If the adjacent node is a LEN end node, this parameter specifies the XID ID number associated with the adjacent node. The XID ID number serves as a unique identification number for the adjacent node.	

Notes:

- The Fully qualified control point name parameter is required when:
  - The 6611 network node will *not* accept connection requests from any node.
  - The adjacent node is a LEN node.
  - The session level security feature is enabled for connections with the adjacent node.

  Otherwise, the adjacent node's CP name is learned automatically during the XID exchange between the 6611 network node and the adjacent node.
- The XID block number is combined with the XID ID number to form a unique XID node identification for the adjacent node. Node identifications are exchanged between the 6611 network node and the adjacent node when the nodes are establishing a connection.

Table 5-518. Configuration Worksheet - LEN Node LU Names

Parameter Information		Your Value
LU Name List - Parameter configured for each LU defined		
Parameter	Fully qualified LU name (required for each LU name defined)	
Valid Values	A string of up to 17 characters in the form *netID.LUname*, where: • *netID* is a network ID from 1 to 8 characters • *LUname* is an LU name from 1 to 8 characters. Each name must conform to the following rules: • First character: A to Z, @, or $ • Second to eighth characters: A to Z, 0 to 9, @, or $	
Default Value	None	
Description	This parameter specifies the name of an LU in an adjacent LEN node that can be reached through the 6611 network node. If a LEN node LU is not defined on the 6611 network node, the 6611 will not be able to locate it (unless the LU name is the same as the CP name of the LEN node).	

Note: To reduce the number of fully qualified LU names that you need to specify, you can use a wildcard character (*) to represent all or a portion of the actual LU name (*LUname*). A wildcard character cannot be used as part of the network ID (*netID*). The rules for using wildcard characters are:

- A wildcard character can be used to represent the entire LU name. This is a *full wildcard* character. Only one entry containing a full wildcard character may be used within the network specified in the network ID portion of the fully qualified name.
- A wildcard character can be used to represent the second to eighth characters of the LU name. The wildcard character is always the last character in the name.
- An LU name defined with a wildcard character must be unique within the local directory of the 6611 network node.

Table 5-519 (Page 1 of 2). Configuration Worksheet - Modify TG Characteristics (DLSw) (See table note)

Parameter Information		Your Value
Parameter	Cost per connect time	
Valid Values	0 to 255	
Default Value	The cost per connect time value specified in Table 5-516 on page 5-396.	
Description	This parameter specifies the cost per connect time for a specific DLSw connection (TG). The cost per connect time expresses the relative cost of maintaining a connection over this TG. The units (0 to 255) are user-defined and are typically based on the applicable tariffs for the transmission facility used by this TG. A value of zero means that connections over this TG can be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.	
Parameter	Cost per byte	
Valid Values	0 to 255	
Default Value	The cost per byte value specified in Table 5-516 on page 5-396.	
Description	This parameter specifies the cost per byte for a specific DLSw connection (TG). The cost per byte is the relative cost of transmitting a byte over this TG. The units (0 to 255) are user-defined. A value of zero means that bytes can be transmitted over this TG at no additional cost. Higher values represent higher costs.	
Parameter	Security	
Valid Values	Nonsecure (X'01'), Public switched network (X'20'), Underground (X'40'), Secure (X'60'), Guarded conduit (X'80'), Encrypted (X'A0'), Guarded radiation (X'C0')	
Default Value	The security value specified in Table 5-516 on page 5-396.	
Description	This parameter specifies the level of security protection provided by a specific DLSw connection (TG). The security values are architecturally defined.	
Parameter	Propagation delay	
Valid Values	Terrestrial (X'71'), Negligible (X'4C'), Packet switched (X'91'), Long (X'99')	
Default Value	The propagation delay specified in Table 5-516 on page 5-396.	
Description	This parameter specifies the propagation delay for a specific DLSw connection (TG). The propagation delay is the length of time it takes for a signal to propagate, or travel, from one end of the TG to the other end.	
Parameter	Effective capacity	
Valid Values	X'00' to X'FF'	
Default Value	The effective capacity specified in Table 5-516 on page 5-396.	
Description	This parameter specifies the effective capacity for a specific DLSw connection (TG). Effective capacity represents the highest bit transmission rate that a TG is allowed to obtain before being considered overloaded. The computed effective capacity approximates the bits per second that the link can transmit (the transmission rate of the link, times a maximum load factor expressed as a percentage). The Configuration Program help for this parameter contains a table that maps effective capacities to link speeds.	
Parameter	First user-defined TG characteristic	
Valid Values	0 to 255	
Default Value	The value specified for this TG characteristic in Table 5-516 on page 5-396.	
Description	This parameter specifies the value of the first user-defined TG characteristic for a specific DLSw connection (TG). In addition to the architected TG characteristics, you can define up to three user-defined characteristics to describe this TG. User-defined TG characteristics are represented as integers in the range of 0 to 255.	

Table 5-519 (Page 2 of 2). Configuration Worksheet - Modify TG Characteristics (DLSw) (See table note)

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Second user-defined TG characteristic 0 to 255 The value specified for this TG characteristic in Table 5-516 on page 5-396. This parameter specifies the value of the second user-defined TG characteristic for a specific DLSw connection (TG).	
Parameter **Valid Values** **Default Value** **Description**	Third user-defined TG characteristic 0 to 255 The value specified for this TG characteristic in Table 5-516 on page 5-396. This parameter specifies the value of the third user-defined TG characteristic for a specific DLSw connection (TG).	

Note: The parameters in Table 5-516 on page 5-396 specify the default TG characteristics for all DLSw connections to adjacent APPN nodes. To modify the default TG characteristics when defining the link station for a specific DLSw connection, configure the appropriate parameters in this table. These parameters override the default characteristics only for the connection being defined.

Table 5-520 (Page 1 of 2). Configuration Worksheet - APPN Default TG Characteristics (IP) (See table note)

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Cost per connect time 0 to 255 0 This parameter specifies the default cost per connect time for all IP connections (TGs). The cost per connect time expresses the relative cost of maintaining a connection over this type of TG. The units (0 to 255) are user-defined and are typically based on the applicable tariffs for the transmission facilities used by this type of TG. A value of zero means that connections over these TGs can be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.	
Parameter **Valid Values** **Default Value** **Description**	Cost per byte 0 to 255 0 This parameter specifies the default cost per byte for all IP connections (TGs). The cost per byte is the relative cost of transmitting a byte over this type of TG. The units (0 to 255) are user-defined. A value of zero means that bytes can be transmitted over these TGs at no additional cost. Higher values represent higher costs.	
Parameter **Valid Values** **Default Value** **Description**	Security Nonsecure (X'01'), Public switched network (X'20'), Underground (X'40'), Secure (X'60'), Guarded conduit (X'80'), Encrypted (X'A0'), Guarded radiation (X'C0') Nonsecure (X'01') This parameter specifies the default level of security protection for all IP connections (TGs). The security values are architecturally defined.	
Parameter **Valid Values** **Default Value** **Description**	Propagation delay Terrestrial (X'71'), Negligible (X'4C'), Packet switched (X'91'), Long (X'99') Terrestrial (X'71') This parameter specifies the default propagation delay for all IP connections (TGs). The propagation delay is the length of time it takes for a signal to propagate, or travel, from one end of a TG to the other end.	

Table 5-520 (Page 2 of 2). Configuration Worksheet - APPN Default TG Characteristics (IP) (See table note)

Parameter Information		Your Value
Parameter	Effective capacity	
Valid Values	X'00' to X'FF'	
Default Value	X'38' (represents approximately 20 Kbps)	
Description	This parameter specifies the default effective capacity for all IP connections (TGs). Effective capacity represents the highest bit transmission rate that TGs are allowed to obtain before being considered overloaded. The computed effective capacity approximates the bits per second that a link can transmit (the transmission rate of the link, times a maximum load factor expressed as a percentage). The Configuration Program help for this parameter contains a table that maps effective capacities to link speeds.	
Parameter	First user-defined TG characteristic	
Valid Values	0 to 255	
Default Value	128	
Description	This parameter specifies the default value for the first user-defined TG characteristic. The default applies to all IP connections (TGs). In addition to the architected TG characteristics, you can define up to three user-defined characteristics to describe TGs in a network. User-defined TG characteristics are represented as integers in the range of 0 to 255.	
Parameter	Second user-defined TG characteristic	
Valid Values	0 to 255	
Default Value	128	
Description	This parameter specifies the default value for the second user-defined TG characteristic. The default applies to all IP connections (TGs).	
Parameter	Third user-defined TG characteristic	
Valid Values	0 to 255	
Default Value	128	
Description	This parameter specifies the default value for the third user-defined TG characteristic. The default applies to all IP connections (TGs).	

Note: You can modify any of the default TG characteristics when defining specific IP connections to adjacent APPN network nodes. See Table 5-522 on page 5-405 (Modify TG Characteristics).

Table 5-521 (Page 1 of 2). Configuration Worksheet - APPN IP Adjacent Node (Link Station) - Detail

Parameter Information		Your Value
Adjacent Node List - Parameters configured for each node defined		
Parameter	Link station name (required for each adjacent node defined)	
Valid Values	A string of 1 to 8 characters, • First character: A to Z, @, or $ • Second to eighth characters: A to Z, 0 to 9, @, or $	
Default Value	None	
Description	This parameter specifies a name that represents the link between the 6611 network node and the adjacent node. You can define only one link station for each adjacent node, but each link station supports multiple sessions. The link station name must be unique within this network node.	
Parameter	IP address (required for each adjacent node defined)	
Valid Values	The valid ranges for IP address classes are: • Class A — 1.0.0.1 through 126.255.255.254 • Class B — 128.0.0.1 through 191.255.255.254 • Class C — 192.0.0.1 through 223.255.255.254	
Default Value	None	
Description	This parameter specifies the IP address of the adjacent node. The adjacent node, in this case, must be another 6611 network node.	

Table 5-521 (Page 2 of 2). Configuration Worksheet - APPN IP Adjacent Node (Link Station) - Detail

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Activate link automatically Enable, Disable Enable When this parameter is enabled, the 6611 network node automatically activates the link to the adjacent node and initiates a connection.	
Parameter **Valid Values** **Default Value** **Description**	Enable session level security Enable, Disable Disable This parameter enables or disables the session level security feature for connections between the 6611 network node and the adjacent node. When the feature is enabled, the 6611 network node will establish a connection with a control point on this link only if the control point has the same hexadecimal *key* as the one specified for the Key parameter.	
Parameter **Valid Values** **Default Value** **Description**	Key (required when session level security is enabled) A string of up to 16 hexadecimal digits (0 to 9, A, B, C, D, E, F). If fewer than 16 digits are specified, the value is padded on the right with zeros. None This parameter specifies a hexadecimal *key* that the 6611 network node uses to verify its connection partner. The connection partner must specify an identical key. The 6611 network node and the adjacent node compare data encrypted using their respective keys before establishing a connection. If the data does not match, the 6611 does not establish the connection. It is recommended that the chosen key uniquely identify the link between the 6611 network node and the adjacent node associated with the link station.	
Parameter **Valid Values** **Default Value** **Description**	Fully qualified control point name (see table notes) A string of up to 17 characters in the form *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a control point name from 1 to 8 characters. Each name must conform to the following rules: • First character: A to Z, @, or $ • Second to eighth characters: A to Z, 0 to 9, @, or $ None This parameter specifies the adjacent node's fully qualified CP name, which consists of the node's network ID and CP name. The network ID is the name of the network that contains the adjacent node. The CP name is the logical name of the adjacent node and must be unique within the network specified by the network ID.	

Note: The Fully qualified control point name parameter is required when:

- The 6611 network node will *not* accept connection requests from any node.
- The session level security feature is enabled for connections with the adjacent node.

Table 5-522 (Page 1 of 2). Configuration Worksheet - Modify TG Characteristics (IP) (See table note)

Parameter Information		Your Value
Parameter	Cost per connect time	
Valid Values	0 to 255	
Default Value	The cost per connect time value specified in Table 5-520 on page 5-402.	
Description	This parameter specifies the cost per connect time for a specific IP connection (TG). The cost per connect time expresses the relative cost of maintaining a connection over this TG. The units (0 to 255) are user-defined and are typically based on the applicable tariffs for the transmission facility used by this TG. A value of zero means that connections over this TG can be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.	
Parameter	Cost per byte	
Valid Values	0 to 255	
Default Value	The cost per byte value specified in Table 5-520 on page 5-402.	
Description	This parameter specifies the cost per byte for a specific IP connection (TG). The cost per byte is the relative cost of transmitting a byte over this TG. The units (0 to 255) are user-defined. A value of zero means that bytes can be transmitted over this TG at no additional cost. Higher values represent higher costs.	
Parameter	Security	
Valid Values	Nonsecure (X'01'), Public switched network (X'20'), Underground (X'40'), Secure (X'60'), Guarded conduit (X'80'), Encrypted (X'A0'), Guarded radiation (X'C0')	
Default Value	The security value specified in Table 5-520 on page 5-402.	
Description	This parameter specifies the level of security protection provided by a specific IP connection (TG). The security values are architecturally defined.	
Parameter	Propagation delay	
Valid Values	Terrestrial (X'71'), Negligible (X'4C'), Packet switched (X'91'), Long (X'99')	
Default Value	The propagation delay specified in Table 5-520 on page 5-402.	
Description	This parameter specifies the propagation delay for a specific IP connection (TG). The propagation delay is the length of time it takes for a signal to propagate, or travel, from one end of the TG to the other end.	
Parameter	Effective capacity	
Valid Values	X'00' to X'FF'	
Default Value	The effective capacity specified in Table 5-520 on page 5-402.	
Description	This parameter specifies the effective capacity for a specific IP connection (TG). Effective capacity represents the highest bit transmission rate that a TG is allowed to obtain before being considered overloaded. The computed effective capacity approximates the bits per second that the link can transmit (the transmission rate of the link, times a maximum load factor expressed as a percentage). The Configuration Program help for this parameter contains a table that maps effective capacities to link speeds.	
Parameter	First user-defined TG characteristic	
Valid Values	0 to 255	
Default Value	The value specified for this TG characteristic in Table 5-520 on page 5-402.	
Description	This parameter specifies the value of the first user-defined TG characteristic for a specific IP connection (TG). In addition to the architected TG characteristics, you can define up to three user-defined characteristics to describe this TG. User-defined TG characteristics are represented as integers in the range of 0 to 255.	

Table 5-522 (Page 2 of 2). Configuration Worksheet - Modify TG Characteristics (IP) (See table note)

Parameter Information	Your Value
Parameter Second user-defined TG characteristic **Valid Values** 0 to 255 **Default Value** The value specified for this TG characteristic in Table 5-520 on page 5-402. **Description** This parameter specifies the value of the second user-defined TG characteristic for a specific IP connection (TG).	
Parameter Third user-defined TG characteristic **Valid Values** 0 to 255 **Default Value** The value specified for this TG characteristic in Table 5-520 on page 5-402. **Description** This parameter specifies the value of the third user-defined TG characteristic for a specific IP connection (TG).	

Note: The parameters in Table 5-520 on page 5-402 specify the default TG characteristics for all IP connections to adjacent APPN network nodes. To modify the default TG characteristics when defining the link station for a specific IP connection, configure the appropriate parameters in this table. These parameters override the default characteristics only for the connection being defined.

Table 5-523 (Page 1 of 2). Configuration Worksheet - APPN Node Tuning

Parameter Information	Your Value
Parameter Max. number of APPN network nodes **Valid Values** 5 to 65535 **Default Value** 5 **Description** This parameter is an *estimate* of the maximum number of network nodes that you expect to support in the APPN network identified by the Network ID parameter.	
Parameter Max. number of serviced end and LEN nodes **Valid Values** 1 to 65535 **Default** 50 **Description** This parameter is an estimate of the maximum number of APPN end nodes and LEN end nodes that you expect to be serviced by this 6611 network node.	
Parameter Avg. number of LUs for serviced nodes **Valid Values** 1 to 65535 **Default Value** 1 **Description** This parameter specifies the average number of LUs associated with end nodes and LEN end nodes serviced by this 6611 network node.	
Parameter Select tuning option **Valid Values** One of the following options: • Best performance (more storage used) • Improved performance • Balanced adjustment • Less storage used • Minimum storage used **Default Value** Balanced adjustment **Description** This parameter specifies the tuning option to be used to tune the performance of the 6611 network node. Each option corresponds to a set of values that the Configuration program automatically generates for the Maximum shared memory parameter and the Maximum cached directory entries parameter. The values are displayed beside the appropriate option on the APPN Node Tuning window. See "Tuning the APPN Network Node" on page 5-372 for information about using the APPN Node Tuning window.	

Table 5-523 (Page 2 of 2). Configuration Worksheet - APPN Node Tuning

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Manual tuning Enable, Disable Disable When enabled, this parameter overrides the tuning calculations generated by the Configuration Program and enables you to specify explicit values for the Maximum shared memory parameter and the Maximum cached directory entries parameter.	
Parameter **Valid Values** **Default Value** **Description**	Maximum shared memory 2 to 11 megabytes Calculated based on the values specified for the following parameters: • Max. number of APPN network nodes • Max. number of serviced end and LEN nodes • Avg. number of LUs for serviced nodes This parameter specifies the amount of shared memory within the 6611 that is allocated to the APPN network node. APPN uses its shared memory allocation to perform network operations and to maintain required tables and directories.	
Parameter **Valid Values** **Default** **Description**	Maximum cached directory entries 10 to 65535 Calculated based on the values specified for the following parameters: • Max. number of APPN network nodes • Max. number of serviced end and LEN nodes • Avg. number of LUs for serviced nodes This parameter specifies the number of directory entries to be stored or cached by the 6611 network node. If a directory entry for a node is cached, the 6611 does not need to broadcast a search request to locate the node. This reduces the time it takes to initiate sessions with the node.	

Note: The simplest way to calculate the average number of LUs associated with adjacent end nodes serviced by the 6611 network node is to divide the total number of LUs in the serviced end nodes by the number of serviced end nodes. When determining the number of LUs associated with a LEN end node, use the number of LUs that are registered in the 6611 network node's local directory. For tuning purposes, you can estimate the number of LUs associated with an adjacent end node. However, more exact estimates will yield more accurate tuning information.

Table 5-524 (Page 1 of 4). Configuration Worksheet - APPN Trace Options

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Process management Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about the management of processes within the APPN network node, including the creation and termination of processes, processes entering a wait state, and the posting of processes.	
Parameter **Valid Values** **Default Value** **Description**	Process to process communication Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about messages exchanged between processes in the APPN network node, including the queuing and receipt of such messages.	

Table 5-524 (Page 2 of 4). Configuration Worksheet - APPN Trace Options

Parameter Information	Your Value
Parameter Locking **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about locks that were obtained and released on processes in the APPN network node.	
Parameter Miscellaneous tower activities **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about miscellaneous activities within the APPN network node.	
Parameter I/O to and from the system **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about the flow of messages entering and exiting the APPN network node.	
Parameter Storage management **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about any shared memory that was obtained and released by the APPN network node.	
Parameter Queue data type management **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about all calls in the APPN network node that manage general purpose queues.	
Parameter Table data type management **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about all calls in the APPN network node that manage general purpose tables, including calls to add table entries and calls to query tables for specific entries.	
Parameter Buffer management **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about buffers in the APPN network node that were obtained and released.	

Table 5-524 (Page 3 of 4). Configuration Worksheet - APPN Trace Options

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Configuration control Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about the activities of the configuration control component of the APPN network node. The configuration control component manages information about node resources.	
Parameter **Valid Values** **Default Value** **Description**	Timer service Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about requests for timer service from the APPN network node.	
Parameter **Valid Values** **Default Value** **Description**	Service provider management Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about the definition and enabling or disabling of services within the APPN network node.	
Parameter **Valid Values** **Default Value** **Description**	Interprocess message segmenting Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about the buffer transfer and freeing of chained messages within the APPN network node.	
Parameter **Valid Values** **Default Value** **Description**	Control of processes outside scope of this tower Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about the definition and activation of processes external to this APPN network node, such as when the node operator facility (NOF) defines the external process configuration control.	
Parameter **Valid Values** **Default Value** **Description**	Monitoring existence of processes, services, towers Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about requests that start or stop the monitoring of processes or services within the APPN network node.	
Parameter **Valid Values** **Default Value** **Description**	Distributed environment control Enable, Disable Disable This parameter enables or disables this APPN trace option. When enabled, the trace option causes the 6611 trace facility to gather data about requests within the APPN network node that define subsystems and create environments.	

Table 5-524 (Page 4 of 4). Configuration Worksheet - APPN Trace Options

Parameter Information		Your Value
Parameter	Process to service dialogs	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables this APPN trace option. When enabled, this trace option causes the 6611 trace facility to gather data about all calls within the APPN network node that open, close, or send data on a dialog.	

Table 5-525. Configuration Worksheet - APPN Node Management

Parameter Information		Your Value
Parameter	Collect intermediate session information (see table note)	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter specifies whether the APPN node should collect data on intermediate sessions passing through this node (session counters and session characteristics). The data is captured in SNMP MIB variables for APPN.	
Parameter	Save RSCV information for intermediate sessions (see table note)	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter specifies whether the APPN node should save the Route Selection control vector (RSCV) for an intermediate session. The data is captured in an associated SNMP MIB variable for APPN. The session RSCV is carried in the BIND request used to activate a session between two logical units (LUs). It describes the optimum route through an APPN network for a particular LU-LU session. The session RSCV contains the CP names and TG associated with each pair of adjacent nodes along a route from an origin node to a destination node.	

Note: See "Intermediate Session Accounting" on page 5-373 for information on the APPN MIB variables associated with this parameter and a description of the specific data collected for intermediate sessions.

Table 5-526 (Page 1 of 3). Configuration Worksheet - APPN Intermediate Session Records

Parameter Information		Your Value
Parameter	Create intermediate session records (see table notes)	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables the creation of data records for intermediate sessions passing through this node. The records contain information on session counters and session characteristics. RSCV information is also included in the data records if the Save RSCV information for intermediate sessions parameter is enabled.	
Parameter	Record creation threshold	
Valid Values	0 to 4294967, in 1000-byte increments	
Default Value	0	
Description	This parameter specifies a byte threshold for creating intermediate session records. When session data exceeds the value in this byte counter by an even multiple, a record is created.	

Recording Media - DASD Parameters

Table 5-526 (Page 2 of 3). Configuration Worksheet - APPN Intermediate Session Records

Parameter Information		Your Value
Parameter	DASD (see table notes)	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables the collection of intermediate session data on the 6611's hard disk.	
Parameter	Maximum buffers	
Valid Values	0 to 3	
Default Value	3	
Description	This parameter specifies the maximum number of DASD buffers to be allocated on the 6611's hard disk for storing intermediate session records.	
Parameter	Maximum records per buffer	
Valid Values	0 to 500	
Default Value	500	
Description	This parameter specifies the maximum number of intermediate session records that may be stored in a single DASD buffer on the 6611's hard disk.	
Parameter	Buffers full	
Valid Values	Stop recording, Wrap	
Default Value	Stop recording	
Description	This parameter specifies the action to take when the DASD buffers allocated to store intermediate session records become full. Select **Stop recording** to instruct the 6611 to discard any new intermediate session records. Select **Wrap** to delete the full buffer and create a new buffer. The oldest buffer is deleted first.	
Parameter	Record format	
Valid Values	ASCII, Binary	
Default Value	ASCII	
Description	This parameter specifies the format in which intermediate session records are to be stored on the 6611's hard disk.	
Recording Media - Memory Parameters		
Parameter	Memory (see table notes)	
Valid Values	Enable, Disable	
Default Value	Enable	
Description	This parameter enables or disables the collection of intermediate session data in the 6611's local memory.	
Parameter	Maximum buffers	
Valid Values	0 to 1	
Default Value	1	
Description	This parameter specifies the number of buffers to be allocated in the 6611's local memory for storing intermediate session records.	
Parameter	Maximum records per buffer	
Valid Values	0 to 500	
Default Value	500	
Description	This parameter specifies the maximum number of intermediate session records that may be stored in the memory buffer on the 6611.	

Table 5-526 (Page 3 of 3). Configuration Worksheet - APPN Intermediate Session Records

Parameter Information	Your Value
Parameter Buffers full **Valid Values** Stop recording, Wrap **Default Value** Stop recording **Description** This parameter specifies the action to take when the memory buffer allocated to store intermediate session records becomes full. Select **Stop recording** to instruct the 6611 to discard any new intermediate session records. Select **Wrap** to allow new records to overwrite existing records in the buffer. The oldest records in the buffer are overwritten first.	
Parameter Record format **Valid Values** ASCII, Binary **Default Value** ASCII **Description** This parameter specifies the format in which intermediate session records are to be stored in the 6611's local memory.	

Note:

- When you enable the collection of intermediate session records, the data associated with the records also is collected, by default, in SNMP MIB variables for APPN. The MIB variables are updated, in this case, whether or not the Collect intermediate session information parameter (in Table 5-525) has been enabled. See "Intermediate Session Accounting" on page 5-373 for a description of the specific data collected for intermediate sessions and a list of the associated APPN MIB variables.
- At least one recording medium, DASD or Memory, must be enabled when the Create intermediate session records parameter is enabled. Intermediate session data can be stored on the 6611 hard disk, in router memory, or in both locations, in the format you specify.

Chapter 6. Configuring Node Management

This chapter describes the node management tasks you can perform for the 6611:

- “Defining General Node Management Parameters”
- “Defining Simple Network Management Protocol (SNMP) Functions” on page 6-2
- “Controlling User IDs and Passwords” on page 6-6
- “Specifying a Scheduled Configuration” on page 6-7
- “Enabling the Auto Configuration Roll Back Function” on page 6-8
- “Listing Configuration Hosts for this 6611” on page 6-11
- “Specifying Name Servers” on page 6-10
- “Specifying Time Servers” on page 6-11
- “Specifying Remote Hosts” on page 6-10

Defining General Node Management Parameters

Node management configures parameters that enable you to manage your 6611. These parameters are not adapter or protocol dependent. Use the worksheet in Table 6-1 to configure the general node management parameters. If you are working with an ASCII-formatted configuration file, refer to tref refid=cfglist. and Table D-20 on page D-16 for a mapping of parameter names and their associated labels.

Before You Configure...

When the 6611 boots from a configuration diskette with the parameter set to **Lock**, the Multiprotocol Network Program is disabled. When the 6611 boots from a configuration diskette with the parameter set to **Unlock**, the Multiprotocol Network Program is enabled.

Table 6-1 (Page 1 of 2). Configuration Worksheet - Node Management

Parameter Information		Your Value
Parameter	6611 host name	
Valid Values	A string of up to 31 alphanumeric characters (optionally, these characters can be separated by periods, underscores, or dashes)	
Default Value	6611host	
Description	This parameter defines the host name by which the 6611 knows itself. If this name is correlated to one of this 6611's IP addresses by a remote IP node, it can be used in place of that IP address by that remote node (when accessing this 6611 remotely over the IP network).	
Parameter	Domain name	
Valid Values	A string of 63 alphanumeric characters (the characters can be separated by periods)	
Default Value	None	
Description	This parameter defines the domain name that is used to qualify hosts identified using a name server.	

Table 6-1 (Page 2 of 2). Configuration Worksheet - Node Management

Parameter Information		Your Value
Parameter	BAUD rate for S1 serial port	
Valid Values	9600, 2400, 1200, 19200, 38400	
Default Value	9600	
Description	This parameter defines the speed at which data is transmitted to and from the device attached to the S1 serial port. For a direct-attached terminal, 9600 bps should be configured. In some cases, you may want to configure 19200 or 38400 bps for attaching a high-function terminal. For a modem-attached terminal, 2400 bps should be configured.	
Parameter	BAUD rate for S2 serial port	
Valid Values	9600, 2400, 1200, 19200, 38400	
Default Value	2400	
Description	This parameter defines the speed at which data is transmitted to and from the device attached to the S2 serial port. For a direct-attached terminal, 9600 bps should be configured. In some cases, you may want to configure 19200 or 38400 bps for attaching a high-function terminal. For a modem-attached terminal, 2400 bps should be configured.	
Parameter	Lock value	
Valid Values	Lock, Unlock	
Default Value	Unlock	
Description	This parameter locks or unlocks the software on the 6611. If the machine is in an unlocked state and it boots from the configuration diskette with the parameter set to **Lock**, the software is disabled. If the machine is in a locked state and it boots from the configuration diskette with the parameter set to **Unlock**, the software unlocks itself. This parameter has no effect if it is set to **Unlock** and the software is already unlocked.	

Defining Simple Network Management Protocol (SNMP) Functions

The Simple Network Management Protocol (SNMP) is part of the TCP/IP suite of protocols, used to manage devices in an IP-based network. For more information about how SNMP works, refer to the *6611 Network Management Reference*.

Use the following worksheets to configure SNMP:

- SNMP on page 6-3
- SNMP Trap Client - Detail on page 6-4
- SNMP Views - Detail on page 6-5
- SNMP Communities - Detail on page 6-6

Restrictions

SNMP can be transported only over links that are configured for IP.

Before You Configure...

- Serial Number

  The serial number of the 6611 is obtained from the hardware vital product data that is burned in at the time of manufacture. You should *not* use the Configuration Program to change the serial number configuration except in the case that the hardware vital product data is corrupted (for example, if a hard drive failure occurs).

- Communities

An SNMP community is defined by a group of one or more SNMP clients and a community name. A community name is a string of octets that an SNMP client must embed in an SNMP request packet for authentication purposes.

At least one SNMP community must be configured, but there is no limit to the number of SNMP communities allowed. The 6611 provides a default SNMP community which allows any host to query this router using the name "public".

- Views

  A MIB view defines one or more MIB subtrees that a specific SNMP community can access. It can be the entire MIB tree or a limited subset of the entire MIB tree. A view consists of the specified subtree and all objects anchored under that subtree.

SNMP Worksheets

Table 6-2 (Page 1 of 2). Configuration Worksheet - SNMP

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable SNMP Enable, Disable Disable This parameter enables or disables configuration of the SNMP protocol.	
Parameter **Valid Values** **Default Value** **Description**	System contact A string of 1 to 255 ASCII characters (new-line characters and blanks may be included; an empty string is not valid) None This parameter provides information on the name and means to contact the person responsible for the 6611.	
Parameter **Valid Values** **Default Value** **Description**	System location A string of 1 to 255 ASCII-printable characters (new line characters and blanks may be included; an empty string is not valid) None This parameter provides directions to the geographic location of the 6611 (for example: telephone closet, 3rd floor, 812 Whyte Avenue).	
Parameter **Valid Values** **Default Value** **Description**	System name A string of 1 to 255 ASCII-printable characters (blanks may be included) None This parameter provides the administratively assigned name of the node. By convention, this is the node's fully qualified domain name.	
Parameter **Valid Values** **Default Value** **Description**	Enterprise-specific trap throttle time 0 to 3600 (seconds) 900 (seconds) This parameter defines the number of seconds that must separate consecutive enterprise-specific traps with identical IDs or numbers. A value of 0 indicates that all traps are to be sent.	

Table 6-2 (Page 2 of 2). Configuration Worksheet - SNMP

Parameter Information	Your Value
Parameter Router serial number prefix **Valid Values** A string composed of 2 alphanumeric characters (all alphabetic characters must be uppercase) **Default Value** None **Description** This parameter specifies the 2-character manufacture code of the serial number of the 6611. The 6611 is shipped with the serial number in the hardware vital product data (VPD). **Note:** If you change the serial number prefix in the Configuration Program, you must use System Manager to apply the change to the hardware VPD. For more information see *Introduction and Planning Guide*.	
Parameter Router serial number suffix **Valid Values** A string composed of 1 to 7 alphanumeric characters (all alphabetic characters must be uppercase) **Default Value** None **Description** This parameter specifies the latter portion of the serial number of this 6611. The 6611 is shipped with the serial number in the hardware VPD. **Note:** If you change this parameter, you must use the System Manager to apply the change to the hardware VPD.	

Table 6-3 (Page 1 of 2). Configuration Worksheet - SNMP Trap Client - Detail

Parameter Information	Your Value
Parameter Trap address **Valid Values** An IP address or Domain name, 1 to 63 alphanumeric characters and periods **Default** None **Description** This parameter specifies the host to which traps generated by the 6611 are sent.	
Parameter Trap community name **Valid Values** An alphanumeric string of 1 to 64 characters in length **Default** Public **Description** This parameter determines the community name encoded in the trap packet sent to the client specified in the Trap address parameter.	
Parameter Enable coldstart trap **Valid Values** Enable, Disable **Default** Enable **Description** This parameter determines if the SNMP coldStart trap is sent to the address specified by the Trap address parameter.	
Parameter Enable warmstart trap **Valid Values** Enable, Disable **Default** Enable **Description** This parameter determines if the SNMP warmStart trap is sent to the address specified by the Trap address parameter.	
Parameter Enable linkDown trap **Valid Values** Enable, Disable **Default** Enable **Description** This parameter determines if the SNMP linkDown trap is sent to the address specified by the Trap address parameter.	

Table 6-3 (Page 2 of 2). Configuration Worksheet - SNMP Trap Client - Detail

Parameter Information	Your Value
Parameter Enable linkUp trap **Valid Values** Enable, Disable **Default** Enable **Description** This parameter determines if the SNMP linkUp trap is sent to the address specified by the Trap address parameter.	
Parameter Enable authenticationFailure trap **Valid Values** Enable, Disable **Default** Enable **Description** This parameter determines if the SNMP authenticationFailure trap is sent to the address specified by the Trap address parameter.	
Parameter Enable egpNeighborLoss trap **Valid Values** Enable, Disable **Default** Enable **Description** This parameter determines if the SNMP egpNeighborLoss trap is sent to the address specified by the Trap address parameter.	
Parameter Enable enterpriseSpecific trap **Valid Values** Enable, Disable **Default** Enable **Description** This parameter determines if the SNMP enterpriseSpecific trap is sent to the address specified by the Trap address parameter.	

Table 6-4. Configuration Worksheet - SNMP Views - Detail

Parameter Information	Your Value
Parameter View name **Valid Values** An object identifier in the form of <element1>.<element2>.<element3>..., where: • You need a minimum of 3 elements. • You can define a maximum of 50 elements. • element1 is either 0, 1, or 2. • element2 is an integer between 1 and 40. • element3 and subsequent elements are integers between 1 and the size of an unsigned integer **Default Value** None **Description** This parameter contains the view name.	
Parameter MIB subtree **Valid Values** An object identifier in the form of <element1>.<element2>.<element3>..., where: • You need a minimum of 3 elements. • You can define a maximum of 50 elements. • element1 is either 0, 1, or 2. • element2 is an integer between 1 and 40. • element3 and subsequent elements are integers between 1 and the size of an unsigned integer **Default Value** None **Description** This parameter contains a MIB subtree name included in the view defined with the View name parameter. All children of a specified MIB subtree are also included in the view.	

Table 6-5. Configuration Worksheet - SNMP Communities - Detail

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Community name A string of 1 to 64 alphanumeric characters None This parameter provides a community name used by the SNMP client. This community name is used when accessing the MIB in the 6611 from the host specified by the Community IP address or domain name parameter.	
Parameter **Valid Values** **Default Value** **Description**	Community IP address or domain name 0.0.0.0, an IP host or network address or a domain name 0.0.0.0 This parameter defines the address of the host from which this 6611 accepts SNMP requests containing the community name specified by the Community name parameter. It represents a community address when accessing the Management Information Base (MIB) present in the 6611. The address is either an IP address or a host name (allowed only if a name server is available to the router).	
Parameter **Valid Values** **Default Value** **Description**	Community address mask 0.0.0.0 to 255.255.255.255 255.255.255.255 Use this parameter to enter into configuration a network mask in dotted-decimal format for the specified community address. If the address mask is specified as 0.0.0.0, the 6611 will accept SNMP requests from any host address as long as the request contains the community name of this community.	
Parameter **Valid Values** **Default Value** **Description**	Community access read only, read/write, None read only This parameter determines the access granted to the community when accessing the MIB in the 6611.	
Parameter **Valid Values** **Default Value** **Description**	Community view name Any object identifier defined in the View name parameter None This parameter allows you to select the view used by the community defined in the Community name parameter. This view determines the MIB objects that this community can access. If no view is specified, the community may access all objects known to the 6611's SNMP agent. This parameter should be answered if you decide to restrict a community from accessing the entire MIB managed by the 6611's SNMP agent.	

Controlling User IDs and Passwords

There are two classes of users:

- Controlling users

  Controlling users perform system administrative tasks on the 6611, such as running a system report or changing the configuration. Each 6611 is preconfigured with a controlling user ID and password of *ibm6611c*. IBM recommends that you change the password immediately after receiving the 6611.

- Viewing users

  Viewing users may view information about the 6611, but cannot perform any system administrative tasks. Each 6611 is preconfigured with a viewing user ID and password of *ibm6611v*. IBM recommends that you delete this user ID or change the password immediately after receiving the 6611.

A maximum of 10 system users can be logged into the 6611 at one time. For more information, refer to the *Operations and Problem Management*.

Use the worksheet in Table 6-6 to prepare to configure this function.

Table 6-6. Configuration Worksheet - Users of 6611 System Manager

Parameter Information		Your Value
Controlling Users List Parameters - Configured for each controlling user defined		
Parameter	Controlling user ID	
Valid Values	A string of up to 8 alphanumeric, lowercase characters (the string must begin with an alphabetic character)	
Default Value	None	
Description	This parameter defines a login user ID for a controlling user to access the 6611.	
Parameter	Password	
Valid Values	A string of up to 8 characters in length (any printable character can be used)	
Default Value	None	
Description	This parameter defines the password associated with the controlling user User ID parameter.	
Viewing users List Parameters - Configured for each viewing user defined		
Parameter	Viewing user ID	
Valid Values	A string of up to 8 alphanumeric, lowercase characters (the string must begin with an alphabetic character)	
Default Value	None	
Description	This parameter defines the login user ID for a viewing user to access the 6611.	
Parameter	Password	
Valid Values	A string of up to 8 characters in length (any printable character can be used)	
Default Value	None	
Description	This parameter defines the password associated with the viewing user User ID parameter.	

Specifying a Scheduled Configuration

This function allows you to build a configuration and to specify when it should be applied by the 6611. This function is designed to be used with configurations built by the Configuration Program using either a direct connection or a diskette. When you select **At a specific day and time**, the day and time specified are the local time on the 6611. When you specify a time delay for the configuration (the Apply configuration parameter is not set to **Immediately**) and the configuration is built from the System Manager, the configuration should be committed immediately. You cannot reject a pending (time delayed) configuration; however you can delete a pending configuration using the Communicate pulldown in the Configuration

Program. Refer to “Viewing the Communicate Pull-down” on page 3-17 for more information.

Use the worksheet in Table 6-7 to prepare to configure this function.

Table 6-7. Configuration Worksheet - Schedule Configuration

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Apply configuration Immediately, At next IML, At a specific time and day, At Upgrade Immediately This parameter indicates when to apply the configuration to the 6611.	
Parameter **Valid Values** **Default Value** **Description**	Source release MPNP V1R1.0, MPNP V1R1.1 or later None This parameter indicates the release of the MPNP before the upgrade is applied.	
Parameter **Valid Values** **Default Value** **Description**	Year 1991 to 2037 None This parameter indicates the year in which the configuration is applied.	
Parameter **Valid Values** **Default Value** **Description**	Month 1 to 12 None This parameter indicates the month of the year in which the configuration is applied.	
Parameter **Valid Values** **Default Value** **Description**	Day 1 to 31 None This parameter indicates the day of the month in which the configuration is applied.	
Parameter **Valid Values** **Default Value** **Description**	Hour 0 to 23 (0 to 11 is a.m., 12 to 23 is p.m.) None This parameter indicates the hour of the day in which the configuration is applied.	
Parameter **Valid Values** **Default Value** **Description**	Minute 0 to 59 None This parameter indicates the minute of the hour in which the configuration is applied.	

Enabling the Auto Configuration Roll Back Function

The auto configuration roll back function allows you to maintain IP connectivity if there is a problem with a newly applied configuration.

After you send a new configuration to a 6611, the 6611 attempts to contact the configured IP stations. If you enable the Test all IP stations before rolling back parameter, the 6611 will reboot if it cannot connect to all of the IP stations. If you disable the Test all IP stations before rolling back parameter, the 6611 will reboot if it cannot connect to any of the IP stations.

Use these worksheets to configure this function:

- Auto Configuration Roll Back on page 6-9
- IP Stations on page 6-9

Table 6-8. Configuration Worksheet - Auto Configuration Roll Back

Parameter Information		Your Value
Parameter **Valid Values** **Default Value** **Description**	Enable configuration auto roll back function Enable, Disable Disable The parameter enables or disables the configuration auto roll back function.	
Parameter **Valid Values** **Default Value** **Description**	Configuration for auto roll back 1 to 32 characters None This parameter contains the name of the configuration file on the 6611 that will be applied during a roll back.	
Parameter **Valid Values** **Default Value** **Description**	Delay before testing 60 to 32 400 seconds 300 This parameter allows you to set the time interval between applying a configuration and sending the first ICMP echo request packet to the first address specified in the IP station address parameter.	
Parameter **Valid Values** **Default Value** **Description**	Maximum test attempts 1 to 100 2 This parameter determines how many ICMP echo request packets will be sent out before activating the roll back function.	
Parameter **Valid Values** **Default Value** **Description**	Test frame timeout 1 to 120 seconds 5 This parameter determines how long the 6611 waits for an ICMP acknowledgement packet to arrive.	
Parameter **Valid Values** **Default Value** **Description**	Test interval 10 to 32 400 seconds 60 This parameter determines how long the 6611 waits between each test attempt.	
Parameter **Valid Values** **Default Value** **Description**	Test all IP stations before rolling back Enable, Disable Disable This parameter determines whether the 6611 must receive responses to its ICMP echo requests from at least one IP station or all IP stations. If you select **Enable**, the 6611 begins the roll back function if *any* IP station does not respond. If you select **Disable**, the 6611 begins the roll back function if *all* the IP stations do not respond.	

Table 6-9. Configuration Worksheet - IP Stations

Parameter Information		Your Value
IP Station List Parameter - Configure for each IP station defined		
Parameter **Valid Values** **Default Value** **Description**	IP station address Any valid IP address None This parameter contains the IP address for a roll back test station.	

Specifying Remote Hosts

The list of remote host names and addresses defines a list of host names matched with IP addresses to access remote IP nodes. These parameters are not required. You can define as many hosts as you want. The purpose of defining host names is to allow you to use a host name instead of an IP address when referring to a host node for remote access. Correlating the host name to an IP address using these parameters works only for the 6611 that is being configured. For consistency, this mapping must be done throughout the IP network for each device and host.

Use the worksheet in Table 6-10 to prepare to configure this function.

Table 6-10. Configuration Worksheet - Remote Hosts

Parameter Information	Your Value
Remote Host List Parameters - Configured for each remote host defined	
Parameter IP address of host **Valid Values** A valid IP address **Default Value** None **Description** This parameter specifies the IP address that has the symbolic name specified in the Host name parameter.	
Parameter Host name **Valid Values** A string of up to 31 alphanumeric characters (optionally, these characters can be separated by periods, underscores, or dashes) **Default Value** None **Description** This parameter specifies the symbolic name that is mapped to the IP address defined in the IP address of host parameter. parameter.	

Specifying Name Servers

A name server translates a host name into an IP address. The 6611 can either function as its own name server, or you can define remote name servers.

Use the worksheet in Table 6-11 to configure this function.

Table 6-11. Configuration Worksheet - Name Servers

Parameter Information	Your Value
Parameter Enable name resolution by remote name servers **Valid Values** Enable, Disable **Default Value** Disable **Description** This parameter enables or disables name resolution using one or more remote name servers running in the IP network connected to this 6611.	
Name server list parameter - Configured for each remote name server defined	
Parameter IP address of name server **Valid Values** A valid IP address **Default Value** None **Description** This parameter defines the IP address of a name server that is running in the IP network. It is answered once for each remote name server defined.	

Specifying Time Servers

A time server receives time service requests and returns the current time. When this function is enabled, the 6611 receives the current time by sending a time service request to the first time server in the list of IP addresses configured with the IP address of remote time server parameter. If a remote time server cannot provide time service, the 6611 sends the request to the next remote time server in the list. The 6611 supports the Time Synchronization Protocol (TSP).

Use the worksheet in Time Servers on page 6-11 to configure this function.

Table 6-12. Configuration Worksheet - Time Servers

Parameter Information		Your Value
Parameter	Enable time service by remote time servers	
Valid Values	Enable, Disable	
Default Value	Disable	
Description	This parameter enables or disables remote time service by a remote time server in the IP network.	
Time Server List Parameter - Configured for each time server defined		
Parameter	IP address of remote time server	
Valid Values	A valid IP address	
Default Value	None	
Description	This parameter defines the IP address of a remote time server that is running in the IP network.	

Listing Configuration Hosts for this 6611

The following parameters configure the IP addresses of remote hosts in the IP network that can perform remote configuration to this 6611. By default, all hosts can perform configuration. There is no limit to the number of hosts that can be configured.

Use the worksheet in Table 6-13 to prepare to configure this function.

Table 6-13 (Page 1 of 2). Configuration Worksheet - Configuration Hosts

Parameter Information		Your Value
Parameter	Hosts that can perform configuration functions on this router	
Valid Values	All hosts, List of specific hosts	
Default Value	All hosts	
Description	This parameter defines which hosts (if any) in the IP network are able to perform remote configuration functions with the 6611 using the Configuration Program.	
Configuration Hosts List Parameters - Configured for each configuration host defined		
Parameter	Host IP address	
Valid Values	A valid IP address	
Default Value	None	
Description	This parameter defines the IP address of a remote host that can: • Access the 6611 via the Configuration Program • Perform updates to the active configuration on the 6611 This parameter has no effect on performing an update to the configuration from a diskette or when using the System Manager.	

Table 6-13 (Page 2 of 2). Configuration Worksheet - Configuration Hosts

Parameter Information		Your Value
Parameter	Address mask	
Valid Values	A four-octet dotted number where each octet is in the range of 0 to 255 (decimal)	
Default Value	255.255.255.255	
Description	This parameter defines the address mask of the IP address of the configuration host given in the IP address of configuration host parameter. Each bit in the mask that is a zero is ignored in the IP address. Use this parameter to allow all hosts on one particular network or subnetwork to perform remote configuration on this 6611.	

Chapter 7. Using System Manager to Receive Configuration Files from the Configuration Program

This chapter provides a brief overview of the IBM Multiprotocol Network Program System Manager (System Manager) and includes instructions for using the System Manager to import and export configuration files.

What Is the System Manager?

The System Manager is a menu-driven, interactive user interface that is designed to perform change management, network management, problem determination, and configuration. It can be accessed locally or remotely by attaching an ASCII terminal to the 6611 or by issuing a remote network access command: for example, the **telnet** command can be used to access the 6611. The System Manager configuration is accessed by selecting **Adapter and Protocol Configuration** from the main menu.

The System Manager provides:

- The ability to perform minimal configuration to attach the 6611 to the network.
- A user interface to change configuration parameters while directly attached to the 6611. However, the System Manager configuration facility provides minimal error checking, which includes no dependency checking on related parameters.

The System Manager also includes a configuration facility that enables you to perform configuration tasks on the 6611. The System Manager configuration facility has three roles:

1. It can be used to update configuration parameters, when the Configuration Program is not available.
2. It is involved in the transfer of the binary configuration file from the Configuration Program to the 6611.
3. It is used to view and transfer the configuration information text files. Only a controlling user can perform configuration tasks from the System Manager.

You must be a controlling user to use the System Manager for most of these configuration tasks.

Initial Configuration Using a Diskette

The Configuration Program is used to configure the 6611 initially:

1. Create the configuration file with the Configuration Program and place it on a diskette. See Chapter 3 on page 3-1 for instructions about using the Configuration Program.
2. Insert the diskette in the 6611 diskette drive.
3. Set the key mode switch on the front window in the Normal position and turn the power switch to **On**.

The configuration file is read and the new parameters are used as the current configuration.

Note: To prevent subsequent configurations from this diskette or accidental overwriting of the configuration data, remove the diskette from the diskette drive.

Initial Configuration without Using a Diskette

The System Manager can be used to configure the 6611 minimally so that it can be initially configured from the Configuration Program without using a diskette. There are three methods to transfer the configuration file from the Configuration Program to the 6611 without using a diskette.

1. Direct IP Connection

   This method is available using a RISC System/6000 workstation only to perform configuration.

2. Modem Attachment

   - A modem must be attached to the configuration workstation and to an 6611 on the network.
   - The configuration workstation must also have a communication package that supports call-out and the Xmodem Protocol.
   - This method could be used with a PS/2 configuration workstation that has a supported communication package.

3. FTP

   - The configuration workstation must be attached to the 6611 through the IP network.
   - This method could be used with a PS/2 configuration workstation that has TCP/IP installed.

One of these methods must be available, if you want to perform initial configuration on the 6611 from the Configuration Program without using a diskette.

Direct IP Connection

Direct IP connection is available only when using a RISC System/6000 configuration workstation attached to the same IP network as the 6611 needing initial configuration. Perform the following steps to configure the 6611 initially over the IP network.

1. The 6611 must be minimally configured for IP. See *Operations and Problem Management* for details about minimal configuration.
2. See "Transporting the Configuration File to the 6611" on page 3-29 for the details about sending the configuration file from the Configuration Program over the direct connection.

Modem Attachment

If you are using the modem-attachment method to configure the 6611 initially and the modem is attached to the 6611 needing to be configured, minimal configuration is not necessary. Perform the following steps to configure the 6611 initially using the modem connection to send the configuration file.

1. Attach a 2400-bps modem to the EIA 232 S2 serial port on the 6611 (labelled S2 on the Model 120 and the Model 170, and labelled Serial 2 on the Model

140). The S2 serial port is initially configured for 2400-bps modem support. See *Operations and Problem Management* for details about using a modem.

2. From the configuration station, establish the modem connection to the 6611 using the directions supplied with the communication package.

3. Log in to the 6611 using the default controlling user ID and password.

   Default userid: ibm6611c

   Default password: ibm6611c

4. Prepare the 6611 to receive the configuration file and use it as the new configuration when it has been received.

   a. Select **Configuration** from the System Manager main menu.

   b. Select **Receive and Apply Configuration** from the Configuration menu.

   c. Select **modem** as the import method on the Import method selector screen.

   See *Operations and Problem Management* for further details about using the Xmodem protocol to transfer files.

5. Determine the location and name of the configuration file at the configuration workstation. You must determine in which subdirectory the .cfg file has been placed. Instruct the configuration workstation to send the configuration file.

If the modem is attached to a different 6611 on the IP network than the 6611 needing to be initially configured, the 6611 has to be minimally configured for an IP connection. Perform the following steps to configure the 6611 initially using the modem connection to send the configuration file.

1. Minimally configure the 6611 using the directions provided in *Operations and Problem Management*.

2. From the configuration workstation, establish a modem connection to the 6611 with a modem that is on the same IP network as the 6611 that you minimally configured. See *Operations and Problem Management* for details about using a modem. Use the directions supplied with the communication package on the configuration workstation for modem connection.

3. Log in to the 6611 with the modem from the configuration workstation. Establish an rlogin session from the 6611 with the modem to the 6611 needing to be configured. See *Operations and Problem Management* for details about using rlogin.

4. Prepare the 6611 that needs to be configured to receive the configuration file and use it as the new configuration when received.

   a. Select **Configuration** from the System Manager main menu.

   b. Select **Receive and Apply Configuration** from the next menu.

   c. Select **modem** as the receive method on the Import method selector screen.

   See *Operations and Problem Management* for further details about using the Xmodem protocol to transfer files.

5. Determine the location and name of the configuration file at the configuration workstation. You must determine in which subdirectory the file has been placed. It will be marked as a **.cfg** file. Instruct the configuration workstation to send the configuration file.

FTP Transfer Method

The configuration file may be sent using FTP, if the configuration workstation is on the IP network and it supports FTP. Use the following steps to configure the 6611 initially using FTP to transfer the file.

1. Minimally configure the 6611 using the directions provided in *Operations and Problem Management*.
2. Know the location and file name of the configuration file on the configuration station. In this procedure, the configuration file name is *config*.
3. From the directory that has the configuration file in the configuration station, use the following scenario to place the configuration file in the transfer directory of the 6611 needing to be configured. What you are expected to input from the configuration station is provided under **Type in**. What you should expect to see displayed on the screen is provided under **Output displayed**.

   Type in:

   ```
   ftp hostname
   ```

   where hostname is the host name of the 6611 needing to be configured. The IP address can be used in place of the host name to identify the 6611 to which the configuration files is sent.

   Output displayed:

   ```
   Connected to hostname.domainname
   220 hostname FTP server (Version 4.1 Date) ready.
   Name (hostname):
   ```

   Type in:

   ```
   6611_userid
   ```

   Output displayed:

   ```
   331 Password required for 6611_userid.
   Password:
   ```

   Type in: (Enter the password. It will not be displayed.)

   Output displayed:

   ```
   230 User 6611_userid logged in.
   /transfer is read-write and /static is read-only.
   ftp>
   ```

   Type in:

   ```
   cd /transfer
   ```

   Output displayed:

   ```
   250 CWD command successful.
   ftp>
   ```

   Type in:

   ```
   bi
   ```

   Output displayed:

   ```
   200 Type set to I.
   ftp>
   ```

   Type in:

```
put "file_name"
```

Output displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for filename1.
226 Transfer complete.
local: "file_name" remote: "file_name"
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)
ftp>
```

Type in:

```
quit
```

Output displayed:

```
221 Goodbye.
```

Note: The numbers associated with the FTP messages are standard message numbers for this protocol. They have no significance other than to identify the message.

4. The configuration file is now in the transfer directory of the 6611. Receive the file and use it as the new configuration:
   a. Select **Configuration** from the System Manager main menu.
   b. Select **Receive and Apply Configuration** from the next menu.
   c. Select **transfer directory** as the import method on the resulting selector screen.
   d. A dialog screen appears requesting you to enter the name of the binary configuration file. The default configuration file name is *config*. If this is not the name of the configuration file that you are importing from the transfer directory, press **F4 (Esc+4)** to list the files in the transfer directory and select the configuration file from the list. Optionally, you can type the file name in the entry field. Press **Enter** after you have selected or typed the name.

See *Operations and Problem Management* for further details about using FTP to transfer files.

Appendixes

Appendix A. Multiprotocol Configuration Examples

Sample Network Running IPX, IP, and DLSw

Figure A-1 illustrates a sample network where IP and IPX routing and data link switching are enabled between two routers (6611 A and 6611 B). Routers 6611 A and 6611 B are configured to route IPX and source route bridge SNA and NetBIOS across the frame relay network.

This network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP, IPX, DLSw, SNA, and NetBIOS over frame relay
  - A token-ring port running SNA and NetBIOS
  - An Ethernet port running IPX
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP, IPX, DLSw, SNA, and NetBIOS over frame relay
  - A token-ring port running SNA and NetBIOS
  - An Ethernet port running IPX

  The following information is shown in Figure A-1:

  - IP addresses
  - Slot and port numbers, abbreviated s*x* p*y*
  - IPX network numbers
  - Ring numbers and ring speeds
  - MAC addresses
  - DLCI numbers

  Note: The configuration of the IP protocol on the token-ring and Ethernet ports is shown to enable you to test your connectivity using the IP ping protocol. IP is *not* required to route IPX, nor is it required on the token-ring ports for DLSw or source route bridging.

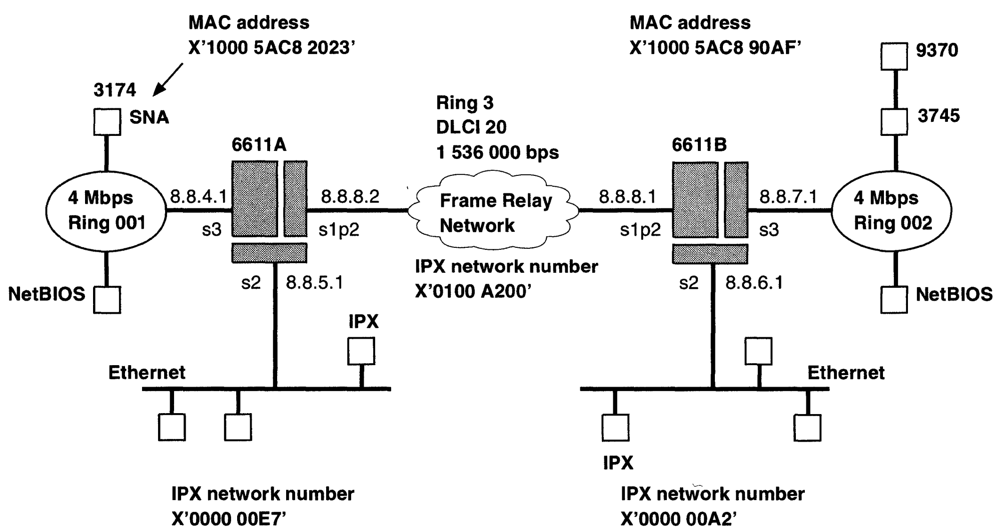


Figure A-1. Sample Network for IPX, IP, and DLSw

This sample network shows the configuration for:

- IPX routing
- Data link switching of SNA and NetBIOS traffic

Summary of All Customized Parameters in Sample

Use the following tables as a reference for Figure A-1 on page A-1. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Serial Ports and Protocols Running on Them

Table A-1. Serial Port Parameter Configured

Parameter	**6611 A Slot 1 Port 2 Value**	**6611 B Slot 1 Port 2 Value**
Data link protocol	Frame Relay	Frame Relay

Table A-2. Serial Port - Physical Interface Parameters Configured

Parameter	**6611 A Slot 1 Port 2 Value**	**6611 B Slot 1 Port 2 Value**
Enable physical interface on this port	Enable	Enable
Interface cable	EIA 422 or X.21	EIA 422 or X.21
Cylink serial number	None	None
Transmit clock source	DTE	DTE
Serial line speed	1536000	1536000
Data encoding	NRZI	NRZI
Locally administered MAC address	40	50
Enable port for transmission group	NA	NA
Transmission group name	NA	NA

Table A-3. Serial Port - Frame-Relay Parameters Configured

Parameter	**6611 A Slot 1 Port 2 Value**	**6611 B Slot 1 Port 2 Value**
Enable Frame Relay on this port	Enable	Enable
Polling interval	10	10
Full inquiry interval	6	6
LMI option	ANSI T1.617 Annex D	ANSI T1.617 Annex D
User InARP to resolve remote protocol addresses	Enable	Enable
DLCIs assigned to this port	20	20

Table A-4. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.8.2	8.8.8.1
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Enable ICMP address mask requests	Enable	Enable
Directed broadcast	Disable	Disable
Point-to-point only	Disable	Disable
Assignment for discovered DLCIs	Mesh	Mesh
IP Priority	NA	NA
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Table A-5. Serial Port - IP Destination per DLCI Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
DLCI number	20	20
Destination IP address	8.8.8.1	8.8.8.2

Table A-6. Serial Port - IPX over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable IPX routing on this port	Enable	Enable
IPX network number	E7	A2
Inbound Port Filters	Disable	Disable

Table A-7. Serial Port - IPX Destination per DLCI Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Destination IPX address	A2	E7
DLCI number	20	20

Table A-8. Serial Port - Bridge over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value	6611 B Slot 1 Port 2 Value
Enable Source Route Bridging on this port	Enable	Enable
Spanning tree mode	Automatic	Automatic
Path cost	0	0
Port priority for Translational Bridging	80	80
Port state	NA	NA
Max. transmission unit (octets)	2052	2052
Ring Number to DLCI Detail List Parameters		
Ring number	3	3
DLCI number	20	20

Token-Ring Ports and Protocols Running on Them

Table A-9. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local

Table A-10. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable Source Route Bridging on this port	Enable	Enable
Spanning tree mode	Automatic	Automatic
Path cost	0	0
Port priority for Translational Bridging	80	80
Port state	NA	NA
Ring number	1	2
Max. transmission unit (octets)	2052	2052

Table A-11. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.4.1	8.8.7.1
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Table A-12. Token-Ring Port - SNA Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Enable SNA frame forwarding on this port	Enable	Enable
SAP value	00, 04	00, 04

Table A-13. Token-Ring Port - NetBIOS Parameters Configured

Parameter	6611 A Slot 3 Value	6611 B Slot 3 Value
Forward on this port		
NetBIOS frame	Enable	Enable
NetBIOS datagram and datagram broadcast messages	Enable	Enable

Ethernet Ports and the Protocols Running on Them

Table A-14. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable physical interface on this port	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
Enable additional multicast addresses	Disable	Disable
Multicast MAC address	None	None

Table A-15. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IP routing on this port	Enable	Enable
IP address	8.8.5.1	8.8.6.1
Subnet mask	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Table A-16. Ethernet Port - IPX Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value
Enable IPX routing on this port	Enable	Enable
IPX network number	E7	A2
Encapsulation method	Ethernet 802.3 LLC	Ethernet 802.3 LLC
Tick override	Disable	Disable
Tick value	NA	NA
Control RIP and SAP broadcasting		
SAP update interval	1	1
SAP age multiplier	4	4
RIP update interval	1	1
RIP age multiplier	4	4
Inbound Port Filters	Disable	Disable

Node-Level Parameters Configured

Table A-17. Node Level - Source Route Bridging Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Source Route Bridging	Enable	Enable
Bridge number	10	10
Enable LAN Bridging Protocol	Enable	Enable
Designated ring number	1	2
Spanning tree parameters		
Bridge priority	8000	8000
Hello time	2	2
Forward delay time	15	15
Max age	20	20

Table A-18. Node Level - DLSw Parameters Configured

Parameter	6611 A Value	6611 B Value
Protocols forwarded by DLSw		
SNA	Enable	Enable
NetBIOS	Enable	Enable
SNA transmission bias	0	0
Maximum NetBIOS frame size	2052	2052
DLSw parameters		
Virtual ring segment number	FAB	FAC
Destination cache timeout	8	8
Default DLSw IP address for this 6611	8.8.8.2	8.8.8.1

Table A-19. Node Level - DLSw Partners Parameters Configured

Parameter	6611 A Value	6611 B Value
Accept connections from specific 6611s only	Disable	Disable
IP address of remote 6611 router	8.8.8.1	8.8.8.2

Table A-20. Node Level - SNA DLSw Parameters Configured

Parameter	6611 A Value	6611 B Value
IP address of destination router	8.8.8.1	8.8.8.2
Destination MAC address	10005A100002	10007CE00010
Source Frame Filters	Disable	Disable
Destination Frame Filters	Disable	Disable

Table A-21. Node Level - NetBIOS Parameters Configured

Parameter	6611 A Value	6611 B Value
Destination name	6611 B	6611 A
IP address of destination router	8.8.8.1	8.8.8.2
Source Name Filters	Disable	Disable
Destination Name Filters	Disable	Disable

Table A-22. Node Level - IPX Routing Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable IPX router	Enable	Enable
SAP Filters	Disable	Disable
RIP Router Filters	Disable	Disable
Inbound RIP Filters	Disable	Disable
Outbound RIP Filters	Disable	Disable

Single Star Frame-Relay Configuration

Figure A-2 on page A-9 illustrates four 6611s (6611 A, 6611 B, 6611 C, and 6611 D) in a partially meshed frame-relay network. This configuration is also known as a single star topology.

To enable any-to-any connectivity between the four 6611s:

- Configure point-to-point connections between each router pair.

  6611 A performs intermediate routing and enables 6611 B, 6611 C, and 6611 D to communicate with each other. DLCIs are discovered using ANSI T1.1617 Annex D for the LMI option; if your network does not support ANSI T1.167, statically configure DLCIs on the Frame Relay window.

- At the node level, define any 6611 with which this 6611 must communicate and to which this 6611 is not connected by a point-to-point link as a RIP source router. To support RIP broadcast, the network must be fully meshed, or RIP source routers must be defined.

This sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 C, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 D, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP

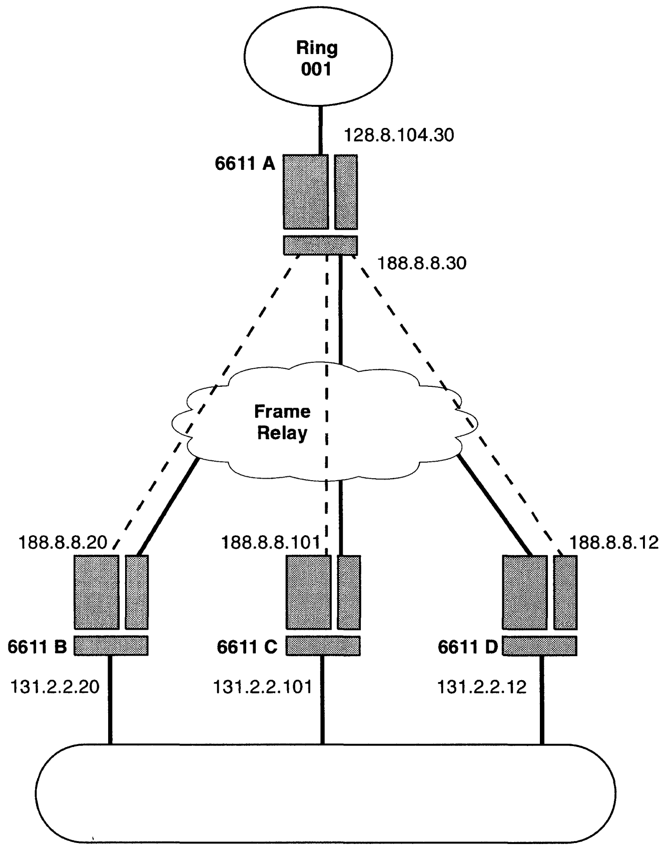


Figure A-2. Sample Network for Single Star Frame Relay

The sample network, which is running with a subnet mask of 255.255.255.0, shows the configuration of:

- Single star frame relay with any-to-any connectivity
- RIP routing
- Serial and token-ring ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure A-2. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

6611 A Serial Port and the Protocols Running on It

Table A-23. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2
Data link protocol	Frame relay	Frame relay	Frame relay	Frame relay

Table A-24. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2
Enable physical interface on this port	Enable	Enable	Enable	Enable
Interface cable	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232
Cylink serial number	None	None	None	None
Transmit clock source	DTE	DTE	DTE	DTE
Serial line speed	19200	19200	19200	19200
Data encoding	NRZ	NRZ	NRZ	NRZ
Locally administered MAC address	None	None	None	None
Enable port for transmission group	NA	NA	NA	NA
Transmission group name	NA	NA	NA	NA

Table A-25. Serial Port - Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2
Enable Frame Relay on this port	Enable	Enable	Enable	Enable
Polling interval	10	10	10	10
Full inquiry interval	6	6	6	6
LMI option	ANSI T1.617 Annex D	ANSI T1.617 Annex D	ANSI T1.617 Annex D	ANSI T1.617 Annex D
Use InARP to resolve remote protocol addresses	Enable	Enable	Enable	Enable
DLCIs assigned to this port	None	None	None	None

Note: DLCIs are not assigned on the Frame Relay window because they are discovered using ANSI T1.1617 Annex D for the LMI option.

Table A-26. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2
Enable IP routing on this port	Enable	Enable	Enable	Enable
IP address	188.8.8.30	188.8.8.20	188.8.8.101	188.8.8.12
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500	1500	1500
Enable ICMP address mask requests	Enable	Enable	Enable	Enable
Directed broadcast	Disable	Disable	Disable	Disable
Point-to-point only	Enable	Enable	Enable	Enable
Assignment for discovered DLCIs	Point-to-point	Point-to-point	Point-to-point	Point-to-point
IP Priority	Disable	Disable	Disable	Disable
Inbound Port Filters	Disable	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable	Disable

Table A-27. Serial Port - 6611 A IP Point-to-Point Addresses Parameters Configured

Parameter	6611 A Value 1	6611 A Value 2	6611 A Value 3
IP point-to-point destination	188.8.8.20	188.8.8.101	188.8.8.12
DLCI number	None	None	None

Table A-28. Serial Port - IP Point-to-Point Addresses Parameters Configured

Parameter	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2
IP point-to-point destination	188.8.8.30	188.8.8.30	188.8.8.30
DLCI number	None	None	None

Token-Ring Ports and Protocols Running on Them

Table A-29. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value	6611 C Slot 2 Value	6611 D Slot 2 Value
Enable physical interface on this port	Enable	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA	NA
MAC address format	NA	NA	NA	NA
Token ring data rate	4 Mbps	4 Mbps	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local	Non-local	Non-local

Table A-30. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 2 Value	6611 C Slot 2 Value	6611 D Slot 2 Value
Enable IP routing on this port	Enable	Enable	Enable	Enable
IP address	128.8.104.30	131.2.2.20	131.2.2.101	131.2.2.12
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492	1492	1492
Enable ICMP address mask requests	Enable	Enable	Enable	Enable
Directed broadcast	Disable	Disable	Disable	Disable
Inbound Port Filters	Disable	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable	Disable

Node-Level Parameters Configured

Table A-31. Node Level - RIP Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value
Enable Routing Information Protocol (RIP)	Enable	Enable	Enable	Enable
Broadcast	Disable	Disable	Disable	Disable
Zero reserved fields	Enable	Enable	Enable	Enable
Route preference	100	100	100	100

Table A-32. Node Level - RIP Interface - Detail Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value
Local IP interface	All	All	All	All
IP address of local interface	NA	NA	NA	NA
RIP interface settings				
Version	Version 1	Version 1	Version 1	Version 1
Broadcast mode	NA	NA	NA	NA
Metric in	1	1	1	1
Metric out	0	0	0	0
Listen for RIP updates	Enable	Enable	Enable	Enable
Send RIP updates	Enable	Enable	Enable	Enable

Table A-33. Node Level - RIP Source Routers Configured

Parameter	6611 B Value	6611 C Value	6611 D Value
IP address of source router	188.8.8.12 188.8.8.101	188.8.8.12 188.8.8.20	188.8.8.20 188.8.8.101

Partially Meshed Frame Relay with Point-to-Point Links Configured

Figure A-3 on page A-14 illustrates five 6611s (6611 A, 6611 B, 6611 C, 6611 D, and 6611 E) in a partially meshed frame-relay physical network. The logical network has a hierarchical topology with redundancy added through the addition of 6611 E on ring 001. 6611 E provides a back up for 6611 A by offering an alternate path to ring 001.

To enable any-to-any connectivity between the five 6611s you could configure:

- Point-to-point links for each PVC
- A combination of point-to-point and mesh links (see "Partially Meshed Frame Relay with Point-to-Point and Mesh Links Configured" on page A-18)

This network illustrated in Figure A-3 on page A-14 is configured with point-to-point links only.

At the node level, you also need to define any 6611 with which this 6611 must communicate and to which this 6611 is not connected by a point-to-point link as a RIP source router. To support RIP broadcast, the network must be fully meshed, or RIP source routers must be defined.

This sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 C, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 D, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 E, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP

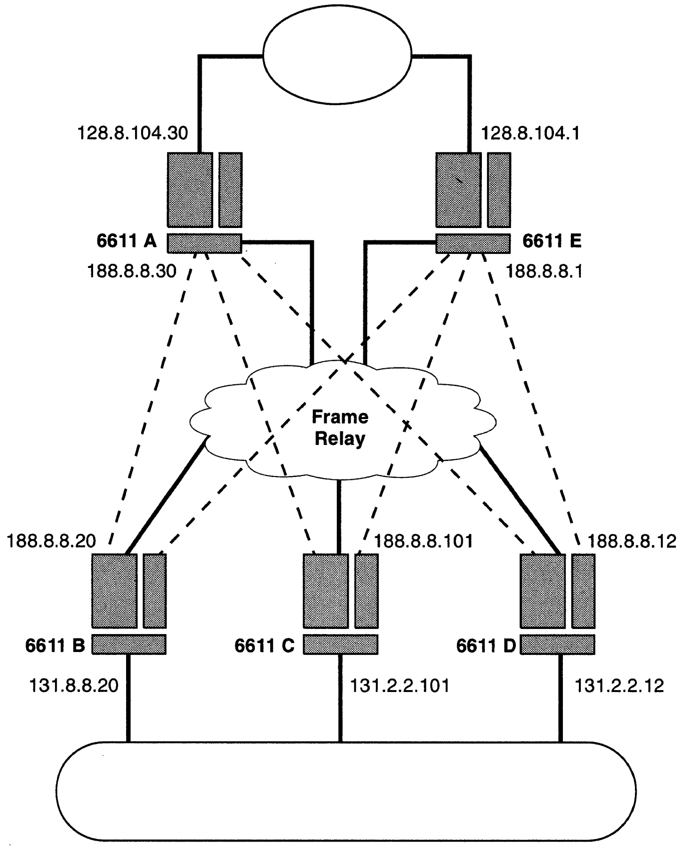


Figure A-3. Sample Network for Partially Meshed Frame-Relay Network - Point-to-Point Links Only

The sample network, which is running with a subnet mask of 255.255.255.0, shows the configuration of:

- Partially meshed frame relay with any-to-any connectivity
- RIP routing
- Serial and token-ring ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure A-3. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

6611 A Serial Port and the Protocols Running on It

Table A-34. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2	6611 E Slot 1 Port 2
Data link protocol	Frame relay	Frame relay	Frame relay	Frame relay	Frame relay

Table A-35. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2	6611 E Slot 1 Port 2
Enable physical interface on this port	Enable	Enable	Enable	Enable	Enable
Interface cable	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232
Cylink serial number	None	None	None	None	None
Transmit clock source	DTE	DTE	DTE	DTE	NA
Serial line speed	19200	19200	19200	19200	19200
Data encoding	NRZ	NRZ	NRZ	NRZ	NRZ
Locally administered MAC address	None	None	None	None	None
Enable port for transmission group	NA	NA	NA	NA	NA
Transmission group name	NA	NA	NA	NA	NA

Table A-36. Serial Port - Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2	6611 E Slot 1 Port 2
Enable Frame Relay on this port	Enable	Enable	Enable	Enable	Enable
Polling interval	10	10	10	10	10
Full inquiry interval	6	6	6	6	6
LMI option	ANSI T1.617 Annex D	ANSI T1.617 Annex D	ANSI T1.617 Annex D	ANSI T1.617 Annex D	ANSI T1.617 Annex D
Use InARP to resolve remote protocol addresses	Enable	Enable	Enable	Enable	Enable
DLCIs assigned to this port	None	None	None	None	None

Note: DLCIs are not assigned on the Frame Relay window because they are discovered using ANSI T1.1617 Annex D for the LMI option.

Table A-37. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2	6611 E Slot 1 Port 2
Enable IP routing on this port	Enable	Enable	Enable	Enable	Enable
IP address	188.8.8.30	188.8.8.20	188.8.8.101	188.8.8.12	188.8.8.1
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500	1500	1500	1500
Enable ICMP address mask requests	Enable	Enable	Enable	Enable	Enable
Directed broadcast	Disable	Disable	Disable	Disable	Disable
Point-to-point only	Enable	Enable	Enable	Enable	Enable
Assignment for discovered DLCIs	NA	NA	NA	NA	NA
IP Priority	NA	NA	NA	NA	NA
Inbound Port Filters	Disable	Disable	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable	Disable	Disable

Table A-38. Serial Port - 6611 A IP Point-to-Point Addresses Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value 1	6611 A Slot 1 Port 2 Value 2	6611 A Slot 1 Port 2 Value 3
IP point-to-point destination	188.8.8.20	188.8.8.12	188.8.8.101
DLCI number	None	None	None

Table A-39. Serial Port - 6611 B and D IP Point-to-Point Addresses Parameters Configured

Parameter	6611 B Slot 1 Port 2 Value 1	6611 B Slot 1 Port 2 Value 2	6611 D Slot 1 Port 2 Value 1	6611 D Slot 1 Port 2 Value 2
IP point-to-point destination	188.8.8.1	188.8.8.30	188.8.8.1	188.8.8.30
DLCI number	None	None	None	None

Table A-40. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2	6611 B Slot 2	6611 C Slot 2	6611 D Slot 2	6611 E Slot 2
Enable physical interface on this port	Enable	Enable	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA	NA	NA
MAC address format	NA	NA	NA	NA	NA
Token ring data rate	4 Mbps	4 Mbps	4 Mbps	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local	Non-local	Non-local	Non-local

Table A-41. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2	6611 B Slot 2	6611 C Slot 2	6611 D Slot 2	6611 E Slot 2
Enable IP routing on this port	Enable	Enable	Enable	Enable	Enable
IP address	128.8.104.30	131.2.2.20	131.2.2.101	131.2.2.12	128.8.104.1
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492	1492	1492	1492
Enable ICMP address mask requests	Enable	Enable	Enable	Enable	Enable
Directed broadcast	Disable	Disable	Disable	Disable	Disable
Inbound Port Filters	Disable	Disable	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable	Disable	Disable

Node-Level Parameters Configured

Table A-42. Node Level - RIP Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value	6611 E Value
Enable Routing Information Protocol (RIP)	Enable	Enable	Enable	Enable	Enable
Broadcast	Enable	Enable	Enable	Enable	Enable
Zero reserved fields	Enable	Enable	Enable	Enable	Enable
Route preference	100	100	100	100	100

Table A-43. Node Level - RIP Interface - Detail Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value	6611 E Value
Local IP interface	All	All	All	All	All
IP address of local interface	NA	NA	NA	NA	NA
RIP interface settings					
Version	Version 1	Version 1	Version 1	Version 1	Version 1
Broadcast mode	NA	NA	NA	NA	NA
Metric in	1	1	1	1	1
Metric out	0	0	0	0	0
Listen for RIP updates	Enable	Enable	Enable	Enable	Enable
Send RIP updates	Enable	Enable	Enable	Enable	Enable

Table A-44. Node Level - RIP Source Router Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value	6611 E Value
IP address of source router	188.8.8.1	188.8.8.101 188.8.8.12	188.8.8.12 188.8.8.20	188.8.8.20 188.8.8.101	188.8.8.30

Partially Meshed Frame Relay with Point-to-Point and Mesh Links Configured

Figure A-4 on page A-19 illustrates five 6611s (6611 A, 6611 B, 6611 C, 6611 D, and 6611 E) in a partially meshed frame-relay physical network. The logical network has a hierarchical topology with redundancy added through the addition of 6611 E on ring 001. 6611 E provides a back up for 6611 A by offering an alternate path to ring 001.

To enable any-to-any connectivity between the five 6611s you could configure:

- Point-to-point links for each PVC (see "Partially Meshed Frame Relay with Point-to-Point Links Configured" on page A-13)
- A combination of point-to-point and mesh links

This network illustrated in Figure A-4 on page A-19 is configured as a combination of point-to-point and mesh links. This configuration can be used when migrating 6611s to a new code level. The 6611s with the new code level can be configured as point-to-point links while the remainder of the 6611s can remains configured as a mesh network.

When configuring a combination of point-to-point and mesh links on the same port, you must do the following:

- On the Frame Relay window, enter the DLCIs used by the point-to-point links. If the frame-relay provider does not support LMI, all DLCIs must be entered. For the purposes of this example, the DLCIs used by the mesh links are discovered by ANSI T1.1617 Annex D and are not entered.
- On the IP over Frame Relay window, set the Assignment for discovered DLCIs parameter to **Mesh**.
- Statically configure the logical mapping between the destination IP address and corresponding DLCI number for each IP Point-to-Point destination.

At the node level, you also need to define any 6611 with which this 6611 must communicate and to which this 6611 is not connected by a point-to-point link as a RIP source router. To support RIP broadcast, the network must be fully meshed, or RIP source routers must be defined.

This sample network includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 B, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 C, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP
- 6611 D, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP

- 6611 E, which has the following port types and protocols running:
  - A serial port running IP and RIP over frame relay
  - A token-ring port running IP and RIP

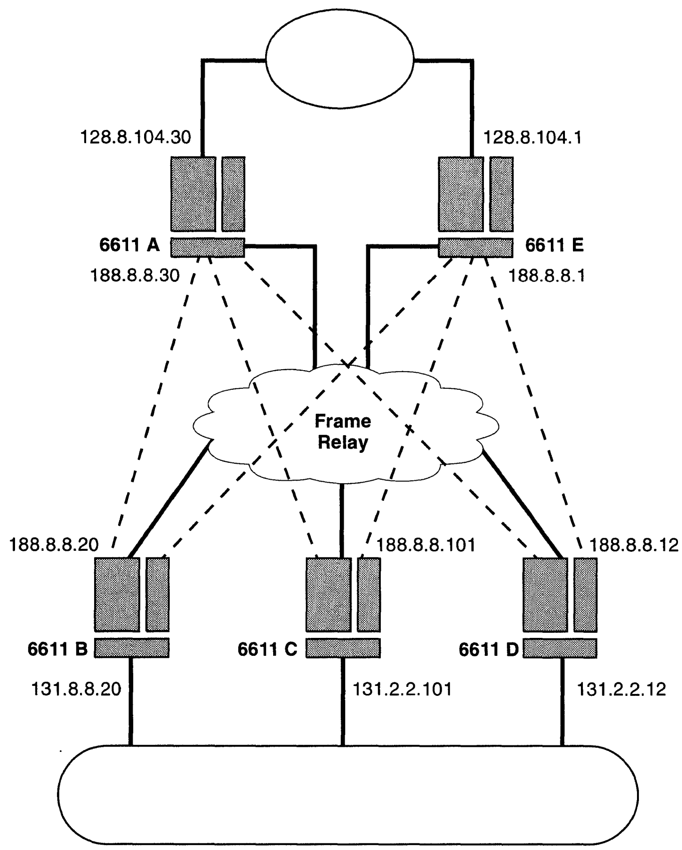


Figure A-4. Sample Network for Partially Meshed Frame-Relay Network - Point-to-Point and Mesh Links

The sample network, which is running with a subnet mask of 255.255.255.0, shows the configuration of:

- Partially meshed frame relay with any-to-any connectivity
- RIP routing
- Serial and token-ring ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure A-4. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

6611 A Serial Port and the Protocols Running on It

Table A-45. Serial Port Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2	6611 E Slot 1 Port 2
Data link protocol	Frame relay	Frame relay	Frame relay	Frame relay	Frame relay

Table A-46. Serial Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2	6611 E Slot 1 Port 2
Enable physical interface on this port	Enable	Enable	Enable	Enable	Enable
Interface cable	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232	V.35, V.36, or EIA 232
Cylink serial number	None	None	None	None	None
Transmit clock source	DTE	DTE	DTE	DTE	NA
Serial line speed	19200	19200	19200	19200	19200
Data encoding	NRZ	NRZ	NRZ	NRZ	NRZ
Locally administered MAC address	None	None	None	None	None
Enable port for transmission group	NA	NA	NA	NA	NA
Transmission group name	NA	NA	NA	NA	NA

Table A-47. Serial Port - Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2	6611 E Slot 1 Port 2
Enable Frame Relay on this port	Enable	Enable	Enable	Enable	Enable
Polling interval	10	10	10	10	10
Full inquiry interval	6	6	6	6	6
LMI option	ANSI T1.617 Annex D	ANSI T1.617 Annex D	ANSI T1.617 Annex D	ANSI T1.617 Annex D	ANSI T1.617 Annex D
Use InARP to resolve remote protocol addresses	Enable	Enable	Enable	Enable	Enable
DLCIs assigned to this port	19,21[1]	None	None	None	51, 53[1]

Note: [1] When configuring a combination of point-to-point and mesh links on a port, you must enter the DLCIs used by the point-to-point links. If the frame-relay provider does not support LMI, all DLCIs must be entered. For the purposes of this example, the DLCIs used by the mesh links are discovered by ANSI T1.1617 Annex D and are not entered.

Table A-48. Serial Port - IP over Frame-Relay Parameters Configured

Parameter	6611 A Slot 1 Port 2	6611 B Slot 1 Port 2	6611 C Slot 1 Port 2	6611 D Slot 1 Port 2	6611 E Slot 1 Port 2
Enable IP routing on this port	Enable	Enable	Enable	Enable	Enable
IP address	188.8.8.30	188.8.8.20	188.8.8.101	188.8.8.12	188.8.8.1
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1500	1500	1500	1500	1500
Enable ICMP address mask requests	Enable	Enable	Enable	Enable	Enable
Directed broadcast	Disable	Disable	Disable	Disable	Disable
Point-to-point only	Disable	Enable	Disable	Enable	Disable
Assignment for discovered DLCIs	Mesh	NA	Mesh	NA	Mesh
IP Priority	NA	NA	NA	NA	NA
Inbound Port Filters	Disable	Disable	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable	Disable	Disable

Table A-49. Serial Port - 6611 A and E IP Point-to-Point Addresses Parameters Configured

Parameter	6611 A Slot 1 Port 2 Value 1	6611 A Slot 1 Port 2 Value 2	6611 E Slot 1 Port 2 Value 1	6611 E Slot 1 Port 2 Value 2
IP point-to-point destination	188.8.8.20	188.8.8.12	188.8.8.20	188.8.8.12
DLCI number	19	21	51	53

Note: When configuring a combination of point-to-point and mesh links on the same port, set the Assignment for discovered DLCIs parameter to **Mesh** and statically configure the logical mapping between the the destination IP address and corresponding DLCI number for each IP Point-to-Point destination.

Table A-50. Serial Port - 6611 B and D IP Point-to-Point Addresses Parameters Configured

Parameter	6611 B Slot 1 Port 2 Value 1	6611 B Slot 1 Port 2 Value 2	6611 D Slot 1 Port 2 Value 1	6611 D Slot 1 Port 2 Value 2
IP point-to-point destination	188.8.8.1	188.8.8.30	188.8.8.1	188.8.8.30
DLCI number	None	None	None	None

Token-Ring Ports and Protocols Running on Them

Table A-51. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 2	6611 B Slot 2	6611 C Slot 2	6611 D Slot 2	6611 E Slot 2
Enable physical interface on this port	Enable	Enable	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA	NA	NA
MAC address format	NA	NA	NA	NA	NA
Token ring data rate	4 Mbps	4 Mbps	4 Mbps	4 Mbps	4 Mbps
Broadcast type	Non-local	Non-local	Non-local	Non-local	Non-local

Table A-52. Token-Ring Port - IP Parameters Configured

Parameter	6611 A Slot 2	6611 B Slot 2	6611 C Slot 2	6611 D Slot 2	6611 E Slot 2
Enable IP routing on this port	Enable	Enable	Enable	Enable	Enable
IP address	128.8.104.30	131.2.2.20	131.2.2.101	131.2.2.12	128.8.104.1
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492	1492	1492	1492
Enable ICMP address mask requests	Enable	Enable	Enable	Enable	Enable
Directed broadcast	Disable	Disable	Disable	Disable	Disable
Inbound Port Filters	Disable	Disable	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable	Disable	Disable

Node-Level Parameters Configured

Table A-53. Node Level - RIP Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value	6611 E Value
Enable Routing Information Protocol (RIP)	Enable	Enable	Enable	Enable	Enable
Broadcast	Enable	Enable	Enable	Enable	Enable
Zero reserved fields	Enable	Enable	Enable	Enable	Enable
Route preference	100	100	100	100	100

Table A-54. Node Level - RIP Interface - Detail Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value	6611 E Value
Local IP interface	All	All	All	All	All
IP address of local interface	NA	NA	NA	NA	NA
RIP interface settings					
Version	Version 1	Version 1	Version 1	Version 1	Version 1
Broadcast mode	NA	NA	NA	NA	NA
Metric in	1	1	1	1	1
Metric out	0	0	0	0	0
Listen for RIP updates	Enable	Enable	Enable	Enable	Enable
Send RIP updates	Enable	Enable	Enable	Enable	Enable

Table A-55. Node Level - RIP Source Router Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value	6611 D Value	6611 E Value
IP address of source router	188.8.8.1 188.8.8.101	188.8.8.101 188.8.8.12	188.8.8.1 188.8.8.12 188.8.8.20 188.8.8.30	188.8.8.20 188.8.8.101	188.8.8.30 188.8.8.101

OSPF, IP, and IPX over X.25 Configuration

Figure A-5 shows a sample network in which three 6611s (6611 A, 6611 B, and 6611 C) are configured to route IP and IPX over and X.25 network. The 6611s communicate using OSPF.

The following information is shown in Figure A-5:

- IP addresses
- Slot and port numbers, abbreviated *sx* p*y*
- Ring numbers and ring speeds

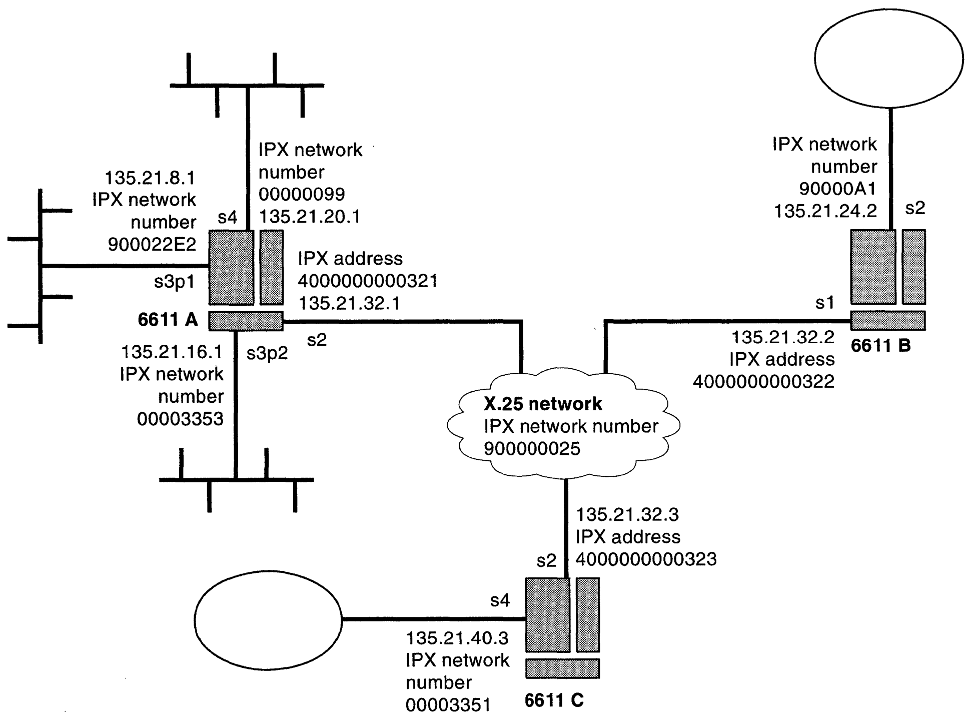


Figure A-5. Sample OSPF and IPX over X.25 Network

The sample network shows the configuration of:

- X.25 connection of routers 6611 B, 6611 B, and 6611 C
- OSPF over X.25
- IPX over X.25
- IP addressing
- Tranparent bridging on the Ethernet segments

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure A-5. The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

X.25 Adapters and the Protocols Running on Them

Table A-56. X.25 Port - X.25 Adapter Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 1 Value	6611 C Slot 2 Value
Enable X.25 interface on this port	Enable	Enable	Enable
Type of line	DTE	DTE	DTE
Locally administered MAC address	4000000000321	4000000000322	4000000000323

Table A-57. X.25 Port - Subscription Mapping Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 1 Value	6611 C Slot 2 Value
Local DTE address (NUA)	321	322	323
Country code ID	none	none	none
Network identifier	other public	other public	other public
Lowest logical channel number for outgoing SVCs	50	251	50
Number of logical channels for outgoing SVCs	0	0	0
Lowest logical channel number for two-way SVCs	20	20	20
Number of logical channels for two-way SVCs	10	10	10
Lowest logical channel number for incoming SVCs	10	5	10
Number of logical channels for incoming SVCs	0	0	0
Lowest logical channel number for PVCs	1	1	1
Number of logical channels for PVCs	1	0	0

Table A-58. X.25 Port - SVC Options Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 1 Value	6611 C Slot 2 Value
SVC defaults			
Receive packet size	128	128	128
Transmit packet size	128	128	128
Receive packet window	2	2	2
Transmit packet window	2	2	2
SVC parameters			
Include calling address in call request packets	include	include	include
include			
Calling address in incoming call packets	*	*	*
*			
Allow incoming calls	Enable	Enable	Enable
Allow outgoing calls	Enable	Enable	Enable

Table A-59. X.25 Port - IP Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 1 Value	6611 C Slot 2 Value
Enable IP routing on this port	Enable	Enable	Enable
IP address	135.21.32.1	135.21.32.2	135.21.32.3
Subnet mask	255.255.248.0	255.255.248.0	255.255.248.0
Max. transmission unit	576	576	576
Enable ICMP address mask request	Enable	Enable	Enable

Table A-60. X.25 Port - 6611 A X.25 Remote Host Parameters Configured

Parameter	6611 A Slot 2 Value 1	6611 A Slot 2 Value 2
List of X.25 remote hosts		
Destination IP address for X.25	135.21.32.2	135.21.32.3
Virtual circuit type	SVC	SVC
Remote DTE address	322	323
Logical channel number	NA	NA

Table A-61. X.25 Port - 6611 B X.25 Remote Host Parameters Configured

Parameter	6611 B Slot 1 Value 1	6611 B Slot 1 Value 2
List of X.25 remote hosts		
Destination IP address for X.25	135.21.32.1	135.21.32.3
Virtual circuit type	SVC	SVC
Remote DTE address	321	323
Logical channel number	NA	NA

Table A-62. X.25 Port - 6611 C X.25 Remote Host Parameters Configured

Parameter	6611 C Slot 2 Value 1	6611 C Slot 2 Value 2
List of X.25 remote hosts		
Destination IP address for X.25	135.21.32.1	135.21.32.2
Virtual circuit type	SVC	SVC
Remote DTE address	321	322
Logical channel number	NA	NA

Table A-63. X.25 Port - IPX Parameters Configured

Parameter	6611 A Slot 2 Value	6611 B Slot 1 Value	6611 C Slot 2 Value
Enable IPX routing on this port	Enable	Enable	Enable
IPX network number	90000025	90000025	90000025
Tick override	Disable	Disable	Disable
Tick value	NA	NA	NA
Split horizon for RIP/SAP updates	On	On	On
SAP update interval	1	1	1
SAP age multiplier	4	4	4
RIP update interval	1	1	1
RIP age multiplier	4	4	4

Table A-64. X.25 Port - 6611 A X.25 Remote Host Detail Parameters Configured

Parameter	6611 A Slot 2 Value 1	6611 A Slot 2 Value 2
Destination IPX address for X.25	4000000000322	4000000000323
Virtual circuit type	SVC	SVC
Remote DTE address	322	323
Logical channel number	NA	NA

Table A-65. X.25 Port - 6611 B X.25 Remote Host Detail Parameters Configured

Parameter	6611 B Slot 2 Value 1	6611 B Slot 2 Value 2
Destination IPX address for X.25	4000000000321	4000000000323
Virtual circuit type	SVC	SVC
Remote DTE address	321	323
Logical channel number	NA	NA

Table A-66. X.25 Port - 6611 C X.25 Remote Host Detail Parameters Configured

Parameter	6611 C Slot 2 Value 1	6611 C Slot 2 Value 2
Destination IPX address for X.25	4000000000321	4000000000322
Virtual circuit type	SVC	SVC
Remote DTE address	321	322
Logical channel number	NA	NA

Ethernet Ports and the Protocols Running on Them

Table A-67. Ethernet Port - Physical Interface Parameters Configured

Parameter	6611 A Slot 3 Port 1 Value	6611 A Slot 3 Port 2 Value	6611 A Slot 4 Value
Enable physical interface on this port	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA
Enable additional multicast addresses	Disable	Disable	Disable
Multicast MAC address	NA	NA	NA

Table A-68. Ethernet Port - IP Parameters Configured

Parameter	6611 A Slot 3 Port 1 Value	6611 A Slot 3 Port 2 Value	6611 A Slot 4 Value
Enable IP routing on this port	Enable	Enable	Enable
IP address	135.21.8.1	135.21.16.1	135.21.20.1
Subnet mask	255.255.248.0	255.255.248.0	255.255.248.0
Max. transmission unit (octets)	1500	1500	1500
Ethernet framing for IP	Ethernet V2.0	Ethernet V2.0	Ethernet V2.0
Enable ICMP address mask requests	Enable	Enable	Enable
Inbound Port Filters	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable

Table A-69. Ethernet Port - IPX Parameters Configured

Parameter	6611 A Slot 3 Port 1 Value	6611 A Slot 3 Port 2 Value	6611 A Slot 4 Value
Enable IPX routing on this port	Enable	Enable	Enable
IPX network number	900022E2	00003353	00000099
Encapsulation method	Ethernet 802.3 LLC	Ethernet 802.3 LLC	Ethernet 802.3 LLC
Tick override	Disable	Disable	Disable
Tick value	NA	NA	NA
Control SAP and RIP broadcasting			
SAP update interval	1	1	1
SAP age multiplier	4	4	4
RIP update interval	1	1	1
RIP age multiplier	4	4	4
Inbound Port Filters	Disable	Disable	Disable

Token-Ring Ports and the Protocols Running on Them

Table A-70. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 B Slot 2 Value	6611 C Slot 4 Port 0 Value
Enable interface	Enable	Enable
MAC address	Universally administered address	Universally administered address
Locally administered address	NA	NA
MAC address format	NA	NA
Token ring data rate	16 Mbps	16 Mbps
Broadcast type	Non-local	Non-local

Table A-71. Token-Ring Port - IP Parameters Configured

Parameter	6611 B Slot 4 Value	6611 C Slot 4 Port 0 Value
Enable IP routing on this port	Enable	Enable
IP address	135.21.24.2	135.21.40.3
Subnet mask	255.255.248.0	255.255.248.0
Max. transmission unit (octets)	1492	1492
Enable ICMP address mask requests	Enable	Enable
Inbound Port Filters	Disable	Disable
UDP Broadcasts	Disable	Disable

Table A-72. Token-Ring Port - IPX Parameters Configured

Parameter	6611 B Slot 2 Value	6611 C Slot 4 Port 0 Value
Enable IPX routing on this port	Enable	Enable
IPX network number	90000A1	00003351
Encapsulation method	Token-Ring 802.5 LLC	Token-Ring 802.5 LLC
Tick override	Disable	Disable
Tick value	NA	NA
Control RIP and SAP broadcasting		
SAP update interval	1	1
SAP age multiplier	4	4
RIP update interval	1	1
RIP age multiplier	4	4
Inbound Port Filters	Disable	Disable

Node-Level Parameters Configured

Table A-73. Node Level - OSPF Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value
Enable OSPF	Enable	Enable	Enable
Router ID	135.21.32.1	135.21.24.2	135.21.40.3

Table A-74. Node Level - OSPF Area Detail Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value
Area ID	0.0.0.0	0.0.0.0	0.0.0.0
Area type	Transit	Transit	Transit
Stub cost	NA	NA	NA
Authentication type	None	None	None

Table A-75. Node Level - 6611 A OSPF Interface Detail Parameters Configured				
Parameter	**6611 A Value 1**	**6611 A Value 2**	**6611 A Value 3**	**6611 A Value 4**
Interface IP address	135.21.8.1	135.21.16.1	135.21.20.1	135.21.32.1
Interface type	Broadcast	Broadcast	Broadcast	Nonbroadcast
Authorization key	NA	NA	NA	NA
Retransmit interval	5	5	5	5
Router priority	1	1	1	1
Interface transit delay	1	1	1	1
Cost	10	10	10	1744
Router dead interval	40	40	40	40
Poll interval	120	120	120	120
Hello interval	10	10	10	10

Table A-76. Node Level - 6611 B OSPF Interface Detail Parameters Configured

Parameter	**6611 B Value 1**	**6611 B Value 2**
Interface IP address	135.21.24.2	135.21.32.2
Interface type	Broadcast	Nonbroadcast
Authorization key	NA	NA
Retransmit interval	5	5
Router priority	1	1
Interface transit delay	1	1
Cost	6	1744
Router dead interval	40	40
Poll interval	120	120
Hello interval	10	10

Table A-77. Node Level - 6611 C OSPF Interface Detail Parameters Configured

Parameter	**6611 C Value 1**	**6611 C Value 2**
Interface IP address	135.21.40.3	135.21.32.3
Interface type	Broadcast	Nonbroadcast
Authorization key	NA	NA
Retransmit interval	5	5
Router priority	1	1
Interface transit delay	1	1
Cost	6	1744
Router dead interval	40	40
Poll interval	120	120
Hello interval	10	10

Table A-78. Node Level - 6611 A OSPF Neighbor Detail Parameters Configured

Parameter	**6611 A Value 1**	**6611 A Value 2**
IP address of neighbor router	135.21.32.2	135.21.32.3
Eligible to become designated router	Disable	Disable

Table A-79. Node Level - 6611 B OSPF Neighbor Detail Parameters Configured

Parameter	6611 B Value 1	6611 B Value 2
IP address of neighbor router	135.21.32.1	135.21.32.3
Eligible to become designated router	Disable	Disable

Table A-80. Node Level - 6611 C OSPF Neighbor Detail Parameters Configured

Parameter	6611 C Value 1	6611 C Value 2
IP address of neighbor router	135.21.32.1	135.21.32.2
Eligible to become designated router	Disable	Disable

Table A-81. Node Level - IPX Routing Parameters Configured

Parameter	6611 A Value	6611 B Value	6611 C Value
Enable IPX router	Enable	Enable	Enable
SAP Filters	Disable	Disable	Enable
RIP Router Filters	Disable	Disable	Disable
Inbound RIP Filters	Disable	Disable	Disable
Outbound RIP Filters	Disable	Disable	Disable

Local DLSw Scenarios

Figure A-6, Figure A-7, and Figure A-8 on page A-32 illustrate remote data link switching scenarios and show how the configuration of the 6611 A differs when SDLC is locally converted for a direct-attached IBM 3174, a remote IBM 3174, and multidrop stations.

These sample networks (Figure A-6, Figure A-7, and Figure A-8 on page A-32) include:

- 6611 A, which has the following port types and protocols running:
  - An SDLC Adapter with SNA stations configured
  - A token-ring port running source route bridging, IP, and SNA

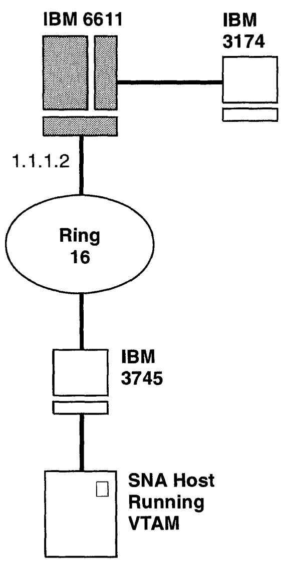


Figure A-6. Sample Network for Local DLSw: SDLC to Direct-Attached IBM 3174

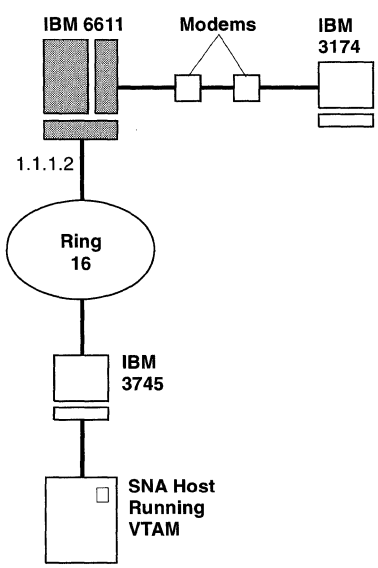


Figure A-7. Sample Network for Local DLSw: SDLC to Remote IBM 3174

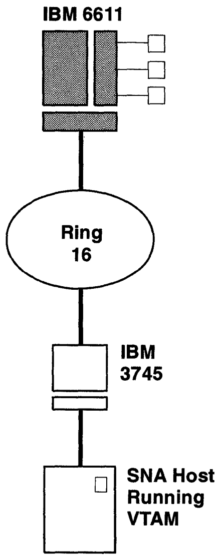


Figure A-8. Sample Network for Local DLSW: SDLC to Multidrop Stations

These sample networks, which are running with a subnet mask of 255.255.255.0, shows the configuration of:

- Local data link switching
- SNA stations
- SLDC to LLC conversion

Summary of All Customized Parameters in Sample Two

Use this section as a reference for Figure A-6 on page A-31, Figure A-7 on page A-31, and Figure A-8 The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

Token-Ring Adapter and the Protocols Running on It

Table A-82. Token-Ring Port - Physical Interface Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Value
Enable physical interface on this port	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA
MAC address format	NA	NA	NA
Token ring data rate	16 Mbps	16 Mbps	16 Mbps
Broadcast type	Non-local	Non-local	Non-local

Table A-83. Token-Ring Port - Source Route Bridging Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Value
Enable Source Route Bridging on this port	Enable	Enable	Enable
Spanning tree mode	automatic	automatic	automatic
Path cost	0	0	0
Port priority for Translational Bridging	80	80	80
Port state	NA	NA	NA
Ring number	16	16	16
Max. transmission unit (octets)	2052	2052	2052

Table A-84. Token-Ring Port - IP Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Value
Enable IP routing on this port	Enable	Enable	Enable
IP address	1.1.1.2	1.1.1.2	1.1.1.2
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Max. transmission unit (octets)	1492	1492	1492
Enable ICMP address mask requests	Disable	Disable	Disable
Inbound Port Filters	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable

Table A-85. Token-Ring Port - SNA Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Value
Enable SNA frame forwarding on this port	Enable	Enable	Enable
SAP value	00, 04	00, 04	00, 04

SDLC Adapter and the Protocols Running on It

Table A-86. SLDC Port Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Value
Data link protocol	V.35	V.35	EIA232D

Table A-87. SDLC Port - Physical Interface Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Value
Enable physical interface on this port	Enable	Enable	Enable
Serial encoding	NRZ	NRZ	NRZ
Request to send	continuous	continuous	continuous
Data rate select	full	full	full
Data terminal ready	Connect data set to line (CDSTL)	Connect data set to line (CDSTL)	Connect data set to line (CDSTL)
Transmit rate (bps)	NA	NA	NA
Bit clocking	NA	NA	NA

Table A-88. SDLC Port - SNA Station Detail Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Station 1	6611 to Multidrop SDLC Station 2	6611 to Multidrop SDLC Station 3
Station address	C1	C1	C1	C2	C3
Station source MAC address[2]	4000123456AA	4000123456AA	4000123123AA	4000456456AA	4000789789AA
Station Source SAP	04	04	04	04	04
Station destination MAC address[1]	400020420451	400020420451	400020420451	400020420451	400020420451
Station Destination SAP	04	04	04	04	04
Station type 2.1	Disable	Disable	Disable	Disable	Disable
Secondary SDLC address for 6611	NA	NA	NA	NA	NA
Station XID value[3]	05D50F59	05D50F59	0D1	0D2	0D3

Node-Level Parameters Configured

Table A-89. Node Level - Source Route Bridging Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Value
Enable Source Route Bridging	Enable	Enable	Enable
Bridge number	6	6	6
Enable LAN Bridging Protocol	Enable	Enable	Enable
Designated ring number	16	16	16
Spanning tree parameters			
Bridge priority	8000	8000	8000
Hello time	2	2	2
Forward delay time	15	15	15
Max age	20	20	20

1 In these examples, the Station destination MAC address is the MAC address of the 3745 connected to the host where VTAM is running.

2 The value of the Station source MAC address parameter must be unique in the network; However, it is not configured in the 3745.

3 The value of the Station XID value parameter is the PU ID provided by VTAM.

Table A-90. System Level - DLSw Parameters Configured

Parameter	6611 to Modem-Attached 3174 Value	6611 to Direct-Attached 3174 Value	6611 to Multidrop SDLC Value
Protocols forwarded by DLSw			
SNA	Enable	Enable	Enable
NetBIOS	Disable	Disable	Disable
SNA transmission bias	NA	NA	NA
Maximum NetBIOS frame size	2052	2052	2052
DLSw parameters			
Virtual ring segment number	FAB	FAB	FAB
Destination cache timeout	8	8	8
Default DLSw IP address for this 6611	1.1.1.2	1.1.1.2	1.1.1.2

Remote DLSw Scenarios

Figure A-9, Figure A-10, and Figure A-11 illustrate remote data link switching scenarios and show how the configuration of the 6611 A differs when the remote device is an IBM 3745, an IBM 3174, or an IBM 3172.

These sample networks includes:

- 6611 A, which has the following port types and protocols running:
  - A serial port running DLSw and IP over PPP
  - A SDLC Adapter running SNA
- 6611 B, which has the following port types and protocols running:
  - A serial port running DLSw and IP over PPP
  - A token-ring port running source route bridging and SNA

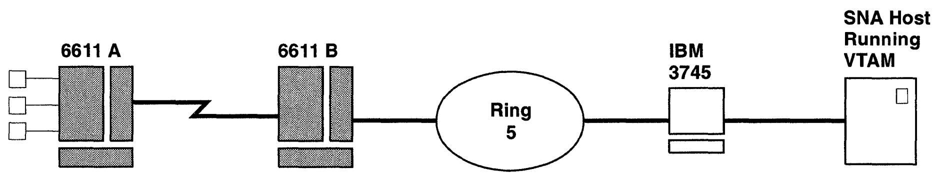


Figure A-9. Sample Network for Remote DLSw: SDLC to Token-Ring Attached 3745

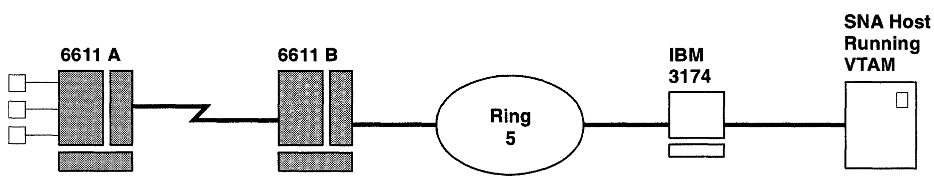


Figure A-10. Sample Network for Remote DLSw: SDLC to Token-Ring Attached 3174

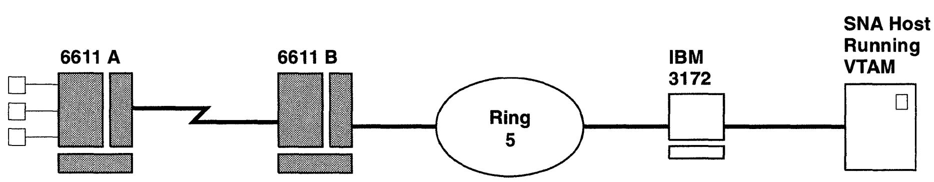


Figure A-11. Sample Network for Remote DLSw: SDLC to Token-Ring Attached 3172

These sample networks, which are running with a subnet mask of 255.255.255.0, shows the configuration of:

- Remote DLSw to various SNA devices
- Source route bridging
- Serial, token-ring, and SDLC ports

Summary of All Customized Parameters in Sample

Use this section as a reference for Figure A-9, Figure A-10, and Figure A-11 The following tables list the parameters for the configuration of the 6611s in the sample network. Defaults are accepted for all configuration options not shown.

6611 A Serial Adapter and the Protocols Running on It

Table A-91. Serial Port Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Data link protocol	PPP	PPP	PPP

Table A-92. Serial Port - Physical Interface Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable physical interface on this port	Enable	Enable	Enable
Interface cable	NA	NA	NA
Cylink serial number	None	None	None
Transmit clock source	NA	NA	NA
Serial line speed	19200	19200	19200
Data encoding	NRZI	NRZI	NRZI
Locally administered MAC address	None	None	None
Enable port for transmission group	NA	NA	NA
Transmission group name	NA	NA	NA

Table A-93. Serial Port - PPP Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable	Enable
Maximum receive unit size	1500	1500	1500
Use magic-number for loopback detection	Disable	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table A-94. Serial Port - IP over PPP Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable IP routing on this port	Enable	Enable	Enable
IP address	8.8.8.1	8.8.8.1	8.8.8.1
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.2	8.8.8.2	8.8.8.2
Max. transmission unit (octets)	1500	1500	1500
Enable ICMP address mask requests	Enable	Enable	Enable
Enable transmission group for IP on this port	NA	NA	NA
Inbound Port Filters	Disable	Disable	Disable
IP Priority	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable

6611 B Serial Adapter and the Protocols Running on It

Table A-95. Serial Port Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Data link protocol	PPP	PPP	PPP

Table A-96. Serial Port - Physical Interface Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable physical interface on this port	Enable	Enable	Enable
Interface cable	NA	NA	NA
Cylink serial number	None	None	None
Transmit clock source	NA	NA	NA
Serial line speed	19200	19200	19200
Data encoding	NRZI	NRZI	NRZI
Locally administered MAC address	None	None	None
Enable port for transmission group	NA	NA	NA
Transmission group name	NA	NA	NA

Table A-97. Serial Port - PPP Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable Point-to-Point Protocol (PPP) on this port	Enable	Enable	Enable
Maximum receive unit size	1500	1500	1500
Use magic-number for loopback detection	Disable	Disable	Disable
Select link quality monitoring method	Link Quality Monitoring protocol	Link Quality Monitoring protocol	Link Quality Monitoring protocol

Table A-98. Serial Port - IP over PPP Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable IP routing on this port	Enable	Enable	Enable
IP address	8.8.8.2	8.8.8.2	8.8.8.2
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Destination IP address	8.8.8.1	8.8.8.1	8.8.8.1
Max. transmission unit (octets)	1500	1500	1500
Enable ICMP address mask requests	Enable	Enable	Enable
Enable transmission group for IP on this port	NA	NA	NA
Inbound Port Filters	Disable	Disable	Disable
IP Priority	Disable	Disable	Disable
UDP Broadcasts	Disable	Disable	Disable

Token-Ring Adapter and the Protocols Running on It

Table A-99. Token-Ring Port - 6611 B Physical Interface Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable physical interface on this port	Enable	Enable	Enable
MAC address	Universally administered address	Universally administered address	Universally administered address
Locally administered address	NA	NA	NA
MAC address format	NA	NA	NA
Token ring data rate	16 Mbps	16 Mbps	16 Mbps
Broadcast type	Non-local	Non-local	Non-local

Table A-100. Token-Ring Port - 6611 B Source Route Bridging Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable Source Route Bridging on this port	Enable	Enable	Enable
Spanning tree mode	Automatic	Automatic	Automatic
Path cost	0	0	0
Port priority for Translational Bridging	80	80	80
Port state	NA	NA	NA
Ring number	5	5	5
Max. transmission unit (octets)	2052	2052	2052

Table A-101. Token-Ring Port - 6611 B SNA Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable SNA frame forwarding on this port	Enable	Enable	Enable
SAP value	00, 04	00, 04	00, 04

SDLC Adapter and the Protocols Running on It

Table A-102. 6611 A SDLC Port Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Data link protocol	EIA232D	EIA232D	EIA232D

Table A-103. SDLC Port - 6611 A Physical Interface Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Enable physical interface on this port	Enable	Enable	Enable
Serial encoding	NRZ	NRZ	NRZ
Request to send	continuous	continuous	continuous
Data rate select	full	full	full
Data terminal ready	Connect data set to line (CDSTL)	Connect data set to line (CDSTL)	Connect data set to line (CDSTL)
Bit clocking	NA	NA	NA
Transmit rate (bps)	NA	NA	NA

Table A-104. SDLC Port - 6611 A SNA Station Detail Parameters Configured

Parameter	SDLC to Token-Ring Attached 3745 Value	SDLC to Token-Ring Attached 3174 Value	SDLC to Token-Ring Attached 3172 Value
Station address	C1	C1	C1
Station source MAC address	4000123456FA	40005C01A555	4000123456FA
Station Source SAP	04	04	04
Station destination MAC address	400037450001	400031740001	400031720001
Station Destination SAP	04	04	04
Station type 2.1	Disable	Disable	Disable
Secondary SDLC address for IBM 6611	NA	NA	NA
Station XID value	05D50F59	None	05D50F59

Note:

When using remote DLSw to communicate between an SDLC-attached device and VTAM via a 3745 or a 3172:

- The value of the Station source MAC address parameter must be unique in the network although it is not configured in the 3745 or 3172.
- The value of the Station XID value parameter is provided by VTAM.

When using remote DLSw to communicate between an SDLC-attached device and VTAM via a 3174:

- The value of the Station source MAC address parameter must be configured in the 3174.
- The value of the Station destination MAC address parameter is the gateway MAC address that is configured in the 3174.
- Do not enter a value for the Station XID value parameter.

Node-Level Parameters Configured

Table A-105. Node Level - Source Route Bridging Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Source Route Bridging	Enable	Enable
Bridge number	6	6
Enable LAN Bridging Protocol	Enable	Enable
Designated ring number	724	5
Spanning tree parameters		
Bridge priority	8000	8000
Hello time	2	2
Forward delay time	15	15
Max age	20	20

Table A-106. Node Level - RIP Parameters Configured

Parameter	6611 A Value	6611 B Value
Enable Routing Information Protocol (RIP)	Enable	Enable
Broadcast	Disable	Disable
Zero reserved fields	Enable	Enable
Route preference	100	100

Table A-107. Node Level - RIP Source Routers Configured

Parameter	6611 A Value	6611 B Value
IP address of source router	8.8.8.2	8.8.8.1

Table A-108. Node Level - DLSw Parameters Configured

Parameter	6611 A Value	6611 B Value
Protocols forwarded by DLSw		
SNA	Enable	Enable
NetBIOS	Disable	Disable
SNA transmission bias	NA	NA
Maximum NetBIOS frame size	2052	2052
DLSw parameters		
Virtual ring segment number	FAB	FAB
Destination cache timeout	8	8
Default DLSw IP address for this 6611	8.8.8.1	8.8.8.2

Table A-109. Node Level - DLSw Partners Parameters Configured

Parameter	6611 A Value
Accept connections from specific 6611s only	Disable
IP address of remote 6611 router	8.8.8.2

4 Because 6611 B does not attach to an actual ring, the value of the Designated ring number parameter is fictitious. The value is required, but in this configuration, it is superfluous.

Appendix B. Service Access Points (SAPs) Reference List

The following table provides a list of the common SAPs.

Table B-1 (Page 1 of 2). Listing of Common SAPs

SAP Value (hex)	Name	Description
X'00'	Null SAP	This address provides some ability to respond to remote nodes even when no SAP has been activated. The SAP supports only connectionless service, and responds only to XID and TEST command LPDUs.
X'02'	LLC Sublayer Management Individual SAP	This SAP is reserved for future use by IEEE-standardized network management facilities.
X'03'	LLC Sublayer Management Group SAP	This SAP is reserved for future use by IEEE-standardized network management entities.
X'04'	SNA Path Control Individual SAP	This is a default individual SAP address, used by SNA nodes, that identifies Path Control as the data link user.
X'05'	SNA Path Control Group SAP	This SAP provides a way to route an LPDU to all SNA SAPs without identifying them beforehand.
X'06'	Department of Defense (DOD) Internal Protocol SAP	This address is reserved for the use by the DOD Internet Protocol.
X'10'	4033 Printer Server SAP	This SAP is used by the IBM LAN connection for printers and plotters.
X'12'	4033 Printer Server SAP	This SAP is used by the IBM LAN connection for printers and plotters.
X'42'	Bridge Spanning Tree Protocol SAP	This SAP is used by the spanning tree protocol.
X'4E'	Manufacturing Message Service (MMS)	This SAP is reserved for use by the Manufacturing Message Service.
X'7E'	ISO 8208 (X.25)	This SAP is reserved for use by the X.25 protocol.
X'80'	Xerox Network Systems (XNS) SAP	This SAP is reserved for use by the XNS protocol.
X'84'	OS/2 Database Manager SAP	This SAP is reserved for use by the OS/2 Database Manager remote data services facility.
X'90'	LMU/2 Fault Manager SAP	This SAP is reserved for use by Library Maintenance Utility (LMU)/2 fault manager facility.
X'AA'	Subnetwork Access Protocol	This SAP signifies the use of a SNAP address within the frame.
X'BC'	VIrtual NEtwork System (VINES) SAP	This SAP is reserved for use by the VINES protocol.
X'D4'	LAN Station Manager Resource Management	This SAP is used by the LAN Station Manager Resource Management facility.
X'DC'	8230 LAN Station Manager Register	This SAP is used by LAN Station Manager when connecting to an IBM 8230 Token-Ring Network Controlled Access Unit.
X'E0'	Internetwork Packet Exchange (IPX) SAP	This SAP is reserved for use by the IPX protocol.
X'F0'	NetBIOS SAP	This SAP is used for all NetBIOS communications.

Table B-1 (Page 2 of 2). Listing of Common SAPs

SAP Value (hex)	Name	Description
X'F2'	LAN Network Manager Managing Process	This SAP is used by LAN Network Manager to manage devices in a bridged token-ring network.
X'F4'	LAN Management Individual SAP	This SAP provides the default individual SAP for LAN management functions when they communicate at the logical link control (LLC) level.
X'F5'	LAN Management Group SAP	This SAP provides the default group SAP address for LAN management functions.
X'F8'	Remote Program Load SAP	This SAP provides a default address to be used for a remote program load (RPL) procedure.
X'FC'	Discovery for Remote Program Load	This SAP is sued for discovery for remote program load.
X'FE'	ISO Network Layer SAP	This SAP is used by the ISO network layer.
X'FF'	Global SAP	This SAP, when used as the DSAP, indicates that copies of the LPDU are to go to each active SAP in this LAN.
X'*x*2', where *x*≠0	Network Management Function SAPs	These SAPs are reserved for future use by IEEE-standardized network management entities.
X'*x*6', where *x*≠0	National Standards Bodies SAP	These SAPs are reserved for assignment by national standards bodies.
X'8*y*'–X'9c', where *y*≠B'xx1x'	User Defined SAPs	These SAPs are to prevent interoperability problems with standards and architectural protocols.
X'F*y*', where *y*≠B'xx1x'	Reserved SAP	These SAPs are reserved for future use by IBM.

Appendix C. Values That Are Set By the X.25 Country Code Parameter

The X.25 country code parameter causes the 6611 to set certain internal values on the X.25 Adapter. Some of these values are set using the Configuration Program while other values are set internally by the 6611 and cannot be changed. Using the Configuration Program, you can set the following values to match your X.25 subscription:

- Subscription Mapping Options (Table 4-91 on page 4-64)
  - CCITT support
  - Connection mode
- PVC Detail (Table 4-92 on page 4-65) and SVC Options (Table 4-93 on page 4-66)
  - Receive packet window (for PVCs)
  - Default SVC receive packet window
- Facilities Control (Table 4-94 on page 4-67)
  - Packet size negotiation facility
  - Packet window size negotiation facility
  - Packet size and packet window size negotiation
  - Reverse charging facility
  - Allow reverse charging
  - CUG basic format
  - CUG extended format
  - CUG with OA selection facility - basic format
  - CUG with OA selection facility - extended format
  - Closed user group

The value of these parameters must match your X.25 network subscription. If you do not use the Configuration Program to specify values for these parameters, the 6611 sets them by default.

Values That Are Set Internally by the 6611

The values set by the 6611 implement CCITT recommendations and meet the requirements of the specific networks supported.

Table C-1 on page C-2 gives the recommended values for these parameters for a wide range of known networks. The majority of networks use a standard set of values.

Notes:

1. The parameters documented in this section *cannot* be set using the Configuration Program. They are set by the 6611 and cannot be changed.
2. The values given are only guaranteed to be correct for those networks on which the homologation and certification tests have been successfully completed and approval for attachment has been received.

Table C-1 (Page 1 of 2). Country Code Values Set Internally by the 6611 (hex)

Network	Feature Codes		Restart on Line Reset	Line Protocol	Valid Throughput Class	
	Frame	Packet			Min	Max
Argentina - Arpac	72 00 00	C0 00 00	01	01	03	0C
Australia - Austpac	72 00 00	C0 00 00	01	01	03	0C
Austria - Datex-P	72 00 00	C0 00 00	01	01	05	0A
Belgium - DCS	72 00 00	C0 00 00	01	01	03	0C
Brazil - Renpac	72 00 00	C0 00 00	01	01	03	0C
Canada - Datapac	72 00 00	C0 00 00	01	01	03	0C
Canada - Infogram	72 00 00	C0 00 00	01	01	03	0C
Canada - Infoswitch X.25/80 CNCP	72 00 00	C0 00 00	01	01	03	0C
CCITT 1980	72 00 00	C0 00 00	01	01	03	0C
CCITT 1984	72 00 00	C0 00 00	01	01	03	0C
Chile - Entel	72 00 00	C0 00 00	01	01	03	0C
China - Chinapac	72 00 00	C0 00 00	01	01	03	0C
Denmark - Datapac	72 00 00	C0 00 00	01	01	03	0C
Denmark - Paxnet	72 00 00	C0 00 00	01	01	03	0C
Egypt - Egyptnet DPS-2500	72 00 00	C0 00 00	01	01	03	0C
Finland - Datapak DPS-1500	72 00 00	C0 00 00	01	01	03	0C
Finland - HTC	72 00 00	C0 00 00	01	01	03	0C
France - Transpac	72 00 00	C0 00 00	01	01	03	0C
Germany - Datex-P	72 00 00	C0 00 08	01	01	03	0C
Germany - Siemens 84	72 00 00	C0 00 00	01	01	03	0C
Greece - Hellaspac	72 00 00	C0 00 00	01	01	03	0C
Hong Kong - Datapak	72 00 00	C0 00 00	01	01	03	0C
Hong Kong - Intelpak	72 00 00	C0 00 00	01	01	03	0C
Iceland - Eripax	72 00 00	C0 00 00	01	01	03	0C
Iceland - Packice	72 00 00	C0 00 00	01	01	03	0C
Indonesia - Indosat	72 00 00	C0 00 00	01	01	03	0C
Indonesia - Packsatnet	72 00 00	C0 00 00	01	01	03	0C
Indonesia - SKDP	72 00 00	C0 00 00	01	01	03	0C
Ireland - Eirpac	72 00 00	C0 00 00	01	01	03	0C
Israel - Isranet	72 00 00	C0 00 00	01	01	03	0C
Italy - node	72 00 00	C0 00 00	01	01	03	0C
Italy - concentrator	72 00 00	C0 00 00	01	01	03	0C
Japan - DDX-P	72 00 00	C0 00 00	01	01	03	0C
Japan - Venus	72 00 00	C0 00 00	01	01	03	0C
Korea - Dacom-net	72 00 00	C0 00 00	01	01	03	0C
Luxemborg - Luxpac	72 00 00	C0 00 00	01	01	03	0C

Table C-1 (Page 2 of 2). Country Code Values Set Internally by the 6611 (hex)

Network	Feature Codes		Restart on Line Reset	Line Protocol	Valid Throughput Class	
	Frame	Packet			Min	Max
Malaysia - Maypac	72 00 00	C0 00 00	01	01	03	0C
Mexico - Telepac	72 00 00	C0 00 00	01	01	03	0C
Netherlands - Datanet 1	72 00 00	C0 00 00	01	01	03	0C
New Zealand - NZPO	72 00 00	C0 00 00	01	01	03	0C
Norway - Datapak	72 00 00	C0 00 00	01	01	03	0C
Portugal - Telepac	72 00 00	C0 00 00	01	01	03	0C
Singapore - Telepac	72 00 00	C0 00 00	01	01	03	0C
South Africa - Saponet	72 00 00	C0 00 00	01	01	03	0C
Spain - Iberpac	72 00 00	C0 00 00	01	01	03	0C
Sweden - Datapak	72 00 00	C0 00 00	01	01	03	0C
Switzerland - Telepac	72 00 00	C0 00 00	01	01	03	0C
Taiwan - Pacnet	72 00 00	C0 00 00	01	01	03	0C
Turkey - Turpak	72 00 00	C0 00 00	01	01	03	0C
UK - PSS-1	72 01 00	E1 2D 00	01	01	03	0C
UK Extended - PSS-1	72 01 00	E1 2E 00	01	01	03	0C
USA - Accunet	72 00 00	C0 00 00	01	01	03	0C
USA - DDN	E0 00 00	DA 00 00	01	00	03	0C
USA - Infonet BBN	72 00 00	C0 00 00	01	01	03	0C
USA - Telenet	FB 00 00	C1 00 00	01	01	03	0C
USA - Tymnet	72 00 00	C0 00 00	01	01	03	0C
XI - PRPQ 2.0	72 00 00	C0 00 00	01	01	03	0C
Yugoslavia - Jupak	72 00 00	C0 00 00	01	01	03	0C

Network

The values in the Network column of Table C-1 on page C-2 identify the X.25 network whose parameter settings are described. This column can include the country name, X.25 provider name, and standard supported.

Feature Codes

The feature codes control various frame and packet level functions. See Table C-2 on page C-4 and Table C-3 on page C-5 for descriptions of the various features that are governed by these controls.

Frame Level Feature Controls

The frame level feature controls consist of 3 unsigned 8 bit values. Reading from left to right, the possible values for

- the first 2 digit field (Frame Level Feature Controls) are described in Table C-2
- the second 2 digit field are described in Frame Level Feature Control 1 on page C-5
- the third 2 digit field are described in Frame Level Feature Control 2 on page C-5.

Table C-2 (Page 1 of 2). Frame Level Feature Controls

Byte	Feature	Description
X'01'	Force Frame Reject (FRMR)	• 0 - FRMR is sent for every frame received. • 1 - FRMR is sent for the first frame received; subsequent frames are ignored.
X'02'	Frame Reject on Receive Ready (FRMR on RR)	• 0 - RRs are ignored in the FRMR state. • 1 - When in the FRMR state, RRs are received and FRMRs are sent.
X'04'	Clear Poll/Final (P/F)	• 0 - The P/F bit is not cleared during the frame identification sequence. • 1 - The P/F bit is cleared during the frame identification sequence.
X'08'	Disconnect Answer (DISC ANSW)	• 0 - When in Set Asynchronous Balance Mode (SABM) Sent state, a Disconnected Mode (DM) is sent in response to a disconnect frame. • 1 - When in SABM Sent state, an Unnumbered Acknowledgement (UA) is sent in response to a disconnect frame.
X'10'	Disconnect (DISC) Action	• 0 - When in SABM sent state, the link is disconnected in response to a disconnect frame. • 1 - When in SABM sent state, a SABM is sent in response to a disconnect frame.
X'20'	Information Counter (INFO COUNT)	• 0 - When the link is in T1 state and the T1 timer expires with no acknowledgement received, the frame is retransmitted. The retransmission counter is cleared when the frame is retransmitted. • 1 - When the link is in T1 state and the T1 timer expires with no acknowledgement received, the frame is retransmitted. The retransmission counter is not cleared until the retransmitted frame is acknowledged.
X'40'	N2 Action	• 0 - When a frame level connection is requested, the current frame level continuously attempts to connect the link. • 1 - When a frame level connection is requested, the current frame level attempts to connect the link for the number of transmissions specified by the N2 timer.
X'80'	Disable Disconnect Mode (DM)	• 0 - When a link is in the disconnect (DISC) state and an RR, Receive Not Ready (RNR), Reject (REJ), or INFO is received, a DM is sent. • 1 - When a link is in the DISC state and an RR, RNR, REJ, or INFO is received, the frames are discarded and no DM is sent.

Table C-2 (Page 2 of 2). Frame Level Feature Controls

Byte	Feature	Description
Frame Level Feature Control 1		
X'01'	Remote Busy	• 0 - When the remote DCE indicates that it is no longer busy and sends an RR response frame, the 6611 begins frame retransmission with a new RR. This causes the DCE to synchronize to the 6611. • 1 - When the remote DCE indicates that it is no longer busy and sends an RR response frame, frame retransmission begins with the sequence number identified in the RR and is therefore equivalent to a Reject (REJ) frame. This causes the 6611 to synchronize to the DCE. This method complies with certain homologation requirements.
Frame Level Feature Control 2		
X'00'	Reserved	This byte is unused but should be set to zero to ensure future compatibility.

Packet Level Feature Controls

The packet level feature controls consist of 3 unsigned 8 bit values. Reading from left to right, the possible values for

- the first 2 digit field (Packet Level Feature Controls) are described in Table C-3
- the second 2 digit field are described in Packet Level Feature Control 1 on page C-6
- the third 2 digit field are described in Packet Level Feature Control 2 on page C-6.

Table C-3 (Page 1 of 3). Packet Level Feature Controls

Byte	Feature	Description
X'010000'	Call Data	• 0 - When the fast select option has not been selected, user data is not allowed in the call accept packet. • 1 - When the fast select option has not been selected, user data is allowed in the call accept packet.
X'020000'	D-bit Confirmation (CONF)	• 0 - The D-bit is enabled in call confirmation packets. • 1 - The D-bit is disabled in call confirmation packets.
X'040000'	Reserved	This bit is reserved.
X'080000'	Time Diagnostics (DIAG)	• 0 - When a restart is sent to the remote DCE, the T20 timer is set. If no acknowledgement for the restart is received when the timer expires, the restart packet is retransmitted with a T20 EXPIRED diagnostic. • 1 - When a restart is sent to the remote DCE, the T20 timer is set. If no acknowledgement for the restart is received when the timer expires, the restart packet is retransmitted with a general diagnostic code that does not specify which timer expired. This is the DDN compliant method.

Table C-3 (Page 2 of 3). Packet Level Feature Controls

Byte	Feature	Description
X'100000'	Clear Length	• 0 - Allows the transmission of facilities and/or user data in clear and clear confirmation packets by accepting packets of lengths greater than those specified by CCITT 1984. • 1 - Enforces the CCITT 1984 standard by rejecting clear packets of more than 5 bytes and clear confirmation packets of more than 3 bytes.
X'200000'	Unassigned	• 0 - A packet received on an unassigned logical channel number (LCN) is ignored. • 1 - A packet received on an unassigned LCN is answered with a clear. This method is Packet Switch Stream (PSS) compliant.
X'400000'	PVC Reset	• 0 - When a permanent virtual circuit (PVC) is opened by a user, the virtual circuit is immediately available for data transfer and no reset is sent. • 1 - When a PVC is opened by a user, a reset packet is sent and the virtual circuit does not go to data transfer state only until the reset confirmation is received.
X'800000'	Collision	• 0 - Clear and reset collisions are transparent to the application and the user. • 1 - The application is notified when clear and reset collisions occur.
Packet Level Feature Control 1		
X'000300'	Call Accept (ACPT)	• X'00' - PSS uses this value to indicate that the length of the call accept packet is not checked. • X'01' - PSS uses this value to enforce a 3 byte maximum length for the call accept packet. • X'02' - PSS uses this value to enforce a 5 byte maximum length for the call accept packet.
X'000400'	Prevent Duplicate (DUP)	• 0 - The facility field is not checked for duplicate facilities. • 1 - The facility field is checked for duplicate facilities. This method is PSS compliant.
X'000800'	Fast Select Restart (SEL REST) Flow	• 0 - All CCITT facilities are allowed. • 1 - Calls with fast select restricted response and flow control facilities are cleared. This method is compliant to PSS restrictions on the use of Fast Select and Flow Control Negotiation facilities.
X'001000'	Fast Select Confirmation (SEL CONF) Flow	• 0 - Does not restrict the addition of Fast Select Call confirmation. • 1 - Prevents flow control facilities from being added to a Fast Select Call confirmation if they were not included in the Call packet.
X'002000'	Fast Select Parity Checking (PAR CHK)	• 0 - All CCITT facilities are allowed. • 1 - Checks for the Fast Select facility are made. This method is compliant with PSS use of the Fast Select facility.
Packet Level Feature Control 2		

Table C-3 (Page 3 of 3). Packet Level Feature Controls

Byte	Feature	Description
X'000001'	DCE Short Restart	• 0 - Rejects Restart packets of 4 bytes or less and sends a diagnostic code. • 1 - Allows Restart packets of 4 bytes or less without sending a diagnostic code.
X'000002'	DCE Short Clear	• 0 - Rejects Clear packets of 4 bytes or less and sends a diagnostic code. • 1 - Allows Clear packets of 4 bytes or less without sending a diagnostic code.
X'000004'	DCE Short Reset	• 0 - Rejects Reset packets of 4 bytes or less and sends a diagnostic code. • 1 - Allows Reset packets of 4 bytes or less without sending a diagnostic code.
X'000008'	DCE Short Connect	• 0 - Rejects Call confirm packets of 4 bytes or less. • 1 - Allows Call confirm packets of 4 bytes or less without a facility length.

Restart on Line Reset

This value controls whether packet level sends a Restart packet after level 2 connected is requested (for example, after XIOUP).

Data Size An unsigned 8 bit value

Range 0 to 1

Typical Value 1

Description

- 0 - When a level 2 connection is requested, packet level will not send a Restart.
- 1 - When a level 2 connection is requested, packet level sends a Restart.

Line Protocol

This value pertains only to line-oriented actions (for example, restarts). It controls whether the diagnostic bytes conform to the ISO 8208 standards or to the IBM SNA standards.

Data Size An unsigned 8 bit value

Range 0, 1, 3

Typical Value 0

Description

- 0 - When line-oriented actions (for example, Restarts) occur, the diagnostic bytes that are sent conform to ISO 8208 cause codes and diagnostics standards.
- 1 - When line-oriented actions (for example, Restarts) occur, the diagnostic bytes that are sent conform to SNA cause

codes and diagnostics standards. See *X.25 1984/1988 Architecture Reference* (SC30-3409) for more information.

Note: X'80' is used as a cause code when using CCITT 1984 extensions. Otherwise, X'00' is used.

Valid Throughput Class

These values control the minimum and maximum throughput classes allowed by the network. These values must be set if the network does not wish to receive requests for a class outside this range of CCITT values. Call set-up packets for requests whose class is outside this range are cleared.

The following information describes the minimum and maximum valid throughput values.

Data Size An unsigned 8 bit value

Range 3 to 12

Typical Value 3

Appendix D. Using the ASCII File Options

Note: This appendix explains how to create, change, and read 6611 configuration files in ASCII format. IBM recommends that only those experienced in configuring 6611s use these functions. The Configuration Program will *not* validate any changes you make to an ASCII version of a configuration file.

6611 configuration files are, by default, saved in binary format. You can, however, use the Configuration Program to create and read 6611 configuration files in ASCII format. You can also convert configuration files from one format to the other.

An ASCII configuration file may be useful if you need to alter many configurations at one time, without having to enter and exit the Configuration Program many times. For example, if you need to update many IP addresses throughout a network, it may be quicker for you to save the affected 6611 configuration files in ASCII format and then manually (or automatically with a program) update the addresses. A configuration file saved in ASCII format is also useful when you want to scan the configuration online or print it for review.

Once updated, the configurations can be saved in either ASCII format or binary format, or both formats. When loading a configuration on a 6611 however, the configuration must be in binary format.

The following sections explain the options available for creating, reading, and converting ASCII configuration files. ASCII file element descriptions are also given. Since configuration parameters are represented in an ASCII file by label rather than by name, a series of label/name mappings are also given.

Creating, Reading and Converting ASCII Configuration Files

To work with ASCII configuration files, first select **Configure** from the Configuration Program main menu pull-down. Then select **ASCII file** from the list of tasks. The following ASCII file options are then displayed:

- The **Read ASCII file** option reads an ASCII formatted configuration file from the hard drive. You specify the path from which the ASCII file is read.
- The **Create ASCII file** option writes an ASCII formatted configuration file to the hard drive.
- The **Convert binary to ASCII** option enables you to select one or more binary formatted configuration files from a configuration database, create ASCII formatted files, and save them to the hard drive.
- The **Convert ASCII to binary** option enables you to select one or more ASCII formatted configuration files from the hard drive, create binary formatted configuration files, and save them to a configuration database.

ASCII File Format

An ASCII-formatted configuration file is human-readable representation of a 6611 configuration. The file is composed of a series of definitions, each related to a specific 6611 configuration parameter.[1]

The following section explains how configuration parameters and their values are represented in an ASCII file.

Configuration Parameter Names and Labels

Each configuration parameter has a name. To uniquely identify a configuration parameter in a shortened format, each parameter also is given a label. Labels begin with one of the following prefixes:

BX- A node-level parameter

PT- A port-level parameter

ST- An SDLC-specific parameter

The remaining part of the parameter label reflects the specific function to which that parameter belongs. For example, if the parameter is used to define the RIP protocol (node level), then the label might be **BX-RIP-10**. The **RIP** in the label identifies the parameter as being part of the RIP protocol definition. The **10** is simply a unique identifier for the specific parameter. In this case, the specific parameter name is **IP address of trusted router**; if you were to save the ASCII file with comments in this case, the comment would show the name associated with this label.

Element Data Type

Each element must have a data type so that the Configuration Program can store the values in the proper format. The following is a list of valid data types supported by the Configuration Program:

Four Segment
: Address Type Used for IP addresses and IP address masks.

Numeric
: Typically used for data that may have mathematical calculations performed on it. Data value ranges are enforced on all numeric data types.

String
: Each string must be within a certain length and can only be composed of a specific set of characters

Enumerated
: Used for multiple-choice values. When an ASCII file is saved with comments, the comments explain the possible values.

Booleans
: Used for a variety of data types:

  Enable/Disable: 1 = enable, 2 = disable. Used mainly for enabling/disabling adapter ports and protocols.

  Deny/Permit: 0 = deny, 1 = permit. Used mainly for setting filters.

[1] Some definitions are not directly related to configuration parameters. IBM recommends that users alter only the definitions that are represented in the Configuration Program.

Yes/No	1 = yes, 2 = no. This is also used for indicating whether an adapter port or protocol is "turned on/off."

Grouping the Parameters and Their Values

The node-level configuration parameters in an ASCII file appear in the first section of the file. Port-level parameters follow the node-level parameters.

Irregardless of whether the parameters are node-level or port-level, related information is structured into groups. The most simple grouping involves a configuration parameter and its value. A more complex grouping may involve several related parameters grouped under a single, high-level parameter.

Here is an example of a simple grouping:

```
#'PT-IP-01' = '9.67.1.5'
```

In this example, the configuration parameter label **PT-IP-01** has a value of **9.67.1.5**. If you were to save a configuration file with this parameter, and the file is saved with comments, you would see that the label **PT-IP-01** corresponds to the parameter named **IP address**.

The preceding example shows the simplest grouping present in an ASCII file. Typically, multiple label/value pairs are grouped together according to some relationship. For example, all IP parameters configured for a certain port are grouped together. Here is an example of a more complex IP configuration parameter grouping:

```
#'PT-IP-At' = {
     #'PT-IP-01' = '9.67.1.5'
     #'PT-IP-07' = '1'
}
```

In this example, two related IP configuration parameters are grouped together under a higher-level heading. The indention shows the relationships of the parameters involved.

There may be cases where several groupings, like the preceding example, are themselves grouped under yet another higher-level heading. Assume that someone has configured two 6611 controlling users and their passwords. The ASCII file structure would appear as follows:

```
#'BX-USER-ControllingList' = {
    #'BX-USER-Controlling-At' = {
       #'BX-USER-01' = 'janet'
       #'BX-USER-02' = 'passwrd1'
    }
    #'BX-USER-Controlling-At' = {
       #'BX-USER-01' = 'roseman'
       #'BX-USER-02' = 'passwrd2'
    }
}
```

In this example, each controlling user/password group is defined under its own **#'BX-USER-Controlling-At'** heading. Both of these groups are included under the heading **#'BX-USER-ControllingList'**, which identifies the beginning of the list of controlling users and their passwords.

The previous examples illustrate the hierarchical structure of the configuration parameters as represented in an ASCII file. This structure is followed consistently. Related parameters are always grouped, and sometimes nested, within higher-level headings.

Port-level parameters always occur under headings that identify the slot number, port number, and adapter type. Here is an example of a heading that identifies the beginning of a port definition:

```
Slot: 1 Port: 0 Adapter: 'Adapter-TR'
```

The example heading shows that slot 1, port 2 is defined as a token-ring adapter. All parameters that follow this heading will be assigned to that port, until a new slot/port/adapter type heading is encountered.

The adapter types, as represented in an ASCII file, are as follows:

ASCII File Label	**Description**
Adapter-ET	Ethernet Adapter
Adapter-ET-1port	1-Port Ethernet Adapter
Adapter-ET-2port	2-Port Ethernet Adapter
Adapter-ET-SE	Multi-Interface Serial/Ethernet Combination Adapter
Adapter-SE	2-Port Serial Adapter
Adapter-SE-2port	2-Port Multi-Interface Serial Adapter
Adapter-SE-4port	4-Port Multi-Interface Serial Adapter
Adapter-TR	Token-Ring Network 16/4 Adapter
Adapter-TR-1port	1-Port Token-Ring Network 16/4 Adapter
Adapter-TR-2port	2-Port Token-Ring Network 16/4 Adapter
Adapter-TR-SE	Multi-Interface Serial/Token-Ring Combination Adapter
Adapter-X25	X.25 Adapter
Adapter-MUL	4-Port SDLC Adapter
Adapter-ISDN	I-I/F BRI RPQ Adapter
Adapter-8Port	8-Port Asynchronous Adapter (ARC Adapter)

Parameter Label Mapping Lists

The Configuration Program represents configuration parameters externally by their names, and internally by their labels. In an ASCII configuration file, all configuration parameters are identified by their labels. If you save an ASCII configuration file with comments, the parameter name will be provided, as a comment, in addition to the label. The following lists show the labels and names associated with all configuration parameters.

General Parameters

Do *not* alter the values of these configuration parameters.

Table D-1. General Parameter Labels

BX-AARELEASE-NO6611	Configuration Number
BX-AAVERSION-NO6611	Version Number

AppleTalk Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheets" on page 5-232 and "Node Level Worksheet" on page 5-255.

Table D-2 (Page 1 of 2). AppleTalk Parameter Labels

BX-APP-01	Enable AppleTalk
PT-APP-01	Network Number Range
PT-APP-03	Default Zone Name

Table D-2 (Page 2 of 2). AppleTalk Parameter Labels

PT-APP-04	Control Routing Information Received on This Port
PT-APP-08	Additional Zone Name
PT-APP-09	Enable Security Filter for Resource Names
PT-APP-10	Enable Network Number Range Filter
PT-APP-11	Network Number Range Start
PT-APP-12	Network Number Range End
PT-APP-13	Enable AppleTalk on this Port
PT-APP-16	Port Type
PT-APP-17	Starting Value for Node ID Acquisition
PT-APP-18	DLCI Number
PT-APP-21	Network Number Range Start
PT-APP-22	Network Number Range End
PT-APP-28	Allowable Zone Name
PT-APP-30	Enable Network Number Range Filter
PT-APP-31	Network Number Range Start
PT-APP-32	Network Number Range End
PT-APP-34	Enable Split Horizon for Routing Table Updates
PT-APP-35	Hop Weight
PT-APP-36	Optimize NBP Broadcast Request Processing
PT-APP-37	Generate DDP Checksum
PT-APP-38	Enable Security Filter for Zone Names
PT-APP-39	Accept All Zone Information Acquired from Selected Network

APPN Parameters

For descriptions of these configuration parameters, refer to "Node Level Worksheets" on page 5-394.

Table D-3 (Page 1 of 2). APPN Parameter Labels

BX-APPN-01	Network ID
BX-APPN-02	Control Point Name
BX-APPN-03	XID ID Number (Subarea Connection)
BX-APPN-04	Accept Connection Requests from Any Node
BX-APPN-05	Maximum Number of APPN Network Nodes
BX-APPN-06	Maximum Cached Directory Entries
BX-APPN-07	Maximum Number of Serviced End and LEN Nodes
BX-APPN-08	Maximum Shared Memory
BX-APPN-11	Select Tuning Option
BX-APPN-12	Average Number of LUs for Serviced Nodes
BX-APPN-13	Manual Tuning
BX-APPN-14	Enable APPN
BX-APPN-30	Process Management
BX-APPN-31	Process to Process Communication
BX-APPN-32	Locking
BX-APPN-33	Miscellaneous Tower Activities
BX-APPN-34	I/O to/from the System
BX-APPN-35	Storage Management
BX-APPN-36	Queue Data Type Management
BX-APPN-37	Table Data Type Management
BX-APPN-38	Buffer Management
BX-APPN-39	Configuration Control
BX-APPN-40	Timer Service
BX-APPN-41	Service Provider Management
BX-APPN-42	Inter-process Message Segmenting
BX-APPN-43	Control of Processes Outside Scope of This Tower
BX-APPN-44	Monitoring Existence of Processes, Services, Towers
BX-APPN-45	Distributed Environment Control
BX-APPN-46	Process to Service Dialogs
BX-APPN-AC-01	Create Intermediate Session Records
BX-APPN-AC-02	Record Creation Threshold
BX-APPN-AC-03	Memory
BX-APPN-AC-04	DASD
BX-APPN-AC-05	Maximum Buffers in Memory
BX-APPN-AC-06	Maximum Records per Buffer in Memory
BX-APPN-AC-07	Buffers in Memory Full

Table D-3 (Page 2 of 2). APPN Parameter Labels

BX-APPN-AC-08	Record Format
BX-APPN-AC-10	Maximum Buffers in DASD
BX-APPN-AC-11	Maximum Records per Buffer in DASD
BX-APPN-AC-12	Buffers in DASD Full
BX-APPN-AC-13	Record Format
BX-APPN-PT-01	Link Type
BX-APPN-PT-02	MAC Address of This Node
BX-APPN-PT-03	SAP Address of This Node
BX-APPN-PT-04	Port Name
BX-APPN-PT-05	My IP Port
BX-APPN-PT-07	Cost Per Connect Time
BX-APPN-PT-08	Cost Per Byte
BX-APPN-PT-09	Security
BX-APPN-PT-10	Propagation Delay
BX-APPN-PT-11	Effective Capacity
BX-APPN-PT-12	First User-Defined TG Characteristic
BX-APPN-PT-13	Second User-Defined TG Characteristic
BX-APPN-PT-14	Third User-Defined TG Characteristic
BX-APPN-SA-01	Collect Intermediate Session Information
BX-APPN-SA-02	Save RSCV Information for Intermediate Sessions
BX-APPN-ST-01	Link Station Name
BX-APPN-ST-02	MAC Address
BX-APPN-ST-03	IP Address
BX-APPN-ST-04	SAP Address
BX-APPN-ST-05	Fully Qualified Control Point Name
BX-APPN-ST-06	XID ID Number
BX-APPN-ST-07	XID Block Number
BX-APPN-ST-08	Adjacent Node Type
BX-APPN-ST-10	Fully Qualified LU Name
BX-APPN-ST-11	Destination IP Port
BX-APPN-ST-13	Activate Link Automatically
BX-APPN-ST-15	Enable Session Level Security
BX-APPN-ST-16	Key
BX-APPN-ST-17	Cost Per Connect Time
BX-APPN-ST-18	Cost Per Byte

Table D-3 (Page 2 of 2). APPN Parameter Labels

BX-APPN-ST-19	Security
BX-APPN-ST-20	Propagation Delay
BX-APPN-ST-21	Effective Capacity
BX-APPN-ST-22	First User-Defined TG Characteristic
BX-APPN-ST-23	Second User-Defined TG Characteristic
BX-APPN-ST-24	Third User-Defined TG Characteristic

ARC Parameters

For descriptions of these configuration parameters, refer to the documentation associated with PRPQ 85251 (IBM 6611ARC).

Table D-4. ARC Parameter Labels

BX-ARC-01	Node Alias
BX-ARC-02	Maximum Sessions
BX-ARC-03	Collector Interval (milliseconds)
BX-ARC-04	Collector Buffer High Water Mark (%)
BX-ARC-05	Maximum Collectors
BX-ARC-06	Maximum Sessions Per Collector
BX-ARC-07	Exit Message
BX-ARC-08	Maximum LAN Users
BX-ARC-09	LAN Inactivity Check
BX-ARC-10	LAN Inactivity Period (Minutes)
BX-ARC-11	LAN Sessions Per User
BX-ARC-12	LAN User Interface
BX-ARC-13	LAN Menu Key
BX-ARC-14	LAN Help Key
BX-ARC-15	LAN Menu Prompt
BX-ARC-16	Enable ARC
BX-BAN-01	Herald Message

BGP Parameters

For descriptions of these configuration parameters, refer to "Node Level Worksheets" on page 5-133.

Table D-5. BGP Parameter Labels

BX-BGP-01	Enable Border Gateway Protocol (BGP)
BX-BGP-02	Default
BX-BGP-03	Default Metric
BX-BGP-04	BGP Group Type
BX-BGP-05	Autonomous System Number
BX-BGP-06	Metric Out
BX-BGP-07	BGP Group Name
BX-BGP-08	Generate Default Route
BX-BGP-09	Next Hop Destination
BX-BGP-10	Preference (0 - 255)
BX-BGP-11	Interface IP Address
BX-BGP-12	Hold Time
BX-BGP-15	Passive
BX-BGP-16	Default Network In
BX-BGP-17	Default Network Out
BX-BGP-19A	IP Address
BX-BGP-19B	Mask
BX-BGP-19	Neighbor
BX-BGP-20	BGP Neighbor IP Address
BX-BGP-21	Metric Out
BX-BGP-23	Generate Default Route
BX-BGP-24	Next Hop Destination
BX-BGP-25	Preference (0-255)
BX-BGP-26	Interface IP Address
BX-BGP-27	Hold Time
BX-BGP-30	Passive
BX-BGP-31	Default Network In
BX-BGP-32	Default Network Out
BX-BGP-34	BGP Neighbor Name
BX-BGPIMP-10	Autonomous System Path Origin
BX-BGPIMP-01	Autonomous System Number (1 - 65534)
BX-BGPIMP-02	Restrict Imports
BX-BGPIMP-03	Preference (0 - 255)
BX-BGPIMP-04	Destination
BX-BGPIMP-05	Destination Mask
BX-BGPIMP-06	Restrict Routes
BX-BGPIMP-07	Preference (0 - 255)
BX-BGPIMP-08	Enable BGP Import Filters
BX-BGPIMP-09	Autonomous System Path Specification
BX-BGPIMP-11	BGP Import Name

Source Route Bridging Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheets" on page 5-16 and "Node Level Worksheets" on page 5-39.

Table D-6 (Page 1 of 3). Source Route Bridging Parameter Labels

BX-BRI-01	Enable Source Route Bridging
BX-BRI-02	Bridge Number
BX-BRI-03	Bridge Priority
BX-BRI-04	Hello Time
BX-BRI-05	Forward Delay
BX-BRI-06	Max Age
BX-BRI-07	Designated Ring Number
BX-BRI-09	Hop Count Filter
BX-BRI-10	RI Field Filter
BX-BRI-11	Source SAP Filter
BX-BRI-12	SNAP Value Filter
BX-BRI-13	MAC Address Filter
BX-BRI-14	Sliding Window Filter
BX-BRI-400	Enable LAN Bridging Protocol
PT-BRI-01	Enable Source Route Bridging on This Port
PT-BRI-02	Ring Number
PT-BRI-03	Ring Number
PT-BRI-04	DLCI Number
PT-BRI-05	Spanning Tree Mode
PT-BRI-06	Enable Forwarding of Single-Route Broadcast Frames
PT-BRI-07	Path Cost
PT-BRI-08	Maximum Transmission Unit
PT-BRI-100	Filtering Mode of Outbound Source SAP Filters
PT-BRI-101	Frame Type of Outbound Source SAP Filter
PT-BRI-103	Source SAP Value

Table D-6 (Page 2 of 3). Source Route Bridging Parameter Labels

PT-BRI-104	Enable Outbound SAP Filters on This Port
PT-BRI-109	Filter Name
PT-BRI-110	Enable Inbound Sliding Window Filters on This Port
PT-BRI-111	Filtering Mode of Inbound Sliding Window Filters
PT-BRI-113	Offset Starting Field
PT-BRI-114	Offset into Frame
PT-BRI-115	Sliding Window Contents
PT-BRI-116	Sliding Window Mask
PT-BRI-119	Filter Name
PT-BRI-120	Enable Outbound Sliding Window Filters on This Port
PT-BRI-121	Filtering Mode of Outbound Sliding Window Filters
PT-BRI-123	Offset Starting Field
PT-BRI-124	Offset into Frame
PT-BRI-125	Sliding Window Contents
PT-BRI-126	Sliding Window Mask
PT-BRI-127	Frame Type of Inbound Sliding Window Filter
PT-BRI-128	Frame Type of Outbound Sliding Window Filter
PT-BRI-130	Inbound Hop Count Filter Order
PT-BRI-131	Inbound Ring Number Filter Order
PT-BRI-132	Inbound Source SAP Filter Order
PT-BRI-133	Inbound SNAP Value Filter Order
PT-BRI-134	Inbound MAC Address Filter Order
PT-BRI-135	Inbound Sliding Window Filter Order
PT-BRI-141	RI Field Filter
PT-BRI-142	Outbound Source SAP Filter Order
PT-BRI-143	Outbound SNAP Value Filter Order
PT-BRI-144	Outbound MAC Address Filter Order
PT-BRI-145	Outbound Sliding Window Filter Order
PT-BRI-20	Filtering Mode of Inbound Source SAP Filters
PT-BRI-21	Frame Type of Inbound Source SAP Filter
PT-BRI-23	Source SAP Value

Table D-6 (Page 2 of 3). Source Route Bridging Parameter Labels

PT-BRI-24	Enable Inbound Source SAP Filters on This Port
PT-BRI-30	Filtering Mode of Inbound RI Field Filters
PT-BRI-31	Frame Type of Inbound RI Field Filter
PT-BRI-33	Ring Number
PT-BRI-34	Ring Number Mask
PT-BRI-35	Enable Inbound Routing Information Field Filters on This Port
PT-BRI-36	Bridge Number
PT-BRI-37	Bridge Number Mask
PT-BRI-38	Select Route Designator
PT-BRI-39	Filter On
PT-BRI-400	Port Priority for Translational Bridging
PT-BRI-401	Override the Default Filter Order Set at the Node
PT-BRI-402	Override the Default Filter Order Set at the Node Level
PT-BRI-40	Filtering Mode of Inbound MAC Address Filters
PT-BRI-41	Frame Type of Inbound MAC Address Filter
PT-BRI-42	Source
PT-BRI-43	Destination
PT-BRI-44	Source Mask
PT-BRI-45	Destination MAC Address Mask
PT-BRI-46	Enable Inbound MAC Address Filters on This Port
PT-BRI-47	Form of MAC Address
PT-BRI-50	Frame Type of Inbound Hop Count Filter
PT-BRI-51	Hop Count of Inbound Hop Count Filter
PT-BRI-60	Filtering Mode of Inbound SNAP Filters
PT-BRI-62	SNAP Value
PT-BRI-63	SNAP Value Mask
PT-BRI-64	Enable Inbound SNAP Filters on This Port
PT-BRI-70	Filtering Mode of Outbound RI Field Filters

Table D-6 (Page 3 of 3). Source Route Bridging Parameter Labels

PT-BRI-71	Frame Type of Outbound RI Field Filter
PT-BRI-73	Ring Number
PT-BRI-74	Ring Number Mask
PT-BRI-75	Enable Outbound Routing Information Field Filters on This Port
PT-BRI-76	Bridge Number
PT-BRI-77	Bridge Number Mask
PT-BRI-78	Select Route Designator
PT-BRI-79	Filter On
PT-BRI-80	Filtering Mode of Outbound MAC Address Filters
PT-BRI-81	Frame Type of Outbound MAC Address Filter
PT-BRI-82	Source
PT-BRI-83	Destination
PT-BRI-84	Source Mask
PT-BRI-85	Destination Mask
PT-BRI-86	Enable Outbound MAC Address Filters on This Port
PT-BRI-87	Form of MAC Address
PT-BRI-90	Filtering Mode of Outbound SNAP Filters
PT-BRI-92	SNAP Value
PT-BRI-93	SNAP Value Mask
PT-BRI-94	Enable Outbound SNAP Filters on This Port

Node Management Configuration Parameters

For descriptions of these configuration parameters, refer to Chapter 6 on page 6-1.

Table D-7 (Page 1 of 2). Node Management Configuration Parameter Labels

BX-CFG-01	Host IP Address
BX-CFG-02	Address Mask
BX-CFG-03	Hosts That Can Perform Configuration Function on this Router
BX-CFG-04	Apply Configuration
BX-CFG-05	Year
BX-CFG-06	Month
BX-CFG-07	Day
BX-CFG-08	Hour
BX-CFG-09	Minute
BX-CFG-10	Enable Configuration Auto Roll Back Function
BX-CFG-11	Delay before testing
BX-CFG-12	Maximum test attempts
BX-CFG-13	Test frame timeout
BX-CFG-14	Test interval
BX-CFG-15	Test all IP stations before rolling back
BX-CFG-16	Configuration for auto roll back
BX-CFG-17	IP station address
BX-DNAME-01	IBM 6611 Domain Name
BX-HOST-01	IBM 6611 Host Name
BX-LOCK-01	Lock Value
BX-RHOST-01	Host Name
BX-RHOST-02	IP Address of Host
BX-RNAME-01	IP Address of Name Server
BX-RNAME-02	Enable Name Resolution by Remote Name Servers
BX-RTIME-01	IP Address of Remote Time Server
BX-RTIME-02	Enable Time Service by Remote Time Servers
BX-SRV-01	Service Name
BX-SRV-02	Description
BX-SRV-03	Display Control
BX-SRV-04	Connection Type
BX-SRV-05	Service Node Name
BX-SRV-06	Service IP Address
BX-SRV-07	ARC Server IP Address
BX-TTY-01	BAUD Rate for S1 Serial Port
BX-TTY-02	BAUD Rate for S2 Serial Port
BX-UPGRADE-sourcereleasec	Source Release
BX-USER-01	Controlling user ID
BX-USER-02	Password
BX-USER-03	Viewing user ID

Table D-7 (Page 2 of 2). Node Management Configuration Parameter Labels

BX-USER-04	Password
BX-USER-05	User ID
BX-USER-06	Password
PT-TTY-01	Baud Rate
PT-TTY-02	Parity
PT-TTY-03	Character Size (bit)
PT-TTY-04	Number of Stop Bits
PT-TTY-05	XON-XOFF Handshaking
PT-TTY-06	Start Character
PT-TTY-07	Stop Character
PT-TTY-08	Port Usage
PT-TTY-09	Inactivity Check
PT-TTY-10	Inactivity Period
PT-TTY-11	Port Identifier
PT-TTY-12	Port Password
PT-TTY-13	Enable Asychronous Interface On This Port
PT-TTY-14	User Interface
PT-TTY-15	Automatic Connection Service Name
PT-TTY-16	Terminal Type
PT-TTY-17	Sessions Allowed
PT-TTY-18	Menu Key
PT-TTY-19	Help Key
PT-TTY-20	Erase Character
PT-TTY-21	Menu Prompt
PT-TTY-22	Service Name
PT-TTY-23	Connection Timeout (seconds)

DECnet Parameters

For descriptions of these configuration parameters, refer to "Node Level Worksheets" on page 5-264 and "Port Level Worksheets" on page 5-269.

Table D-8. DECnet Parameter Labels

BX-DEC-01	Enable DECnet
BX-DEC-02	Local DECnet Address
BX-DEC-03	Node Type
BX-DEC-04	Maximum Cost (Area)
BX-DEC-05	Maximum Hops (Area)
BX-DEC-06	Maximum Address
BX-DEC-07	Maximum Area
BX-DEC-08	Maximum Cost (Routing-IV)
BX-DEC-09	Maximum Hops (Routing-IV)
BX-DEC-11	Maximum Visits
BX-DEC-13	Non-Routers (Maximum Broadcast)
BX-DEC-14	Routers (Maximum Broadcast)
BX-DEC-15	Routing Buffer Size
BX-DEC-16	Filter ID
BX-DEC-17	Filter Type
BX-DEC-18	Filtering Mode
BX-DEC-19	Filter DECnet Address 1
BX-DEC-20	Filter Mask 1
BX-DEC-21	Filter DECnet Address 2
BX-DEC-22	Filter Mask 2
BX-DEC-23	All Routers (Token Ring Functional Address)
BX-DEC-24	All End Nodes (Token Ring Functional Address)
BX-DEC-25	Enable Split Horizon with Poison Reverse
PT-DEC-01	Enable DECnet Routing on This Port
PT-DEC-02	Circuit Cost
PT-DEC-03	Hello Timer
PT-DEC-04	Router Priority
PT-DEC-05	Routing Timer
PT-DEC-06	Maximum Routers
PT-DEC-07	Remote DECnet Address
PT-DEC-08	Remote DECnet Node Type
PT-DEC-09	Filter ID
PT-DEC-10	Direction in Which Packet Is Moving
PT-DEC-12	Enable DECnet Filters on This Port
PT-DEC-13	DECnet Circuit Type
PT-DEC-20	Destination DECnet Address
PT-DEC-21	Destination DECnet Node Type
PT-DEC-22	DLCI Number

DLSw Parameters

For descriptions of these configuration parameters, refer to "Node Level Worksheets" on page 5-350.

Table D-9. DLSw Parameter Labels

BX-DLS-01	Enable SNA DLSw
BX-DLS-02	Enable NetBIOS DLSw
BX-DLS-03	Virtual Ring Segment Number
BX-DLS-04	IP Address of Remote 6611 Router
BX-DLS-05	Accept Connections From Specific IBM 6611s Only
BX-DLS-06	Destination Cache Timeout
BX-DLS-07	Default DLSw IP Address for this 6611

EGP Parameters

For descriptions of these configuration parameters, refer to "Node Level Worksheets" on page 5-148.

Table D-10. EGP Parameter Labels
Table D-10. EGP Parameter Labels

BX-EGP-01	Enable Exterior Gateway Protocol (EGP)
BX-EGP-02	Preference
BX-EGP-03	Default Metric
BX-EGP-06	Neighbor ASN
BX-EGP-08	Maximum Active Neighbors
BX-EGP-09	Preference
BX-EGP-11	Default Metric
BX-EGP-12	Generate Default from This Neighbor Group
BX-EGP-13	Import Default Route
BX-EGP-14	Export Default Route
BX-EGP-15	Next Hop Address or Domain Name
BX-EGP-18	Minimum Hello Interval
BX-EGP-19	Minimum Polling Interval
BX-EGP-20	EGP Neighbor IP Address
BX-EGP-21	Default Metric
BX-EGP-22	Generate Defaults from This Neighbor
BX-EGP-23	Import Default Route
BX-EGP-24	Export Default Route
BX-EGP-28	Minimum Hello Interval
BX-EGP-29	Minimum Polling Interval
BX-EGP-30	EGP Group Name
BX-EGPIMP-01	Autonomous System Number
BX-EGPIMP-02	Restrict
BX-EGPIMP-03	Preference
BX-EGPIMP-04	Destination
BX-EGPIMP-05	Destination Mask
BX-EGPIMP-06	Restrict Routes
BX-EGPIMP-07	Preference
BX-EGPIMP-08	Enable EGP Import Filters
BX-EGPIMP-09	Destination address

Export Filter Parameters

For descriptions of these configuration parameters, refer to "Node Level Worksheet" on page 5-208.

Table D-11 (Page 1 of 2). Export Filter Parameter Labels

BX-EXP-02	To Protocol
BX-EXP-03	From
BX-EXP-04	Specific Route
BX-EXP-05	Mask
BX-EXP-06	Metric
BX-EXP-07	Restrict Export
BX-EXP-08	AS Number of Source Protocol
BX-EXP-09	Type (1 - 2) of Desitnation Protocol
BX-EXP-10	Tag (1 - 65536) of Destination Protocol
BX-EXP-11	AS Number of Destination Protocol
BX-EXP-14	AS Path Origin of Source Protocol
BX-EXP-15	AS Path Origin
BX-EXP-16	Route(s) to be Exported
BX-EXP-20	IP Address of Local Source Interface
BX-EXP-21	IP Address of Remote Source Router
BX-EXP-22	IP Address of Local Destination Interface

Table D-11 (Page 2 of 2). Export Filter Parameter Labels

BX-EXP-23	IP Address of Remote Destination Router
BX-EXP-24	Filter routes from
BX-EXP-25	Filter routes to

Hello Parameters

For descriptions of these configuration parameters, refer to "Node Level Worksheets" on page 5-158.

Table D-12. Hello Parameter Labels

BX-HELLO-01	Enable Hello
BX-HELLO-02	Broadcast
BX-HELLO-03	Route Preference
BX-HELLO-05	IP Address of Local Interface
BX-HELLO-06	Listen For Hello Updates
BX-HELLO-07	Send Hello Updates
BX-HELLO-09	IP Address of Trusted Router
BX-HELLO-11	IP Address of Source Router
BX-HIMP-01	Name of Import Filter
BX-HIMP-02	Destination
BX-HIMP-03	Destination Mask
BX-HIMP-04	Restrict From Routing Table
BX-HIMP-05	Preference
BX-HIMP-06	Filter Routes from
BX-HIMP-07	IP Address of Local Interface
BX-HIMP-08	IP Address of Remote Router
BX-HIMP-09	Destination Address

IP Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheets" on page 5-113 and "Node Level Worksheets" on page 5-124.

Table D-13 (Page 1 of 2). IP Parameter Labels

BX-IP-03	Connection Decay Interval
BX-IP-04	Enable IP Packet Filters
BX-IP-10	Destination Address
BX-IP-11	Destination Mask
BX-IP-12	Next Hop Router 2
BX-IP-13	Next Hop Router 3
BX-IP-14	Next Hop Router 1
BX-IP-15	Preference
BX-IP-16	Retain Route in Master Table
BX-IP-20	IP Filter ID
BX-IP-21	Filter Type
BX-IP-22	Filtering Mode
BX-IP-23	Filter IP Address 1
BX-IP-24	Filter Subnet Mask 1
BX-IP-25	Filter IP Address 2
BX-IP-26	Filter Subnet Mask 2
BX-IP-27	Protocol
BX-IP-28	Filter 1
BX-IP-29	Filter 2
BX-IP-30	Filter 3
BX-IP-31	Filter 4
BX-IP-32	Destination IP Address
PT-IP-01	IP Address
PT-IP-02	Subnet Mask
PT-IP-03	Max. Transmission Unit (MTU)
PT-IP-05	Destination IP Address
PT-IP-06	Destination IP Address
PT-IP-07	Enable IP Routing on this Port
PT-IP-08	Enable Inbound Port Filters
PT-IP-09	DLCI Number
PT-IP-10	Ethernet Framing for IP
PT-IP-21	Destination IP Address for X.25
PT-IP-22	Virtual Circuit Type
PT-IP-23	Logical Channel Number
PT-IP-24	Remote DTE Address
PT-IP-25	Receive Packet Size
PT-IP-26	Transmit Packet Size
PT-IP-27	Receive Packet Window Size
PT-IP-28	Transmit Packet Window Size
PT-IP-29	Closed User Group Index
PT-IP-300	Enable ICMP Address Mask Requests
PT-IP-30	CUG with Outgoing Access Index

Table D-13 (Page 2 of 2). IP Parameter Labels

PT-IP-31	RPOA Indexes
PT-IP-32	User-Defined Facilities
PT-IP-33	Enable IP Priority
PT-IP-34	Default Priority for IP
PT-IP-35	IP Port Number
PT-IP-36	Priority
PT-IP-37	Port Type
PT-IP-39	Protocol
PT-IP-407	Assignment for Discovered DLCIs
PT-IP-408	Directed Broadcast
PT-IP-409	IP Point-to-Point Destination
PT-IP-40	Protocol Well-Known Ports
PT-IP-410	DLCI Number
PT-IP-411	Point-to-Point Only
PT-IP-41	Enable Transmission Group for IP on This Port
PT-IP-42	Filter 1
PT-IP-43	Filter 2
PT-IP-44	Filter 3
PT-IP-45	Filter 4
PT-IP-50	Filter ID
PT-IP-51	Filter Type
PT-IP-52	Filtering Mode
PT-IP-53	Filter IP Address 1
PT-IP-54	Filter Subnet Mask 1
PT-IP-55	Filter IP Address 2
PT-IP-56	Filter Subnet Mask 2
PT-IP-58	Enable UDP Broadcast Forwarding
PT-IP-59	Target UDP Port IP Address
PT-IP-60	UDP Port

IPX Parameters

For descriptions of these configuration parameters, refer to “Port Level Worksheets” on page 5-285 and “Node Level Worksheets” on page 5-297

Table D-14 (Page 1 of 2). IPX Parameter Labels

BX-IPX-01	Enable Internetwork Packet Exchange (IPX) Router
BX-IPX-03	Server Name
BX-IPX-04	Name
BX-IPX-05	Server Type
BX-IPX-06	Type
BX-IPX-07	Network Number
BX-IPX-08	Network
BX-IPX-09	Filtering Mode
BX-IPX-10	Filtering Mode (Inbound RIP)
BX-IPX-11	Local IPX Network to Filter On
BX-IPX-12	Network Numbers to Filter On
BX-IPX-13	Network Number
BX-IPX-14	Filter ID
BX-IPX-20	Filtering Mode (Outbound RIP)
BX-IPX-21	Local IPX Network to Filter On
BX-IPX-22	Network Numbers to Filter On (Outbound RIP)
BX-IPX-23	Network Number
BX-IPX-24	Filter ID
BX-IPX-30	Filtering Mode
BX-IPX-31	Filter ID
BX-IPX-32	Network Numbers to Filter On
BX-IPX-33	Network Number
BX-IPX-34	Host Address to Filter On
BX-IPX-35	Host Address
BX-IPX-40	Enable SAP Filters
BX-IPX-41	Enable Inbound RIP Filters
BX-IPX-42	Enable Outbound RIP Filters
BX-IPX-43	Enable RIP Router Filters
BX-IPX-50	Filter ID
BX-IPX-60	IPX Internal Network Number
BX-IPX-61	IPX Router Name
BX-IPX-62	Lower Limit
BX-IPX-63	Upper Limit
BX-IPX-401	Slot Number
BX-IPX-402	Port Number
BX-IPX-411	Slot Number
BX-IPX-412	Port Number
BX-IPX-421	Slot Number
BX-IPX-422	Port Number
PT-IPX-01	IPX Network Number

Table D-14 (Page 2 of 2). IPX Parameter Labels

PT-IPX-02	Enable IPX Routing on This Port
PT-IPX-03	Destination IPX Address
PT-IPX-04	DLCI Number
PT-IPX-05	Encapsulation Method (Token-Ring Port)
PT-IPX-07	Filtering Mode
PT-IPX-10	Enable Hop Count
PT-IPX-11	Hop Count
PT-IPX-12	Relational Compare Operator
PT-IPX-13	Enable Packet Type
PT-IPX-14	Packet Type
PT-IPX-15	Enable Destination Network
PT-IPX-16	Destination Network
PT-IPX-17	Enable Destination Host
PT-IPX-18	Destination Host
PT-IPX-19	Enable Destination Socket
PT-IPX-20	Destination Socket
PT-IPX-21	Enable Source Network
PT-IPX-22	Source Network
PT-IPX-23	Enable Source Host
PT-IPX-24	Source Host
PT-IPX-25	Enable Source Socket
PT-IPX-26	Source Socket
PT-IPX-30	Software Loopback Active
PT-IPX-32	Filter ID
PT-IPX-33	Encapsulation Method (Ethernet Port)
PT-IPX-400	Destination IPX Address for X.25
PT-IPX-401	Virtual Circuit Type
PT-IPX-402	Logical Channel Number
PT-IPX-403	Remote DTE Address
PT-IPX-404	Receive Packet Size
PT-IPX-405	Transmit Packet Size
PT-IPX-406	Receive Packet Window Size
PT-IPX-407	Transmit Packet Window Size
PT-IPX-408	Closed User Group Index
PT-IPX-409	Closed User Group with Outgoing Access Index
PT-IPX-40	Enable Inbound Port Filters
PT-IPX-410	RPOA Indices (1-10 indices of 4 decimal digits)
PT-IPX-411	User-Defined Facilities
PT-IPX-412	Single LCN Session
PT-IPX-413	Recall Time
PT-IPX-416	SVC Inactivity Timer
PT-IPX-417	Split Horizon for RIP and SAP Updates
PT-IPX-44	SAP Age Multiplier
PT-IPX-45	SAP Update Interval
PT-IPX-46	RIP Age Multiplier
PT-IPX-47	RIP Update Interval
PT-IPX-48	Enable SAP and RIP Pacing
PT-IPX-62	Enable Tick Override
PT-IPX-63	Tick Override
PT-IPX-65	Enable IPXWAN

ISDN Parameters

For descriptions of these configuration parameters, refer to the documentation associated with PRPQs P85400, P85402, P85401, and P85403.

Table D-15 (Page 1 of 2). ISDN Parameter Labels

BX-ISDN-01	Filter ID
PT-ISDN-301	Enable ISDN on This Port
PT-ISDN-302	Inactivity Timeout
PT-ISDN-303	ISDN Dialout Number
PT-ISDNA-501	Enable Physical Interface on This Port
PT-ISDNA-502	Adapter Type
PT-ISDNA-503	Casual
PT-ISDNA-504	Backup
PT-ISDNA-505	Network Type
PT-ISDNA-506	Non-automatic TEI
PT-ISDNA-507	TEI
PT-ISDNA-508	Call Number
PT-ISDNA-509	Line Speed
PT-ISDNA-510	Destination Call Number
PT-ISDNA-512	Acceptable Call Numbers
PT-ISDNA-514	Auto-disconnect Timeout
PT-ISDNA-515	Destination IP Address for ISDN

Table D-15 (Page 2 of 2). ISDN Parameter Labels

PT-ISDNA-516	Virtual Circuit Type
PT-ISDNA-517	Bearer Channel Number
PT-ISDNA-518	Data Link Protocol
PT-ISDNA-519	High Priority Queue
PT-ISDNA-520	Medium Priority Queue
PT-ISDNA-521	Low Priority Queue
PT-ISDNA-522	High Priority Queue
PT-ISDNA-523	Medium Priority Queue
PT-ISDNA-524	Low Priority Queue
PT-ISDNA-525	Locally Administered MAC Address
PT-ISDNA-526	Backup Destination IP Address
PT-ISDNA-527	Backup Destination Call Number

NetBIOS Parameters

For descriptions of these configuration parameters, refer to “Port Level Worksheet” on page 5-356 and “Node Level Worksheets” on page 5-357.

Table D-16. NetBIOS Parameter Labels

BX-NETB-02	Filtering Mode of Destination Name Filters
BX-NETB-03	Destination Name of Source Name Filters
BX-NETB-04	Filtering Mode
BX-NETB-05	Source Name
BX-NETB-06	Destination Name
BX-NETB-07	IP Address of Destination Router
BX-NETB-08	Source Name
BX-NETB-09	Destination Name
BX-NETB-10	Enable Destination Name Filters
BX-NETB-11	Enable Source Name Filters
BX-NETB-13	Maximum NetBIOS Frame Size
PT-NETB-01	Forward NetBIOS Frames
PT-NETB-02	Forward NetBIOS Datagram and Datagram Broadcast Messages

OSPF Parameters

For descriptions of these configuration parameters, refer to “Node Level Worksheets” on page 5-177.

Table D-17. OSPF Parameter Labels

BX-GATED-01	Local Autonomous System Number
BX-GATED-02	Generate Default Route
BX-GATED-03	Router ID
BX-OSPF-04	ASE Route Preference
BX-OSPF-10	Area ID
BX-OSPF-11	Area Type
BX-OSPF-12	Stub Cost
BX-OSPF-13	Authentication Type
BX-OSPF-20	Virtual Neighbor ID
BX-OSPF-21	Transit Area ID
BX-OSPF-22	Retransmit Interval
BX-OSPF-23	Interface Transit Delay
BX-OSPF-24	Hello Interval
BX-OSPF-25	Router Dead Interval
BX-OSPF-26	Authorization Key
BX-OSPF-27	Virtual Link ID
BX-OSPF-30	Network Number
BX-OSPF-31	Network Mask
BX-OSPF-32	Advertise Network Range
BX-OSPF-40	IP Address of Neighbor Router
BX-OSPF-41	Eligible to Become Designated Router
BX-OSPF-50	Interface IP Address
BX-OSPF-51	Retransmit Interval
BX-OSPF-52	Interface Transit Delay
BX-OSPF-53	Router Priority
BX-OSPF-54	Hello Interval
BX-OSPF-55	Router Dead Interval
BX-OSPF-56	Authorization Key
BX-OSPF-57	Cost
BX-OSPF-58	Poll Interval
BX-OSPF-59	Interface Type

RIP Parameters

For descriptions of these configuration parameters, refer to "Node Level Worksheets" on page 5-189.

Table D-18. RIP Parameter Labels

BX-RIMP-01	Name of Import Filter
BX-RIMP-02	Destination
BX-RIMP-03	Destination Mask
BX-RIMP-04	Restrict
BX-RIMP-05	Preference
BX-RIMP-06	Filter Routes From
BX-RIMP-07	IP Address of Local Interface
BX-RIMP-08	IP Address of Remote Router
BX-RIMP-09	Destination Address
BX-RIP-01	Enable Routing Information Protocol (RIP)
BX-RIP-02	Broadcast
BX-RIP-03	Zero Reserved Fields
BX-RIP-04	Route Preference
BX-RIP-06	IP Address of Local Interface
BX-RIP-07	Listen for RIP Updates
BX-RIP-08	Send RIP Updates
BX-RIP-10	IP Address of Trusted Router
BX-RIP-12	IP Address of Source Router
BX-RIP-301	Metric In
BX-RIP-302	Metric Out
BX-RIP-303	Version
BX-RIP-304	Broadcast Mode
BX-RIP-305	Local IP Address Interface

SNA Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheets" on page 5-361 and "Node Level Worksheets" on page 5-361.

Table D-19. SNA Parameter Labels

BX-SNA-02	Filtering Mode of Source Frame Filters
BX-SNA-03	Source Address
BX-SNA-04	Source Address Mask
BX-SNA-05	Destination Address
BX-SNA-06	Destination Address Mask
BX-SNA-07	Filter Mode of Destination Frame Filters
BX-SNA-08	Source Address
BX-SNA-09	Source Address Mask
BX-SNA-10	Destination Address
BX-SNA-11	Destination Address Mask
BX-SNA-12	Dest. MAC Address
BX-SNA-13	IP Address of Destination Router
BX-SNA-16	SNA Transmission Bias
BX-SNA-20	Enable SNA Source Frame Filters
BX-SNA-21	Enable SNA Destination Frame Filters
PT-SNA-01	SAP Value
PT-SNA-02	Enable SNA Frame Forwarding on This Port

SNMP Parameters

For descriptions of these configuration parameters, refer to "SNMP Worksheets" on page 6-3.

Table D-20 (Page 1 of 2). SNMP Parameter Labels

BX-SNMP-01	Enable SNMP
BX-SNMP-02	System Contact
BX-SNMP-03	System Name
BX-SNMP-04	System Location
BX-SNMP-05	Enterprise-Specific Trap Throttle Time
BX-SNMP-06	Community Name
BX-SNMP-07	Community IP Address or Domain Name
BX-SNMP-08	Community Address Mask
BX-SNMP-09	Community Access
BX-SNMP-10	Community View Name
BX-SNMP-11	View Name
BX-SNMP-12	MIB Subtree
BX-SNMP-13	Trap Community Name
BX-SNMP-14	Trap Address (IP Address or Domain Name)

Table D-20 (Page 2 of 2). SNMP Parameter Labels

BX-SNMP-15	Enable ColdStart Trap
BX-SNMP-16	Enable WarmStart Trap
BX-SNMP-17	Enable LinkDown Trap
BX-SNMP-18	Enable LinkUp Trap
BX-SNMP-19	Enable AuthenticationFailure Trap
BX-SNMP-20	Enable EGPNeighborLoss Trap
BX-SNMP-21	Enable Enterprise-Specific Trap
BX-SNMP-22	Router Serial Number - Prefix
BX-SNMP-23	Router Serial Number - Suffix

Translational Bridging Parameters

For descriptions of these configuration parameters, refer to “Port Level Worksheets” on page 5-89 and “Node Level Worksheets” on page 5-94.

Table D-21. Translational Bridging Parameter Labels

BX-SRTB-BRI-400	Enable Translational Bridging
BX-SRTB-BRI-401	Route Discovery Mode
BX-SRTB-BRI-403	Bridge Number
BX-SRTB-BRI-404	Enable LAN Bridging Protocol
BX-SRTB-BRI-405	Designated Ring Number
BX-SRTB-BRI-410	Map Token-Ring to Ethernet Addresses
BX-SRTB-BRI-411	Convert Token-Ring to Ethernet Broadcast Address
BX-SRTB-BRI-412	Token Ring (Address)
BX-SRTB-BRI-413	Ethernet (Address)
BX-SRTB-BRI-414	Description
BX-SRTB-BRI-420	Mode of Translation between Token Ring and Ethernet
BX-SRTB-BRI-421	Mode Priority
BX-SRTB-BRI-422	Transmit Multicast As Both Ethernet V2.0 and Ethernet 802.3
BX-SRTB-BRI-423	Enable Encapsulation of LLC-Based Protocols in Ethernet V2.0
BX-SRTB-BRI-424	SAP Enabled for LLC-on-Ethernet V2.0 Encapsulation
BX-SRTB-BRI-425	Description of This SAP
BX-SRTB-BRI-430	Enable ARP/RARP Conversion
BX-SRTB-BRI-440	Enable IPX Conversion
BX-SRTB-BRI-441	Enable AppleTalk Conversion
BX-SRTB-BRI-450	Form of MAC Address
BX-SRTB-BRI-451	Duplicate Address Check
BX-SRTB-BRI-452	Overflow Policy
BX-SRTB-BRI-453	Aging Time
BX-SRTB-BRI-454	Static Destination MAC Address
BX-SRTB-BRI-460	Bridge Priority
BX-SRTB-BRI-461	Hello Time
BX-SRTB-BRI-462	Forward Delay
BX-SRTB-BRI-463	Max Age
BX-SRTB-BRI-470	Hop Count Filter
BX-SRTB-BRI-471	Source SAP Filter
BX-SRTB-BRI-472	Ethernet/SNAP Type Filter
BX-SRTB-BRI-473	RI Field Filter
BX-SRTB-BRI-474	MAC Address Filter
BX-SRTB-BRI-475	Sliding Window Filter
PT-SRT-BRI-400	Enable Dual Mode Bridging on This Port
PT-SRT-BRI-401	Port Priority
PT-SRT-BRI-402	Spanning Tree Mode
PT-SRT-BRI-403	Port State
PT-SRT-BRI-404	Path Cost
PT-SRT-BRI-405	Emulated Ring Number
PT-SRT-BRI-406	Emulated Ring Number
PT-SRT-BRI-407	DLCI Number
PT-SRT-BRI-408	Maximum Transmission Unit

Transparent Bridging Parameters

For descriptions of these configuration parameters, refer to “Port Level Worksheets” on page 5-55 and “Node Level Worksheets” on page 5-71.

Table D-22 (Page 1 of 3). Transparent Bridging Parameter Labels

BX-TBRI-01	Enable Transparent Bridging
BX-TBRI-02	Form of MAC Address
BX-TBRI-04	Duplicate Address Check
BX-TBRI-05	Bridge Priority

Table D-22 (Page 2 of 3). Transparent Bridging Parameter Labels

BX-TBRI-06	Max Age
BX-TBRI-07	Hello Time
BX-TBRI-08	Forward Delay
BX-TBRI-09	Aging Time
BX-TBRI-10	Overflow Policy
BX-TBRI-11	Static Destination MAC Address
BX-TBRI-12	Source SAP Filter
BX-TBRI-13	Ethernet Type Filter
BX-TBRI-14	MAC Address Filter
BX-TBRI-15	Sliding Window Filter
PT-TBRI-01	Enable Transparent Bridging on this Port
PT-TBRI-03	DLCI Number
PT-TBRI-04	Port Priority
PT-TBRI-05	Port State
PT-TBRI-06	Spanning Tree Mode
PT-TBRI-07	Path Cost
PT-TBRI-08	Maximum Transmission Unit Size
PT-TBRI-10	Filtering Mode
PT-TBRI-11	Source SAP Value
PT-TBRI-12	Filtering Mode of Inbound MAC Address Filters
PT-TBRI-13	Source MAC Address
PT-TBRI-14	Destination MAC Address
PT-TBRI-15	Source MAC Address Mask
PT-TBRI-16	Destination MAC Address Mask
PT-TBRI-17	Filtering Mode of Inbound Ethernet Type Filters
PT-TBRI-18	Type Field
PT-TBRI-19	Type Mask
PT-TBRI-20	Filtering Mode of Outbound Source SAP Filters
PT-TBRI-21	Source SAP Value
PT-TBRI-22	Filtering Mode of Outbound MAC Address Filter
PT-TBRI-23	Source MAC Address
PT-TBRI-24	Destination MAC Address
PT-TBRI-25	Source MAC Address Mask
PT-TBRI-26	Destination MAC Address Mask
PT-TBRI-27	Filtering Mode of Outbound Ethernet Type Filters

Table D-22 (Page 2 of 3). Transparent Bridging Parameter Labels

PT-TBRI-28	Type Field
PT-TBRI-29	Type Mask
PT-TBRI-31	Form of MAC Addresses
PT-TBRI-32	Form of MAC Addresses
PT-TBRI-38	Filter Name
PT-TBRI-39	Filter Name
PT-TBRI-400	Emulated Ring Number
PT-TBRI-401	Emulated Ring Number
PT-TBRI-402	Override the Default Filter Order Set at the Node
PT-TBRI-403	Override the Default Filter Order Set at the Node
PT-TBRI-40	Enable Inbound Sliding Window Filters on This Port
PT-TBRI-41	Filtering Mode of Inbound Sliding Window Filters
PT-TBRI-43	Offset into Frame
PT-TBRI-44	Sliding Window Contents
PT-TBRI-45	Sliding Window Mask
PT-TBRI-46	Inbound Source SAP Filter Order
PT-TBRI-47	Inbound Ethernet Type Filter Order
PT-TBRI-48	Inbound MAC Address Filter Order
PT-TBRI-49	Inbound Sliding Window Filter Order
PT-TBRI-50	Enable Outbound Sliding Window Filters on This Port
PT-TBRI-51	Filtering Mode of Outbound Sliding Window Filters
PT-TBRI-53	Offset into Frame
PT-TBRI-54	Sliding Window Contents
PT-TBRI-55	Sliding Window Mask
PT-TBRI-56	Outbound Source SAP Filter Order
PT-TBRI-57	Outbound Ethernet Type Filter Order
PT-TBRI-58	Outbound MAC Address Filter Order
PT-TBRI-59	Outbound Sliding Window Filter Order
PT-TBRI-60	Enable Inbound Source SAP Filters on This Port
PT-TBRI-61	Enable Inbound MAC Address Filters on This Port

Table D-22 (Page 3 of 3). Transparent Bridging Parameter Labels

PT-TBRI-62	Enable Inbound Ethernet Type Filters on This Port
PT-TBRI-63	Enable Outbound Source SAP Filters on This Port
PT-TBRI-64	Enable Outbound MAC Address Filters on This Port
PT-TBRI-65	Enable Outbound Ethernet Type Filters on This Port
PT-TBRI-68	Offset Starting Field
PT-TBRI-69	Offset Starting Field

VINES Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheets" on page 5-311 and "Node Level Worksheets" on page 5-319.

Table D-23 (Page 1 of 2). VINES Parameter Labels

BX-VINES-01	Enable VINES Router
BX-VINES-03	VINES Network Number
BX-VINES-05	VINES Routing Server Name
BX-VINES-10	Filtering Mode of Inbound RTP Filters
BX-VINES-12	VINES Networks To Filter
BX-VINES-13	VINES Network Number
BX-VINES-14	Filter ID
BX-VINES-15	Slot Number
BX-VINES-16	Port Number
BX-VINES-20	Filtering Mode of Outbound RTP Filters
BX-VINES-22	VINES Networks To Filter
BX-VINES-23	VINES Network Number
BX-VINES-24	Filter ID
BX-VINES-25	Slot
BX-VINES-26	Port
BX-VINES-30	Filtering Mode of RTP Router Filters
BX-VINES-31	Filter ID
BX-VINES-32	VINES Networks to Filter
BX-VINES-33	VINES Network Number
BX-VINES-41	Enable Inbound RTP Filters
BX-VINES-42	Enable Outbound RTP Filters
BX-VINES-43	Enable RTP Router Filters
PT-VINES-01	Enable VINES Routing on This Port
PT-VINES-02	Encapsulation Method (Ethernet Port)
PT-VINES-03	Encapsulation Method (Token-Ring Port)
PT-VINES-04	Enable Inbound Port Filters
PT-VINES-05	Filtering Mode of Inbound Port Filters
PT-VINES-06	Enable Hop Count
PT-VINES-07	Hops
PT-VINES-08	Relational Compare Operator
PT-VINES-09	Enable Protocol Type
PT-VINES-10	Inbound Protocol Type
PT-VINES-11	Enable Destination Network
PT-VINES-12	Destination Network
PT-VINES-13	Enable Destination Subnetwork
PT-VINES-14	Destination Subnetwork
PT-VINES-15	Enable Destination Port
PT-VINES-16	Destination Port
PT-VINES-17	Enable Source Network
PT-VINES-18	Source Network
PT-VINES-19	Enable Source Subnetwork
PT-VINES-20	Source Subnetwork
PT-VINES-21	Enable Source Port
PT-VINES-22	Source Port
PT-VINES-23	Destination VINES Address
PT-VINES-24	DLCI Number
PT-VINES-25	Enable ARP
PT-VINES-26	Enable Serverless Support
PT-VINES-27	Neighbor Metric Override
PT-VINES-28	Filter ID
PT-VINES-29	Filter ID
PT-VINES-34	Enable Outbound Port Filters
PT-VINES-35	Filtering Mode of Outbound Port Filters
PT-VINES-36	Enable Hop Count
PT-VINES-37	Hops
PT-VINES-38	Relational Compare Operator

Table D-23 (Page 2 of 2). VINES Parameter Labels

PT-VINES-39	Enable Protocol Type
PT-VINES-40	Outbound Protocol Type
PT-VINES-41	Enable Destination Network
PT-VINES-42	Destination Network
PT-VINES-43	Enable Destination Subnetwork
PT-VINES-44	Destination Subnetwork
PT-VINES-45	Enable Destination Port
PT-VINES-46	Destination Port
PT-VINES-47	Enable Source Network
PT-VINES-48	Source Network
PT-VINES-49	Enable Source Subnetwork
PT-VINES-50	Source Subnetwork
PT-VINES-51	Enable Source Port
PT-VINES-52	Source Port
PT-VINES-61	VINES Destination Address
PT-VINES-62	Override Architected Neighbor Metric
PT-VINES-63	Distance to Server
PT-VINES-64	Enable Periodic Full Routing Updates

XNS Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheets" on page 5-328 and "Node Level Worksheets" on page 5-334.

Table D-24 (Page 1 of 2). XNS Parameter Labels

BX-XNS-01	Enable Xerox Network Systems (XNS) Router
BX-XNS-02	Split Horizon Window
BX-XNS-03	Enable Static Routes
BX-XNS-10	Filtering Mode of Inbound RIP Filters
BX-XNS-11	Local XNS Network to Filter On
BX-XNS-12	Network Numbers to Filter On
BX-XNS-13	Network Number
BX-XNS-14	Filter ID
BX-XNS-20	Filtering Mode of Outbound RIP Filters
BX-XNS-21	Local Network to Filter On

Table D-24 (Page 1 of 2). XNS Parameter Labels

BX-XNS-22	Network Numbers to Filter On
BX-XNS-23	Network Number
BX-XNS-24	Filter ID
BX-XNS-30	Filtering Mode of RIP Router Filters
BX-XNS-31	Filter ID
BX-XNS-32	Network Numbers to Filter On
BX-XNS-33	Network Number
BX-XNS-34	Host Address to Filter On
BX-XNS-35	Host Address
BX-XNS-41	Enable Inbound RIP Filters
BX-XNS-42	Enable Outbound RIP Filters
BX-XNS-43	Enable RIP Router Filters
BX-XNS-60	Destination Network Number
BX-XNS-62	Network Number of Next Hop Router
BX-XNS-63	Next Hop Router Host Address
PT-XNS-01	XNS Network Number
PT-XNS-02	Enable XNS Routing on This Port
PT-XNS-03	Destination XNS Address
PT-XNS-04	DLCI Number
PT-XNS-05	Encapsulation Method (Token-Ring Port)
PT-XNS-07	Filtering Mode
PT-XNS-08	Enable Checksum
PT-XNS-09	Checksum
PT-XNS-10	Enable Hop Count
PT-XNS-11	Hops
PT-XNS-12	Relational Compare Operator
PT-XNS-13	Enable Packet Type
PT-XNS-14	Packet Type Value
PT-XNS-15	Enable Destination Network
PT-XNS-16	Destination Network
PT-XNS-17	Enable Destination Host
PT-XNS-18	Destination Host
PT-XNS-19	Enable Destination Socket
PT-XNS-20	Destination Socket
PT-XNS-21	Enable Source Network
PT-XNS-22	Source Network Value
PT-XNS-23	Enable Source Host
PT-XNS-24	Source Host

Table D-24 (Page 2 of 2). XNS Parameter Labels

PT-XNS-25	Enable Source Socket
PT-XNS-26	Source Socket
PT-XNS-28	Error Protocol Active
PT-XNS-29	Error Protocol Packet Size
PT-XNS-32	Filter ID
PT-XNS-33	Encapsulation Method (Ethernet Port)
PT-XNS-40	Enable Inbound Port Filters

LAN Bridging Protocol Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheet" on page 4-24.

Table D-25. LAN Bridging Protocol Port Parameter Labels

PT-BNPPP-01	Bridge Performance Counter Threshold
PT-BNPPP-02	Telecommunications Link Error Threshold
PT-BNPPP-03	Auto Reboot on Error
PT-BNPPP-04	Memory Dump on Error
PT-BNPPP-05	Event Log Drive
PT-BNPPP-07	Enable LAN Bridging Protocol on This Port
PT-BNPPP-08	Enable Ring Parameter Server
PT-BNPPP-09	Enable Ring Error Monitor
PT-BNPPP-10	Enable Configuration Report Server
PT-BNPPP-11	Link Password 0
PT-BNPPP-12	Link Password 1
PT-BNPPP-13	Link Password 2
PT-BNPPP-14	Link Password 3
PT-BNPPP-300	Virtual MAC Address
PT-BNPPP-301	MAC Address Format
PT-BNPPP-302	Locally Administered Address

Ethernet Port Parameters

For descriptions of these configuration parameters, refer to "Worksheet" on page 4-36.

Table D-26. Ethernet Port Parameter Labels

PT-ET-01	Enable Physical Interface On This Port
PT-ET-02	MAC Address
PT-ET-03	Locally Administered Address
PT-ET-04	Enable Additional Multicast Addresses
PT-ET-05	Multicast MAC Address
PT-LNMLLC-400	Enable LNM Communication Through This Port

Frame-Relay Port Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheet" on page 4-16.

Table D-27. Frame Relay Port Parameter Labels

PT-FRM-01	DLCIs Assigned to This Port
PT-FRM-03	Polling Interval
PT-FRM-04	Full Inquiry Interval
PT-FRM-05	Local Management Interface (LMI) Option
PT-FRM-06	Use Inverse ARP (InARP) to Resolve Remote Protocol Addresses
PT-FRM-07	Enable Frame Relay On This Port

SDLC Port Parameters

For descriptions of these configuration parameters, refer to "Worksheets" on page 4-41.

Table D-28 (Page 1 of 2). SDLC Port Parameter Labels

PT-MUL-01	Enable Interface
PT-MUL-02	Physical Link Type
PT-MUL-03	Serial Encoding
PT-MUL-04	Request to Send
PT-MUL-05	Data Terminal Ready
PT-MUL-06	Bit Clocking
PT-MUL-07	Data Rate Select
PT-MUL-08	Transmit Rate
ST-MUL-01	Station Address

Table D-28 (Page 2 of 2). SDLC Port Parameter Labels

ST-MUL-02	Station Source MAC Address
ST-MUL-03	Station Destination MAC Address
ST-MUL-04	Transmit Window Count
ST-MUL-05	Retransmit Count
ST-MUL-06	Retransmit Threshold
ST-MUL-07	Force Disconnect Timeout
ST-MUL-08	Maximum I-Field Size
ST-MUL-09	Primary Repoll Timeout
ST-MUL-10	Primary Repoll Count
ST-MUL-11	Primary Repoll Threshold
ST-MUL-12	Primary Slow List Timeout
ST-MUL-13	Station Source SAP
ST-MUL-14	Station Token-Ring Destination SAP
ST-MUL-15	Station XID Value
ST-MUL-400	Station Type 2.1
ST-MUL-401	Secondary SDLC Address for 6611

PPP Port Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheets" on page 4-32.

Table D-29. PPP Port Parameter Labels

PT-PPP-01	Maximum Receive Unit
PT-PPP-04	Select Link Quality Monitoring Method
PT-PPP-05	Link Quality Monitoring Interval
PT-PPP-08	Enable Point-to-Point Protocol (PPP) on This Port
PT-PPP-09	Use Magic-number for Loopback Detection
PT-PPP-12	Allowable Number of Lost Link Quality Reports
PT-PPP-13	Allowable Percentage of Lost Packets
PT-PPP-14	Allowable Percentage of Lost Octets
PT-PPP-15	Allowable Number of Lost LCP Pings
PT-PPP-16	LCP Ping Timeout
PT-PPP-17	Enable Allowable Number of Lost Link Quality Reports
PT-PPP-18	Enable Allowable Percentage of Lost Packets
PT-PPP-19	Enable Allowable Percentage of Lost Octets
PT-PPP-20	Number of Successful LCP Pings for Recovery

Serial Port Parameters

For descriptions of these configuration parameters, refer to "Worksheets" on page 4-3.

Table D-30. Serial Port Parameter Labels

PT-SE-01	Enable Physical Interface On This Port
PT-SE-02	Data Link Protocol
PT-SE-03	Cylink Serial Number
PT-SE-04	Data Encoding
PT-SE-05	Locally Administered MAC Address
PT-SE-06	Serial Line Speed
PT-SE-08	Link Bandwidth Allocation for High Priority Queue
PT-SE-09	Link Bandwidth Allocation for Medium Priority Queue
PT-SE-10	Link Bandwidth Allocation for Low Priority Queue
PT-SE-11	Queue Bandwidth Reservation for High Priority Queue
PT-SE-12	Queue Bandwidth Reservation for Medium Priority Queue
PT-SE-13	Queue Bandwidth Reservation for Low Priority Queue
PT-SE-400	Interface Cable
PT-SE-402	Transmit Clock Source
PT-TG-01	Enable Port Transmission Group
PT-TG-02	Transmission Group (TG) name
PT-LNMLLC-400	Enable LNM Communication Through This Port

SMDS Parameters

For descriptions of these configuration parameters, refer to the documentation associated with PRPQ P85417.

Table D-31. SMDS Parameter Labels

BX-SMDS-01	Enable SMDS
PT-BRI-500	Ring Number
PT-BRI-501	E.164 Address
PT-SMDS-01	Enable SMDS on This Port
PT-SMDS-04	SMDS Individual Address
PT-SMDS-05	SMDS Group Address
PT-SRT-BRI-500	Emulated Ring Number
PT-SRT-BRI-501	E.164 Address
PT-TBRI-500	Ring Number
PT-TBRI-501	E.164 Address

Token-Ring Port Parameters

For descriptions of these configuration parameters, refer to "Worksheets" on page 4-46.

Table D-32. Token-Ring Port Parameter Labels

PT-TR-01	Enable Physical Interface On This Port
PT-TR-02	MAC Address
PT-TR-03	Locally Administered Address
PT-TR-04	Token-Ring Data Rate
PT-TR-06	MAC Address Format
PT-TR-07	Broadcast type
PT-TRLNM-300	Enable LNM To Manage This Port
PT-TRLNM-301	Virtual MAC Address
PT-TRLNM-302	MAC Address Format
PT-TRLNM-303	Locally Administered Address
PT-TRLNM-304	Link Password 0
PT-TRLNM-305	Link Password 1
PT-TRLNM-306	Link Password 2
PT-TRLNM-307	Link Password 3
PT-TRLNM-308	Bridge Performance Counter Threshold
PT-TRSURR-300	Enable Ring Error Monitor

Table D-32. Token-Ring Port Parameter Labels

PT-TRSURR-301	Enable Configuration Report Server
PT-TRSURR-302	Enable Ring Parameter Server
PT-TRSURR-303	Token Ring Segment Number
PT-LNMLLC-400	Enable LNM Communication Through This Port

X.25 Port Parameters

For descriptions of these configuration parameters, refer to "Port Level Worksheets" on page 4-62.

Table D-33 (Page 1 of 2). X.25 Port Parameter Labels

PT-X25-01	Local DTE Address
PT-X25-02	Network Identifier
PT-X25-04	SVC Incoming - Lowest Number
PT-X25-05	SVC Incoming Number of Channels
PT-X25-06	SVC 2-Way Lowest Number
PT-X25-07	SVC 2-Way Number of Channels
PT-X25-08	SVC Outgoing Lowest Number
PT-X25-09	SVC Outgoing Number of Channels
PT-X25-10	PVC Lowest Number
PT-X25-113	Enable X.25 Interface on This Port
PT-X25-114	Calling Address in Incoming Call Packets
PT-X25-115	Country Code
PT-X25-11	PVC Number of Channels
PT-X25-12	Auto-Call Unit
PT-X25-13	Auto-Call Unit Disconnection Timeout
PT-X25-14	CCITT Support
PT-X25-15	Packet Modulo
PT-X25-16	Type of Line
PT-X25-17	Receive Packet Size
PT-X25-18	Transmit Packet Size
PT-X25-19	Receive Packet Window
PT-X25-20	Transmit Packet Window
PT-X25-300	Automatic Link Restart
PT-X25-32	T24 Timer

Table D-33 (Page 2 of 2). X.25 Port Parameter Labels

PT-X25-33	T25 Timer
PT-X25-36	Packet Size and Packet Window Size Negotiation
PT-X25-37	Allow Incoming Calls
PT-X25-38	Allow Outgoing Calls
PT-X25-39	Allow Fast Select
PT-X25-401	Locally Administered MAC Address
PT-X25-41	Max Number of Reset Packets
PT-X25-42	Max Number of Clear Packets
PT-X25-43	Closed User Group
PT-X25-45	Allow Reverse Charging
PT-X25-47	Include Calling Address in Call Request Packets
PT-X25-48	Packet Size Negotiation Facility
PT-X25-49	Packet Window Size Negotiation Facility
PT-X25-51	Basic Format
PT-X25-52	Extended Format
PT-X25-53	CUG with OA Selection Facility - Basic Format
PT-X25-54	CUG with OA Selection Facility - Extended Format
PT-X25-56	Reverse Charging Facility
PT-X25-70	Frame Window Size
PT-X25-71	T1 Timer
PT-X25-72	T4 Timer
PT-X25-73	N2 Counter
PT-X25-74	Connection Mode
PT-X25-75	Startup Counter
PT-X25-76	Poll Timer
PT-X25-78	Frame Modulo
PT-X25-79	Receive Packet Size
PT-X25-80	Transmit Packet Size
PT-X25-81	Receive Packet Window
PT-X25-82	Transmit Packet Window
PT-X25-84	Autoreset Value
PT-X25-86	Logical Channel Number
PT-X25-87	Receive Packet Size
PT-X25-88	Transmit Packet Size
PT-X25-89	Receive Packet Window
PT-X25-90	Transmit Packet Window
PT-X25-92	Autoreset Value

Unsupported Parameters Present in the ASCII File

These parameters, although they will appear in an ASCII configuration file, are not configurable from the Configuration Program.

Table D-34. Unsupported Parameters Present in the ASCII File

BX-APPN-09	Constrained Threshold
BX-APPN-10	Critical Threshold

Abbreviations, Glossary, Bibliography, and Index

List of Abbreviations

A	ampere
AARP	AppleTalk Address Resolution Protocol
AC	alternating current
ACLST	AC logic self-test
ADCCP	advanced data communication control procedures
AEP	AppleTalk Echo Protocol
AIPGM	array initialization program
AIX	Advanced Interactive Executive
AMA	arbitrary MAC addressing
AMI	alternate mark inversion
AMT	address mapping table
ANSI	American National Standards Institute
APAR	Authorized Program Analysis Report
API	application programming interface
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
AS	Australian standard
ASCII	American National Standard Code for Information Interchange
ASE	autonomous system externals
ASN	Autonomous System Number
ASN	abstract syntax notation
AST	array self test
ASYNC	asynchronous
AT	Attention
ATE	Asynchronous Terminal Emulation
ATP	AppleTalk Transaction Protocol
AUI	attachment unit interface
AWG	American Wire Gauge
BCR	branch-on-condition register
BECN	backward explicit congestion notification
BER	basic encoding rules
BER	Bit error rate
BIOS	basic input/output system
BGP	Border Gateway Protocol
BIST	built-in self-test
BIU	basic information unit
BPDU	bridge protocol data unit
bps	bits per second
BS	British Standard
BSCRW	binary synchronous read/write
BTU	British thermal unit
B8ZS	binary 8 zero suppression coding scheme
C	Celsius
CBA	common on-chip-processor bus address
CCITT	Consultative Committee on International Telegraph and Telephone
CD-ROM	compact disk read-only memory
CEE	International Commission for Conformity Certification of Electrical Equipment
CEI	Comitato Elettrotechnico Italiano
CEPT	Conference of European Post and Telecommunications Associations
CIO	common input/output
cm	centimeter
COS	class of service
CP	control point
CPMS	control point management services
CP-MSU	control point management services unit
CPS	call progress signal
CPU	central processing unit
CR	carriage return
CRC	cyclic redundancy check
CRS	configuration report server
CRT	cathode ray tube
CSA	Canadian Standards Association
CSMA/CD	carrier sense multiple access with collision detection
CSU	channel service unit
CTS	clear to send
CUG	closed user group
DA	destination address; diagnostic application
dB	decibel
DC	direct current
DCD	data carrier detect
DCE	data circuit-terminating equipment
DCLST	DC logic self-test

DDCMP Digital Data Communications Message Protocol

DDN Defense Data Network

DDP Datagram Delivery Protocol

DIS draft international standard

DISC disconnect character

DLC data link control

DLCI data link connection identifier

DLSw data link switching

DM data mode

DMA direct memory access

DNA Digital Network Architecture

DoD Department of Defense

DOS Disk Operating System

DRAM dynamic random access memory

DS directory services

DSAP destination service access point

DSE data switching equipment

DSE data switching exchange

DSPU downstream physical unit

DSR data set ready

DSU data service unit

DTE data terminal equipment

DTR data terminal ready

DUSCC dual universal serial communications controller

EC engineering change

ECC error correcting code

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

EIB error information block

ELAP EtherTalk Link Access Protocol

EMEA Europe/Middle East/Africa

EMI electromagnetic interference

EN end node

EP entry point

EPOW early power on warning

EPROM erasable programmable read-only memory

ESD electrostatic discharge

ESF extended super frame

ETX end of text

F Fahrenheit

FCS frame check sequence

FDDI Fiber Distributed Data Interface

FDL facilities data link

FDX full duplex

FECN forward explicit congestion notification

FFC failing function code

FP focal point

FRP Fragmentation Protocol

FRU field replaceable unit

FSCK File System Check

ft foot, feet

FTP File Transfer Protocol

GDS general data stream

HDLC high-level data link control

HVPD hardware vital product data

Hz hertz

I information

IAB Internet Architecture Board

IANA Internet Assigned Numbers Authority

ICMP Internet Control Message Protocol

ICP Internet Control Protocol

ID identification

IDP Internet Datagram Protocol

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

in. inch

InARP Inverse Address Resolution Protocol

IML initial machine load

I/O input/output

IOCC input/output channel control

ICP Internet Control Protocol

IP Internet Protocol

IPC Interprocess Communications Protocol

IPCP IP Control Protocol

IPL initial program load

IPRTS permanent request to send

IPX Internetwork Packet Exchange

IRTF Internet Research Task Force

ISDN	integrated services digital network
ISO	International Organization for Standardization
ISR	intermediate session routing
KB	kilobyte
Kbps	kilobits per second
kg	kilogram
KHz	kilohertz
kVA	kilovolt ampere
LAN	local area network
LAPB	link access protocol-balanced
LAPD	link access procedure for D-channel of ISDN
lb	pound
LBO	line build out
LBS	LAN bridge server
LCN	logical channel number
LCP	Link Control Protocol
LED	light-emitting diode
LEN	low-entry networking
LF	line feed
LLC	logical link control
LMI	local management interface
LNM	LAN Network Manager
LpAm	level pressure A-weighted mean
LRM	LAN reporting mechanism
LU	logical unit
LVM	logical volume manager
LWAd	level watts A-weighted declared
m	meter
MAC	medium access control
MAN	metropolitan area network
MAP	maintenance analysis procedure
MAP	Manufacturing Automation Protocol
Mb	megabit
MB	megabyte
Mbps	megabits per second
MBps	megabytes per second
MDS	multiple domain support
MDS-MU	multiple domain support message unit
MES	Miscellaneous Equipment Specifications
MHz	megahertz
MIB	Management Information Base
MILNET	military network
MLTG	multi-link transmission group
mm	millimeter
MPNP	Multiprotocol Network Program
ms	millisecond
MTU	maximum transmission unit
NAU	network addressable unit
NAUN	nearest active upstream neighbor
NBP	Name Binding Protocol
NCP	Network Control Program
NCP	Network Control Protocol
NCP	Network Core Protocol
NCTE	Network Customer Equipment
NEMA	National Electrical Manufacturers Association
NetBIOS	Network Basic Input/Output System
NetRPC	Network Remote Procedure Calls
NFS	Network File System
NI	network interface
NIC	Network Information Center
NIC	network interface card
NICE	Network Information and Control Exchange
NIO	native input/output
NL	new line
NLPID	network layer protocol ID
NMVT	network management vector transport
NN	network node
NOC	network operations center
NRM	normal response mode
NRZ	non-return-to-zero
NRZI	non-return-to-zero inverted
NS/2	Networking Services/2
NSFNET	National Science Foundation NETwork
NUA	network user address
NUI	network user identification
NVRAM	non-volatile random access memory
NZS	New Zealand Standard
OA	Outgoing Access
OCS	outboard communication server; on-card sequencer
ODI	Open Datalink Interface
ODM	object data manager

OEM	original equipment manufacturer
OS/2	Operating System/2
OSI	open systems interconnection
OSPF	Open Shortest Path First
OSPFase	Open Shortest Path First autonomous system external
PAL	programmable array logic
PAP	Password Authentication Protocol
PAP	Printer Access Protocol
PC	personal computer
PCSA	Personal Computing Systems Architecture
PdAt	Predefined Attributes
PDU	protocol data unit
PIU	path information unit
PMX	Presentation Management X–Server
POR	power-on reset
POS	programmable option select
POST	power-on self-test
PPP	Point-to-Point Protocol
PROM	programmable read-only memory
PRPQ	programming request for price quotation
PRTS	permanent request to send
PS/2	Personal System/2
PSDN	packet switching data network
PSE	packet switching equipment
PSP	portable service platform
PSS	packet switch stream
PTF	program temporary fix
PTY	pseudo teletype port
PU	physical unit
PVC	permanent virtual circuit
QLLC	qualified link level control
RAM	random access memory
REM	ring error monitor
REXEC	Remote Execution Protocol
RFC	Request for Comments
RFI	radio frequency interference
RH	request header
RI	routing information
RIP	Routing Information Protocol
RISC	reduced instruction-set computer
RLBT	remote loopback test
RLSD	received line signal detector
RNN	reporting network node
RNR	receive not ready
ROM	read-only memory
ROS	read-only storage
RPOA	Recognized Private Operating Agency
RPS	ring parameter server
RPQ	request for price quotation
RR	receive ready
RSCV	route selection control vector
RSH	Remote Shell Protocol
RSN	resource sequence number
RTMP	Routing Table Maintenance Protocol
RTP	RouTing update Protocol
RU	request/response unit
SA	source address
SABS	South African Bureau of Standards
SAP	service access point
SAP	Service Advertising Protocol
SABME	set asynchronous balanced mode extended
SCRLL	scroll
SCSI	small computer systems interface
SDLC	synchronous data link control
SELV	safety extra low voltage
SEV	Schweizerischer Elektrotechnischer Verein
SII	Standards Institution of Israel
SIMM	single inline memory module
SIO	serial input/output
SIP	single inline package
SLA	serial link adapter
SLSS	System Library Subscription Service
SMI	Structure of Management Information
SNA	Systems Network Architecture
SNA/MS	Systems Network Architecture Management Services
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SOC	sphere of control
SPP	Sequenced Packet Protocol
SPX	Sequenced Packet Exchange

SRAM	static random access memory
SRN	service request number
SRT	source routing transparent (bridging)
SRTB	source routing to transparent bridging
SR-TB	source routing to transparent bridging
SSAP	source service access point
SSCP	system services control point
STP	spanning tree protocol
STP	shielded twisted pair
SVC	switched virtual circuit
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDU	topology database update
TG	transmission group
TLAP	TokenTalk Link Access Protocol
TR	terminal ready
TRB	transparent bridging
TT	terminal timing
UA	unnumbered acknowledgment
UDP	User Datagram Protocol
UI	unnumbered information
UL	Underwriter's Laboratories
UPS	uninterruptible power supply
V AC	volts alternating current
VAX	virtual address extension
VCCI	Voluntary Control Council for Interference
VGA	video graphics adapter
VINES	VIrtual NEtworking System
VPD	vital product data
VRN	virtual routing node
VTAM	Virtual Telecommunications Access Method
WAN	wide area network
X.25	packet-switched networks
XID	exchange identification
XNS	Xerox Network Systems
ZIP	Zone Information Protocol
ZIT	Zone Information Table

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology*. Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The Network Working Group Request for Comments: 1208.
- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.

The following cross-references are used in this glossary:

Contrast with: This refers to a term that has an opposed or substantively different meaning.

Synonym for: This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with: This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also: This refers the reader to terms that have a related, but not synonymous, meaning.

Deprecated term for: This indicates that the term should not be used. It refers to a preferred term, which is defined in its proper place in the glossary.

A

AARP. AppleTalk Address Resolution Protocol.

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also *abstract syntax notation 1 (ASN.1)* and *basic encoding rules (BER)*.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in ISO 8824. See also *basic encoding rules (BER)*.

ACCESS. In the Simple Network Management Protocol (SNMP), the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

access method. A technique, implemented in software, that controls the flow of information through a network.

access unit. A unit that allows attaching devices to access a local area network (LAN) at a central point, such as a wiring closet or an open work area.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active. (1) Operational. (2) Pertaining to a node or device that is connected or is available for connection to another node or device.

adapter. A part that electrically or physically connects a device to a computer or to another device.

address. In data communication, the unique code assigned to each device or workstation connected to a network.

address mapping table (AMT). A table, maintained within the AppleTalk router, that provides a current mapping of node addresses to hardware addresses.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an internet address. Synonymous with *subnet mask* and *subnetwork mask*.

address resolution. A method for mapping network-layer addresses to media-specific addresses. See also *Address Resolution Protocol (ARP)* and *AppleTalk Address Resolution Protocol (AARP)*.

Address Resolution Protocol (ARP). In the Internet suite of protocols, the protocol that dynamically maps an IP address to an address used by a supporting metropolitan or local area network such as Ethernet or token-ring. See also *Reverse Address Resolution Protocol (RARP)*.

addressing. In data communication, the way in which a station selects the station to which it is to send data.

adjacent nodes. Two nodes connected together by at least one path that connects no other node. (T)

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) end node. A node that provides a broad range of end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to a subarea network as a peripheral node or to other end nodes.

Advanced Peer-to-Peer Networking (APPN) network. A collection of interconnected network nodes and their client end nodes.

Advanced Peer-to-Peer Networking (APPN) network node. A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

Advanced Peer-to-Peer Networking (APPN) node. An APPN network node or an APPN end node.

AEP. AppleTalk Echo Protocol.

agent. A system that assumes an agent role.

AIX. Advanced Interactive Executive.

all-stations address. Synonym for *broadcast address*.

alternate route. A secondary or backup route that is used if normal routing is not possible.

AMA. Arbitrary MAC addressing.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

AMT. Address mapping table.

analog. (1) Pertaining to data consisting of continuously variable physical quantities. (A) (2) Contrast with *digital*.

ANSI. American National Standards Institute.

API. (1) Application program interface. (2) Application programming interface.

AppleTalk. A network protocol developed by Apple Computer, Inc. This protocol is used to interconnect network devices, which can be a mixture of Apple and non-Apple products.

AppleTalk Address Resolution Protocol (AARP). In AppleTalk networks, a protocol that a) translates AppleTalk node addresses into hardware addresses and b) reconciles addressing discrepancies in networks that support more than one set of protocols.

AppleTalk Echo Protocol (AEP). In AppleTalk networks, a protocol that provides a node destination test function by means of a send and receive transaction where the packet received at the source node is identical to the packet sent to the destination node.

AppleTalk Transaction Protocol (ATP). In AppleTalk networks, a protocol that provides client/server request and response functions for hosts accessing the Zone Information Protocol (ZIP) for zone information.

application. A collection of software components used to perform specific types of user-oriented work on a computer.

application program interface (API). A functional interface used by an executing application program to access the specific functions and services provided by an underlying operating system or service program.

application programming interface (API). (1) The set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by an underlying operating system or service program. (2) In VTAM, the language structure used in control blocks so that application programs can reference them and be identified to VTAM.

APPN. Advanced Peer-to-Peer Networking.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network.*

APPN network node. See *Advanced Peer-to-Peer Networking (APPN) network node.*

APPN node. See *Advanced Peer-to-Peer Networking (APPN) node.*

arbitrary MAC addressing (AMA). In DECnet architecture, an addressing scheme used by DECnet Phase IV-Prime that supports universally administered addresses and locally administered addresses.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

ARP. Address Resolution Protocol.

ASCII (American National Standard Code for Information Interchange). The standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters. (A)

ASN.1. Abstract syntax notation 1.

ASYNC. Asynchronous.

asynchronous (ASYNC). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

ATP. AppleTalk Transaction Protocol.

attachment unit interface (AUI). In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (I) (A)

AUI. Attachment unit interface.

auto-call. Synonym for *automatic calling.*

automatic calling. A feature that permits a station to initiate a connection with another station over a switched line without operator action. Synonymous with *auto-call.*

automatic single-route broadcast. A function used by some IBM bridge programs to determine the correct settings and to set the bridge single-route broadcast configuration parameters dynamically, without operator intervention. As bridges enter and leave the network, the parameter settings may need to change to maintain a single path between any two LAN segments for single-route broadcast messages.

autonomous system. In TCP/IP, a group of networks and routers under one administrative authority. These networks and routers cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. In TCP/IP, a number assigned to an autonomous system by the same central authority that also assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

autonomous system path. In the Border Gateway Protocol (BGP), the autonomous systems that are traversed to reach the networks listed in the update message. The path helps to suppress looping of routing information.

B

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges or routers. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected.

backbone network. A central network to which smaller networks, normally of lower speed, connect. The backbone network usually has a much higher capacity than the networks it helps interconnect or is a wide-area network (WAN) such as a public packet-switched datagram network.

basic encoding rules (BER). The rules specified in ISO 8825 for encoding data units described in abstract syntax notation 1 (ASN.1). The rules specify the encoding technique, not the abstract syntax.

basic information unit (BIU). In SNA, the unit of data and control information passed between half-sessions. It consists of a request/response header (RH) followed by a request/response unit (RU).

Basic Input/Output System (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

baud. (1) A unit of signaling speed equal to the number of discrete conditions or signal events per second; for example, one baud equals one-half dot cycle per second in Morse code, one bit per second in a train of binary signals, and one 3-bit value per second in a train of signals each of which can assume one of eight different states. (A) (2) In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud. (A)

BER. Basic encoding rules.

BGP. Border Gateway Protocol.

BGP configured neighbor. A specific router (as defined by its BGP neighbor's IP address) in a BGP group with which the IBM 6611 Network Processor exchanges routing information.

BGP group. An autonomous system made up of neighbors that be configured or learned. The neighbors have the same group type, such as external, test, internal, or Interior Gateway Protocol.

bilingual circuit. In DECnet architecture, a circuit that accepts, translates, and routes DECnet Phase IV and DECnet Phase IV-Prime frames. The circuit must be configured with the DECnet MAC address specific to the attached LAN segment.

BIND. In SNA, a request to activate a session between two logical units (LUs). See also *session activation request*. Contrast with *UNBIND*.

BIOS. Basic Input/Output System. See also *NetBIOS*.

bit clocking. In an EIA 232 interface, the field that indicates which piece of equipment, either the modem or the computer, provides the clock signal for synchronized data transactions.

BIU. Basic information unit.

block. A string of data elements recorded or transmitted as a unit. The elements may be characters, words, or physical records. (T)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems. Contrast with *Exterior Gateway Protocol (EGP)*.

border router. In Internet communications, a router, positioned at the edge of an autonomous system, that communicates with a router that is positioned at the edge of a different autonomous system.

BPDU. Bridge protocol data unit.

bps. Bits per second.

bridge. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address.

bridge identifier. An 8-byte field, used in a spanning tree protocol, composed of the MAC address of the port with the lowest port identifier and a user-defined value.

bridging. In LANs, the forwarding of a frame from one LAN segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

bridge protocol data unit (BPDU). A bridge message that contains configuration and topology information. BPDUs are periodically multicast by one bridge on each LAN segment of an extended LAN to the other bridges on that segment. These messages are used to determine the root bridge for a spanning tree and to maintain and update the spanning tree.

broadcast. (1) Transmission of the same data to all destinations. (T) (2) Simultaneous transmission of data to more than one destination. Contrast with *multicast*.

broadcast address. In SDLC, a station address (eight 1's) reserved as an address common to all stations on a link. Synonymous with *all-stations address*.

bus. (1) A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment. (T) (2) A computer configuration in which processors are interconnected in series.

button. A word or picture on the screen that can be selected. Once selected and activated, a button begins an action in the same manner that pressing a key on the keyboard can begin an action.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. (4) To place, hide, or store in a cache.

call-accepted packet. A call supervision packet that a called data terminal equipment (DTE) transmits to indicate to the data circuit-terminating equipment (DCE) that it accepts the incoming call.

call request packet. (1) A call supervision packet that a data terminal equipment (DTE) transmits to ask that a connection for a call be established throughout the network. (2) In X.25 communications, a call supervision packet transmitted by a DTE to ask for a call establishment through the network.

calling. (1) The process of transmitting selection signals in order to establish a connection between data stations. (I) (A) (2) In X.25 communications, pertaining to the location or user that makes a call.

carrier. An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system. (T)

carrier sense. In a local area network, an ongoing activity of a data station to detect whether another station is transmitting. (T)

carrier sense multiple access with collision detection (CSMA/CD). A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again. (T) (A)

CCITT. International Telegraph and Telephone Consultative Committee. An organization (one of four permanent organs of the International Telecommunication Union [ITU], headquartered in Geneva, Switzerland) that is concerned with the problems relating to international telephony and telegraphy. The CCITT Plenary Assembly meets at regular intervals to prepare a list of technical questions related to telephone and telegraph services. The Assembly assigns these questions to study groups, which then prepare recommendations to be presented at the next plenary meeting. Approved recommendations are published for the use of engineers, scientists, and manufacturers around the world.

CDSTL. Connect data set to line.

central processing unit (CPU). The part of a computer that includes the circuits that control the interpretation and execution of instructions.

Note: A CPU is the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

change management. The process of planning (for example, scheduling) and controlling (for example, distributing, installing, and tracking) changes in an SNA network.

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) A functional unit, controlled by the processor, that handles the transfer of data between processor storage and local peripheral equipment. See *input/output channel*.

channel service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal's performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loopback testing, which includes the transmission of test signals between the CSU and the network carrier's office channel unit. See *data service unit (DSU)*.

check box. A square box with associated text that represents a choice. When a user selects a choice, an X appears in the check box to indicate that the choice is in effect. The user can clear the check box by selecting the choice again.

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

circuit. (1) One or more conductors through which an electric current can flow. See *physical circuit* and *virtual circuit*. (2) A logic device.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with *line switching*.

class. In object-oriented design or programming, a group of objects that share a common definition and that therefore share common properties, operations, and behavior. Members of the group are called instances of the class.

|...+....1....+....2....+....3....+....4....+....5....+....6....+....7..

class of service (COS). A set of characteristics (such as route security, transmission priority, and bandwidth) used to construct a route between session partners. initiator of a session.

click. To press and release a button on a pointing device without moving the pointer off the choice.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

clocking. (1) In binary synchronous communication, the use of clock pulses to control synchronization of data and control characters. (2) A method of controlling the number of data bits sent on a telecommunication line in a given time.

closed user group (CUG). In data communication, a group of users who can communicate with other users in the group, but not with users outside the group.

Note: A data terminal equipment (DTE) may belong to more than one closed user group.

closed user group with outgoing access. (1) A closed user group that has a user-assigned facility which enables that user to communicate with other users of a data network transmission service where appropriate, with users having a data terminal equipment connected to any other switched network to which interworking facilities are available, or both. (T) (A) (2) In data communication, a closed user group in which one or more users can communicate with users outside the closed group, under certain conditions.

collision. An unwanted condition that results from concurrent transmissions on a channel. (T)

collision detection. In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

component. Hardware or software that is part of a functional unit.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

configuration file. A file that specifies the characteristics of a system device or network.

configuration parameter. A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

configuration report server (CRS). A program that sends notifications about the current active configuration on each ring to one or more LAN managers through the LAN reporting mechanism (LRM). Changes in the nearest active upstream neighbor (NAUN) addresses and active monitor on the ring are reported.

congestion. See *network congestion*.

connect data set to line (CDSTL). In SNA, an option that determines how the data terminal ready (DTR) signal to the modem operates. It is used if a DTR indicates an unconditional command from the data terminal equipment (DTE) to the attached data circuit-terminating equipment (DCE) to connect to or remove itself from the network.

connection. In data communication, an association established between functional units for conveying information. (I) (A)

connection network. A representation within an APPN network of a shared-access transport facility (SATF), such as a token ring, that allows nodes identifying their connectivity to the SATF by a common virtual routing node to communicate without having individually defined connections to one another.

connectionless service. A network service that treats each packet or datagram as a separate entity that contains the source address and destination address and for which no acknowledgment is returned to the originating source. Connectionless services are on a best-effort basis and do not guarantee reliable or in-sequence delivery. Contrast with *connection-oriented service*.

connectivity. (1) The capability of a system or device to be attached to other systems or devices without modification. (T) (2) The capability to attach a variety of functional units without modifying them.

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

control point management services (CPMS). A component of a control point, consisting of management services function sets, that provides facilities to assist in performing problem management, performance and accounting management, change management, and configuration management. Capabilities provided by the CPMS include sending requests to physical unit management services (PUMS) to test system resources, collecting statistical information (for example, error and performance data) from PUMS about the system resources, and analyzing and presenting test results and statistical information collected about the system resources. Analysis and presentation responsibilities for problem determination and performance monitoring can be distributed among multiple CPMSs.

control point management services unit (CP-MSU). The message unit that contains management services data and flows between management services function sets. This message unit is in general data stream (GDS) format. See also *management services unit (MSU)* and *network management vector transport (NMVT)*.

Controlled Access Unit (CAU). An intelligent concentrator, such as the IBM 8230. The Controlled Access Unit is used as a point to control physical access to the ring, and to provide a method to bypass faulty or inactive devices.

COS. Class of service.

CP. Control point.

CP-MSU. Control point management services unit.

CPMS. Control point management services.

CPU. Central processing unit.

CRS. Configuration report server.

CSMA/CD. Carrier sense multiple access with collision detection.

CSU. Channel service unit.

CUG. Closed user group.

D

D-bit. In X.25 communications, the bit in a data packet or call-request packet that is set to 1 if end-to-end acknowledgment (delivery confirmation) is required from the recipient.

DASD. Direct access storage device.

data circuit. (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (I) (2) In SNA, synonym for *link connection*. (3) See also *physical circuit* and *virtual circuit*.

Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.
2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

data communication. (1) Transfer of data among functional units by means of data transmission according to a protocol. (T) (2) The transmission, reception, and validation of data. (A)

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	in-channel signaling
1–15	reserved
16–991	assigned using frame-relay connection procedures
992–1007	layer 2 management of frame-relay bearer service
1008–1022	reserved
1023	in-channel layer management

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link layer. In the Open Systems Interconnection reference model, the layer that provides services to transfer data between entities in the network layer over a communication link. The data link layer detects and possibly corrects errors that may occur in the physical layer. (T) See also *Open Systems Interconnection (OSI) reference model*.

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. See also *packet level* and *physical level*. (2) In X.25 communications, synonym for *frame level*.

data link switching (DLSw). A method of transporting network protocols that use IEEE 802.2 logical link control (LLC) type 2. SNA and NetBIOS are examples of protocols that use LLC type 2. See also *encapsulation* and *spoofing*.

data network. An arrangement of data circuits and switching facilities for establishing connections between data terminal equipment. (I)

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

data set ready. Synonym for *DCE ready*.

data stream. A continuous stream of data elements being transmitted, or intended for transmission, in character or binary-digit form, using a defined format.

data switching exchange (DSE). The equipment installed at a single location to provide switching functions, such as circuit switching, message switching, and packet switching. (I)

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (I)

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.
2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (I) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram consists of an IP header followed by the transport layer data. See also *packet* and *segment*.

Datagram Delivery Protocol (DDP). In AppleTalk networks, a protocol that provides network connectivity by means of connectionless socket-to-socket delivery service on the internet layer.

DCE. Data circuit-terminating equipment.

DCE ready. A signal, defined in the EIA 232 standard, that indicates to the data terminal equipment (DTE) that the local data circuit terminating equipment (DCE) is connected to the communication channel and is ready to send data. Synonymous with *data set ready*.

DDP. Datagram Delivery Protocol.

DECnet. A network architecture that defines the operation of a family of software modules, databases, and hardware components typically used to tie Digital Equipment Corporation systems together for resource sharing, distributed computation, or remote system configuration. DECnet network implementations follow the Digital Network Architecture (DNA) model.

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

designated router. A router that informs end nodes of the existence and identity of other routers. The selection of the designated router is based upon the router with the highest priority. When several routers share the highest priority, the router with the highest station address is selected.

destination node. The node to which a request or data is sent.

destination port. The 8-port asynchronous adapter that serves as a connection point with a serial service.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. Contrast with *source service access point (SSAP)*.

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

digital. (1) Pertaining to data that consist of digits. (T) (2) Pertaining to data in the form of digits. (A) (3) Contrast with *analog*.

Digital Network Architecture (DNA). The model for all DECnet hardware and software implementations.

direct access storage device (DASD). A device in which access time is effectively independent of the location of the data.

direct memory access (DMA). The system facility that allows a device on the Micro Channel bus to get direct access to the system or bus memory without the intervention of the system processor.

directory. A table of identifiers and references to the corresponding items of data. (I) (A)

directory service (DS). An application service element that translates the symbolic names used by application processes into the complete network addresses used in an OSI environment. (T)

directory services (DS). A control point component of an APPN node that maintains knowledge of the location of network resources.

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line.

DLC. Data link control.

DLCI. Data link connection identifier.

DLSw. Data link switching.

DMA. Direct memory access.

DNA. Digital Network Architecture.

DNS. Domain name system.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In the Internet, a part of a naming hierarchy in which the domain name consists of a sequence of names (labels) separated by periods (dots). (3) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies.

domain name system (DNS). The online distributed database system used to map domain names to internet addresses.

dotted decimal notation. The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent IP addresses.

DS. (1) Directory service. (2) Directory services.

DSAP. Destination service access point.

DSE. Data switching exchange.

DSU. Data service unit.

DTE. Data terminal equipment. (A)

DTR. Data terminal ready.

dual filter. A filter that identifies two endpoints from which to deny or allow traffic.

dual mode bridging. The recommended bridging method for connecting, using a serial link, two 6611s configured as translational bridges. In dual mode bridging, frames are translated only if the source and destination LANs require different MAC frame formats.

dump. (1) Data that has been dumped. (T) (2) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

E

early token release. A function, supported by token-ring adapter types 2 and 3, that allows a transmitting station to release the token after transmitting the ending delimiter.

echo. In data communication, a reflected signal on a communications channel. On a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

EGP. Exterior Gateway Protocol.

EIA. Electronic Industries Association.

EIA 232. In data communications, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

EIA 422. In data communications, a specification of the Electronic Industries Association (EIA) that defines the electrical characteristics for balanced voltage digital interface circuits for the interchange of serial binary data between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), or any point-to-point interconnection of serial binary signals between digital equipment. The international equivalent is CCITT Recommendation V.11.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

EN. End node.

enable. To make functional.

enabled. (1) Pertaining to a state of the processing unit that allows the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or an audio response unit can accept incoming calls on a line.

encapsulation. In communications, a technique used by layered protocols by which a layer adds control information to the protocol data unit (PDU) from the layer it supports. In this respect, the layer encapsulates the data from the supported layer. In the Internet suite of protocols, for example, a packet would contain control information from the physical layer, followed by control information from the network layer, followed by the application protocol data. See also *data link switching*.

end node (EN). (1) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node*. (2) In communications, a node that is frequently attached to a single data link and cannot perform intermediate routing functions.

entry point (EP). In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

EP. Entry point.

ER. (1) Explicit route. (2) Exception response.

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

exception. An abnormal condition such as an I/O error encountered in processing a data set or a file.

exception response (ER). In SNA, a protocol requested in the form-of-response-requested field of a request header that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, can be returned. Contrast with *definite response* and *no response*.

exchange identification (XID). A specific type of basic link unit that is used to convey node and link characteristics between adjacent nodes. XIDs are exchanged between link stations before and during link activation to establish and negotiate link and node characteristics, and after link activation to communicate changes in these characteristics.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR).*

explorer frame. See *explorer packet*.

explorer packet. In LANs, a packet that is generated by the source host and that traverses the entire source routing part of a LAN, gathering information on the possible paths available to the host.

exterior gateway. In Internet communications, a gateway on one autonomous system that communicates with another autonomous system. Contrast with *interior gateway*.

Exterior Gateway Protocol (EGP). In the Internet suite of protocols, a protocol, used between domains and autonomous systems, that enables network reachability information to be advertised and exchanged. IP network addresses in one autonomous system are advertised to another autonomous system by means of EGP-participating routers. Contrast with *Border Gateway Protocol (BGP).*

E1. See *T1*.

F

fast select. (1) An option of a virtual call facility that allows inclusion of data in call-setup and call-clearing packets. (I) (2) In X.25 communications, an optional facility that allows inclusion of data in call-request and clear-request packets.

FDDI. Fiber Distributed Data Interface.

Fiber Distributed Data Interface (FDDI). An American National Standards Institute (ANSI) standard for a 100-megabit-per-second LAN using optical fiber cables.

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit may contain other field replaceable units.

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter. A device or program that separates data, signals, or material in accordance with specified criteria. (A)

flow control. In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the rate of flow of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units. See also *adaptive session-level pacing*, *pacing*, and *session-level pacing*.

FMD. Function management data.

focal point (FP). See *management services focal point (MSFP).*

FP. Focal point.

fragmentation. The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted. See also *segmenting*.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures.

frame level. See *link level*.

frame relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

frequency. The rate of signal oscillation, expressed in hertz.

FRU. Field replaceable unit.

FTP. File Transfer Protocol.

fully meshed network. A frame-relay network in which each router is directly connected to every other router and there is only one hop to reach another router. A data link connection identifier (DLCI) is subscribed from each router to every other router.

function management data (FMD). An RU category used for end-user data exchanged between logical units (LUs) and for requests and responses exchanged between network services components of LUs, PUs, and control points.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols.

GDS. General data stream.

general data stream (GDS). The data stream used for conversations in LU 6.2 sessions.

general data stream (GDS) variable. A type of RU substructure that is preceded by an identifier and a length field and includes either application data, user control data, or SNA-defined control data.

H

hard disk. (1) A rigid magnetic disk such as the internal disks used in the system units of personal computers and in external hard disk drives. (2) A rigid disk used in a hard disk drive.

HDLC. High-level data link control.

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

Hello. A protocol used by a group of cooperating, trusting routers to allow them to discover minimal delay routes.

hello message. (1) A message sent periodically to establish and test reachability between routers or between routers and hosts. (2) In the Internet suite of protocols, a message defined by the Hello protocol as an Interior Gateway Protocol (IGP).

high-level data link control (HDLC). In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

hop. (1) In APPN, a portion of a route that has no intermediate nodes. It consists of only a single transmission group connecting adjacent nodes. (2) To the routing layer, the logical distance between two nodes in a network.

hop count. (1) A metric or measure of distance between two points. (2) In Internet communications, the number of routers that a datagram passes through on its way to its destination. (3) In SNA, a measure of the number of links to be traversed in a path to a destination.

host. In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe.

I

I frame. Information frame.

I/O. Input/output.

IAB. Internet Architecture Board.

ICMP. Internet Control Message Protocol.

ICP. Internet Control Protocol.

IDP. Internet Datagram Protocol.

IEEE. Institute of Electrical and Electronics Engineers.

IETF. Internet Engineering Task Force.

IGP. Interior Gateway Protocol.

InARP. Inverse Address Resolution Protocol.

inbound. In communications, data that is received from the network.

inbound filter. A filter applied to frames flowing into a port from a transmission link or LAN.

incoming call packet. A call supervision packet transmitted by a data circuit-terminating equipment (DCE) to inform a called data terminal equipment (DTE) that another DTE has requested a call.

information (I) frame. A frame in I format used for numbered information transfer.

inoperative. The condition of a resource that has been active but is not currently active. A resource may be inoperative for reasons such as the following: a) it may have failed, b) it may have received an INOP request, or c) it may be suspended while a reactivate command is being processed. See also *inactive*.

input/output channel. In a data processing system, a functional unit that handles transfer of data between internal and peripheral equipment. (I) (A)

insert. In LANs, to make an attaching device an active part of the LAN.

integrated services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data.

Note: ISDNs are used in public and private network architectures.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interior gateway. In Internet communications, a gateway that communicates only with its own autonomous system. Contrast with *exterior gateway*.

Interior Gateway Protocol (IGP). In the Internet suite of protocols, a protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

intermediate node. A node that is at the end of more than one branch. (T)

intermediate session routing (ISR). A type of routing function within an APPN network node that provides session-level flow control and outage reporting for all sessions that pass through the node but whose end points are elsewhere.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Architecture Board (IAB). The technical body that oversees the development of the Internet suite of protocols that are known as TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Control Protocol (ICP). The VIrtual NEtworking System (VINES) protocol that provides exception notifications, metric notifications, and PING support. See also *RouTing update Protocol (RTP)*.

Internet Datagram Protocol (IDP). A Xerox Network Systems (XNS) connectionless datagram protocol.

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

Internetwork Packet Exchange (IPX). The network protocol used to connect Novell's servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology. See also *Xerox Network Systems (XNS)*.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units. (T)

Inverse Address Resolution Protocol (InARP). In the Internet suite of protocols, the protocol used for locating a protocol address through the known hardware address. In a frame-relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IP. Internet Protocol.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comment (RFC) 791. It is usually represented in dotted decimal notation.

IP datagram. In the Internet suite of protocols, the fundamental unit of information transmitted through an internet. It contains source and destination addresses, user data, and control information such as the length of the datagram, the header checksum, and flags indicating whether the datagram can be or has been fragmented.

IP router. A device in an IP internet that is responsible for making decisions about the paths over which network traffic will flow. Routing protocols are used to gain information about the network and to determine the best route over which the datagram should be forwarded toward the final destination. The datagrams are routed based on IP destination addresses.

IPX. Internetwork Packet Exchange.

IPXWAN. A Novell protocol that is used to exchange router to router information before exchanging standard IPX routing information and traffic over the WAN data links.

ISDN. Integrated services digital network.

ISO. International Organization for Standardization.

ISR. Intermediate session routing.

K

Kbps. Kilobits per second.

L

LAN. Local area network.

LAN bridge server (LBS). A program that maintains statistical counters about frames forwarded between two or more rings (through a bridge). The LBS sends these statistics to the appropriate LAN managers through the LAN reporting mechanism (LRM).

LAN Network Manager (LNM). A program that enables you to manage and to monitor LAN resources from a central workstation. It can be used as a problem determination aid.

LAN reporting mechanism (LRM). A management server positioned with each server on the LAN that communicates with the LAN managers. The LRM:

- Distributes reports generated by servers to each interested LAN manager
- Monitors that only one LAN manager actively manages collocated servers at one time

LAN segment. (1) Any portion of a LAN (for example, a bus or ring) that can operate independently, but that is connected to other parts of the network by means of bridges. (2) A ring or bus network without bridges.

LAPB. Link access protocol-balanced.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture. (T) (2) In the Open Systems Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols, that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions in other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

LBS. LAN bridge server.

LEN. Low-entry networking.

line data rate. The rate of data transmission over a telecommunication link.

line switching. Synonym for *circuit switching*.

link. The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

link access protocol-balanced (LAPB). A protocol used for accessing an X.25 network at the link level. LAPB is a duplex, asynchronous, symmetric protocol, used in point-to-point communication.

link-attached. Pertaining to devices that are connected to a controlling unit by a data link. Contrast with *channel-attached*. Synonymous with *remote*.

link connection. The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). Synonymous with *data circuit*.

link level. A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber's machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT. See *data link level*.

link-state. In routing protocols, the advertised information about the usable interfaces and reachable neighbors of a router or network. The protocol's topological database is formed from the collected link-state advertisements.

link station. The hardware and software components within a node representing a connection to an adjacent node over a specific link. For example, if node A is the primary end of a multipoint line that connects to three adjacent nodes, node A will have three link stations representing the connections to the adjacent nodes. See also *adjacent link station*.

LLC. Logical link control.

LMI. Local management interface.

local. Pertaining to a device accessed directly without use of a telecommunication line. Synonym for *channel-attached*.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. See also *Ethernet* and *token ring*.
(3) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local bridging. A function of a bridge program that allows a single bridge to connect multiple LAN segments without using a telecommunication link. Contrast with *remote bridging*.

local management interface (LMI). See *local management interface (LMI) protocol*.

local management interface (LMI) protocol. In NCP, a set of frame-relay network management procedures and messages used by adjacent frame-relay nodes to exchange line status information over DLCI X'00'. NCP supports both the American National Standards Institute (ANSI) and International Telegraph and Telephone Consultative Committee (CCITT) versions of LMI protocol. These standards refer to LMI protocol as *link integrity verification tests (LIVT)*.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

lock. The means by which integrity of data is ensured by preventing more than one user from accessing or changing the same data or object at the same time.

logical channel. In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

logical link. A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network.

logical link control (LLC). The data link control (DLC) LAN sublayer that provides two types of DLC operation for the orderly exchange of information. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery.

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T)

Note: The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical link control (LLC) protocol data unit. A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP), a source service access point (SSAP), a control field, and user data.

logical unit (LU). A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

low-entry networking (LEN). A capability of nodes to attach directly to one another using basic peer-to-peer protocols to support multiple and parallel sessions between logical units.

low-entry networking (LEN) end node. A LEN node receiving network services from an adjacent APPN network node.

low-entry networking (LEN) node. A node that provides a range of end-user services, attaches directly to other nodes using peer protocols, and derives network services implicitly from an adjacent APPN network node, that is, without the direct use of CP-CP sessions.

LRM. LAN reporting mechanism.

LU. Logical unit.

M

MAC. Medium access control.

MAN. Metropolitan area network.

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

management services (MS). Services that assist in the management of systems and networks in areas such as problem management, performance management, business management, operations management, configuration management, and change management.

management services focal point (MSFP). For any given management services discipline (for example, problem determination or response time monitoring), the control point that is responsible for that type of network management data for a sphere of control. This responsibility may include collecting, storing or displaying the data or all of these. (For example, a problem determination focal point is a control point that collects, stores, and displays problem determination data.)

management station. In Internet communications, the system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol, such as the Simple Network Management Protocol (SNMP).

manager. A system that assumes a manager role.

mapping. The process of converting data that is transmitted in one format by the sender into the data format that can be accepted by the receiver.

mask. (1) A pattern of characters used to control retention or elimination of portions of another pattern of characters. (I) (A) (2) To use a pattern of characters to control retention or elimination of portions of another pattern of characters. (I) (A)

maximum transmission unit (MTU). In LANs, the largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for Ethernet is 1500 bytes.

Mbps. One million bits per second.

MDS. Multiple-domain support.

MDS-MU. Multiple-domain support message unit.

medium access control (MAC). In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

medium access control (MAC) protocol. In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T) See also *logical link control protocol.*

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

metric. In Internet communications, a value, associated with a route, which is used to discriminate between multiple exit or entry points to the same autonomous system. The route with the lowest metric is preferred.

metropolitan area network (MAN). A network formed by the interconnection of two or more networks which may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with *local area network (LAN)* and *wide area network (WAN).*

MIB. (1) MIB module. (2) Management Information Base.

MIB object. In the Simple Network Management Protocol (SNMP), an object contained in the Management Information Base (MIB). Synonymous with *MIB variable.*

MIB tree. In the Simple Network Management Protocol (SNMP), the structure of the Management Information Base (MIB).

MIB variable. In the Simple Network Management Protocol (SNMP), a specific instance of a specific data object in a MIB module. Synonym for *MIB object.*

MIB view. In the Simple Network Management Protocol (SNMP), the collection of managed objects, known to the agent, that is visible to a particular community.

MILNET. The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

mode name. The name used by the initiator of a session to designate the characteristics desired for the session, such as traffic pacing values, message-length units, synch point and cryptography options, and the class of service (COS) within the transport network.

modulo. (1) Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. (2) See also *modulus*.

modulus. A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 (9 - 4 = 5; 4 - 9 = -5; and 5 divides both 5 and -5 without leaving a remainder).

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

MPNP. Multiprotocol Network Program.

MS. Management services.

MSFP. Management services focal point.

MTU. Maximum transmission unit.

multicast. (1) Transmission of the same data to a selected group of destinations. (T) (2) A special form of broadcast in which copies of a packet are delivered to only a subset of all possible destinations.

multiple-domain support (MDS). A technique for transporting management services data between management services function sets over LU-LU and CP-CP sessions. See also *multiple-domain support message unit (MDS-MU)*.

multiple-domain support message unit (MDS-MU). The message unit that contains management services data and flows between management services function sets over the LU-LU and CP-CP sessions used by multiple-domain support. This message unit, as well as the actual management services data that it contains, is in general data stream (GDS) format. See also *control point management services unit (CP-MSU)*, *management services unit (MSU)*, and *network management vector transport (NMVT)*.

Multiprotocol Network Program (MPNP). The IBM software that controls the functions of the IBM 6611 Network Processor. It is a licensed program made up of base code and the Configuration Program.

N

Name Binding Protocol (NBP). In AppleTalk networks, a protocol that provides name translation function from the AppleTalk entity (resource) name (character string) into an AppleTalk internet address (16-bit number) on the transport layer.

name resolution. In Internet communications, the process of mapping a machine name to the corresponding Internet Protocol (IP) address. See also *domain name system (DNS)*.

name server. In Internet communications, the station that translates host names into their respective internet addresses when requested by the stations on the network.

NAU. (1) Network accessible unit.

NAUN. Nearest active upstream neighbor.

NBP. Name Binding Protocol.

NCP. Network Control Program.

nearest active upstream neighbor (NAUN). In the IBM Token-Ring Network, the station sending data directly to a given station on the ring.

neighbor. A router on a common subnetwork that has been designated by a network administrator to receive routing information.

NetBIOS. (1) Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols. (2) See also *BIOS*.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) A group of nodes and the links interconnecting them.

network accessible unit (NAU). A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the destination of information transmitted by the path control network. Synonymous with *network addressable unit*.

network address. According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU). Synonym for *network accessible unit*.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion. An undesirable overload condition caused by traffic in excess of what a network can handle.

network identifier. (1) In TCP/IP, that part of the Internet address that defines a network. The length of the network ID depends on the type of network class (A, B, or C). See also *subnet address*. (2) A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

Network Information Center (NIC). In Internet communications, local, regional, and national groups throughout the world who provide assistance, documentation, training, and other services to users.

network layer. In Open Systems Interconnection (OSI) architecture, the layer that is responsible for routing, switching, and link-layer access across the OSI environment.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network node (NN). Synonym for *Advanced Peer-to-Peer Networking (APPN) network node*.

network operations center (NOC). Any center that has responsibility for the operational aspects of a production network. Examples of NOC tasks are monitoring and control, troubleshooting, and user assistance.

network user address (NUA). In X.25 communications, the X.121 address containing up to 15 binary code digits.

NIC. Network Information Center.

NMVT. Network management vector transport.

NN. Network node.

NOC. Network operations center.

node. (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data.

nonseed router. In AppleTalk networks, a router that acquires network number range and zone list information from a seed router attached to the same network.

nonswitched line. A telecommunication line on which connections do not have to be established by dialing. Contrast with *switched line*.

notification. An unscheduled, spontaneously generated report of an event that has occurred.

NRZ. Non-return-to-zero recording.

NRZ-1. Non-return-to-zero change-on-ones recording. (I) (A)

NRZI. Non-return-to-zero (inverted) recording. Deprecated term for *non-return-to-zero change-on-ones recording (NRZ-1)*.

NUA. Network user address.

O

object. In object-oriented design or programming, an abstraction consisting of data and the operations associated with that data. See also *class*.

object identifier. An administratively assigned data value of the type defined in abstract syntax notation 1 (ASN.1).

octet. A byte that consists of 8 bits. (T)

open. (1) A break in an electrical circuit. (2) To make an adapter ready for use.

Open Shortest Path First (OSPF). In the Internet suite of protocols, a function that provides intradomain information transfer. An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

Open Systems Interconnection (OSI). (1) The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) (2) The use of standardized procedures to enable the interconnection of data processing systems.

Note: OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

Open Systems Interconnection (OSI) architecture. Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

Open Systems Interconnection (OSI) reference model. A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

origin. An external logical unit (LU) or application program from which a message or other data originates. See also *destination*.

OSI. Open Systems Interconnection.

OSPF. Open Shortest Path First.

outbound. In communications, data that is transmitted to the network.

outbound filter. A filter that is applied to frames flowing from a port onto a transmission link or LAN.

P

pacing. A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. See *session-level pacing*, *send pacing*, and *virtual route (VR) pacing*. See also *flow control*.

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet mode operation. Synonym for *packet switching*.

packet modulo. The highest sequence number the packet level uses before resetting the count and beginning the count again.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with *packet mode operation*. See also *circuit switching*.

page. (1) In a virtual storage system, a fixed-length block that has a virtual address and is transferred as a unit between real storage and auxiliary storage. (I) (A) (2) The information displayed at the same time on the screen of a display device. (3) To replace the information displayed on the screen with prior or subsequent information from the same file.

parallel port. An access point through which a computer transmits or receives data that consists of several bits sent simultaneously on separate wires. Contrast with *serial port*.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also *explicit route (ER)*, *route extension*, and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control.

Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path cost. In link-state routing protocols, the sum of the link costs along the path between two nodes or networks.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment. See also *transmission header.*

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with *global character* and *wildcard character.*

PC. Path control.

PDU. Protocol data unit.

permanent virtual circuit (PVC). In X.25 and frame-relay communications, a virtual circuit that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with *switched virtual circuit (SVC).*

permit packet. At the interface between a data terminal equipment (DTE) and a data circuit-terminating equipment (DCE), a packet used to transmit permits over a virtual circuit.

PEX. Packet exchange.

physical circuit. A circuit established without multiplexing. See also *data circuit.* Contrast with *virtual circuit.*

physical connection. A connection that establishes an electrical circuit.

physical unit (PU). The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. See also *peripheral PU* and *subarea PU.*

PING. Packet internet groper.

PIU. Path information unit.

Point-to-Point Protocol (PPP). A protocol that provides a method for encapsulating and transmitting packets over serial point-to-point links.

poison reverse. A technique for minimizing the time to achieve network convergence. After a connection disappears, the router advertising the connection retains the routing table entry for several update periods and specifies an infinite cost in its broadcasts.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. Synonymous with *socket.* (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine.

port number. In Internet communications, the identification of an application entity to the transport service.

PPP. Point-to-Point Protocol.

preferential closed user group (CUG). In X.25 communications, the default closed user group.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

processor. In a computer, a functional unit that interprets and executes instructions. A processor consists of at least an instruction control unit and an arithmetic and logic unit. (T)

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with *line control discipline* and *line discipline*. See *bracket protocol* and *link protocol*.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

PU. Physical unit.

PVC. Permanent virtual circuit.

R

RARP. Reverse Address Resolution Protocol

reachability. The ability of a node or a resource to communicate with another node or resource.

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

reassembly. In communications, the process of putting segmented packets back together after they have been received.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See *RNR packet*.

received line signal detector (RLSD). A signal defined in the EIA-232 standard that indicates to the data terminal equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE). The older EIA terms for RLSD are data carrier detect and carrier detect.

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

Recommendation X.21. See *X.21*.

Recommendation X.25. See *X.25*.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

REM. Ring error monitor.

remote. Pertaining to a system, program, or device that is accessed through a telecommunication line. Contrast with *local*. Synonym for *link-attached*.

remote bridging. The function of a bridge that allows two bridges to connect multiple LANs using a telecommunication link. Contrast with *local bridging*.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any host in the network. The local host receives the results of the command execution.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

Reverse Address Resolution Protocol (RARP). In the Internet suite of protocols, the protocol that maps a hardware (MAC) address to an IP address. See also *Address Resolution Protocol (ARP)*.

REX. Route extension.

REXEC. Remote Execution Protocol.

RFC. Request for Comments.

RH. Request/response header.

ring. See *ring network*.

ring error monitor (REM). A program that collects ring error data from ring stations, analyzes the data, and forwards the results of that analysis to one or more LAN network managers through the LAN reporting mechanism (LRM).

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

ring parameter server (RPS). A management server that is responsible for setting and maintaining a consistent set of operational parameters in ring stations on a particular ring. It also informs the LAN manager, through the LAN reporting mechanism (LRM), of stations that are added to the ring.

ring segment. A section of a ring that can be isolated (by unplugging connectors) from the rest of the ring. See *LAN segment*.

RIP. Routing Information Protocol.

RISC. Reduced instruction-set computer.

rlogin (remote login). A service, offered by Berkeley UNIX-based systems, that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes information about the user's environment (for example, terminal type) to the remote machine.

RLSD. Received line signal detector.

RNR. Receive not ready.

RNR packet. A packet used by a data terminal equipment (DTE) or by a data circuit-terminating equipment (DCE) to indicate a temporary inability to accept additional packets for a virtual call or permanent virtual circuit.

ROM. Read-only memory. (A)

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunication link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

Route Selection control vector (RSCV). A control vector that describes a route within an APPN network. The RSCV consists of an ordered sequence of control vectors that identify the TGs and nodes that make up the path from an origin node to a destination node.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. Contrast with *bridge* and *gateway*. (3) In OSI terminology, a function that determines a path by which an entity can be reached.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing information field (RIF). In a frame, the sequence of bridge and LAN segment numbers from which bridges make frame forwarding decisions.

Routing Information Protocol (RIP). In the Internet suite of protocols, an interior gateway protocol used to exchange intradomain routing information and to determine optimum routes between internet hosts. RIP determines optimum routes on the basis of route metrics, not link transmission speed.

routing protocol. A technique used by a router to find other routers and to remain up to date about the best way to get to reachable networks.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). In AppleTalk networks, a protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

RouTing update Protocol (RTP). The VIrtual NEtworking System (VINES) protocol that maintains the routing database and allows the exchange of routing information between VINES nodes. See also *Internet Control Protocol (ICP)*.

RPOA. Recognized Private Operating Agency.

RPS. Ring parameter server.

RSCV. Route Selection control vector.

rsh. A variant of the rlogin command that invokes a command interpreter on a remote UNIX machine and passes the command-line arguments to the command interpreter, skipping the login step completely.

RTMP. Routing Table Maintenance Protocol.

RTP. RouTing update Protocol.

RU. Request/response unit.

S

SAP. (1) Service access point. (2) Service Advertising Protocol.

SCSI. Small computer system interface.

SDLC. Synchronous Data Link Control.

seed router. In AppleTalk networks, a router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed router must be initially set up using the configurator tool. Contrast with *nonseed router.*

segment. (1) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

segmenting. In OSI, a function performed by a layer to map one protocol data unit (PDU) from the layer it supports into multiple PDUs.

sequence number. In communications, a number assigned to a particular frame or packet to control the transmission flow and receipt of data.

serial port. An access point through which a computer transmits or receives data, one bit at a time. Contrast with *parallel port.*

server. A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

Service Advertising Protocol (SAP). In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and internet address recorded in all file servers running NetWare.
- A mechanism that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type.
- A mechanism that allows a workstation to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session.

session activation request. In SNA, a request that activates a session between two network accessible units (NAUs) and specifies session parameters that control various protocols during session activity; for example, BIND and ACTPU. Contrast with *session deactivation request.*

session deactivation request. In SNA, a request that deactivates a session between two network accessible units (NAUs); for example, UNBIND and DACTPU. Synonymous with *generic unbind.* Contrast with *session activation request.*

set. An SMNP function that allows a network management station to establish the value of a managed object (for example, set counter to 0).

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

singular filter. A filter that identifies a host, subnet, or all hosts with a single expression.

sliding window. A positive acknowledgment and retransmission technique, used by protocols when sending a stream of packets, that allows the sender to transmit a certain number of packets (usually around 10 packets) before an acknowledgment arrives. After the sender receives an acknowledgment for the first packet, it “slides” along the stream and sends another.

sliding window filter. A filter of variable window length that can be placed anywhere on a frame for scrutiny of the frame.

small computer system interface (SCSI). A standard hardware interface that enables a variety of peripheral devices to communicate with one another.

SMI. Structure of Management Information.

SNA. Systems Network Architecture.

SNA management services (SNA/MS). The services provided to assist in management of SNA networks.

SNA/MS. SNA management services.

SNAP. Subnetwork Access Protocol.

SNMP. Simple Network Management Protocol.

SOC. Sphere of control.

socket. The abstraction provided by Berkeley Software Distribution (BSD) that serves as an endpoint for communication between processes or applications.

source route bridging. In LANs, a bridging method that uses the routing information field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The routing information field is inserted into the MAC header by the source node. The information in the routing information field is derived from explorer packets generated by the source host.

source router. In LANs, the router that determines the route that the frame will follow.

source routing. In LANs, a method by which the sending station determines the route the frame will follow and includes the routing information with the frame. Bridges then read the routing information to determine whether they should forward the frame.

source service access point (SSAP). In SNA and TCP/IP, a logical address that allows a system to send data to a remote device from the appropriate communications support. Contrast with *destination service access point (DSAP).*

spanning tree. In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topology to ensure that there is only one route between any two LANs in the bridged network. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

sphere of control (SOC). The set of control point domains served by a single management services focal point.

sphere of control (SOC) node. A node directly in the sphere of control of a focal point. A SOC node has exchanged management services capabilities with its focal point. An APPN end node can be a SOC node if it supports the function to exchange management services capabilities.

split horizon. A technique for minimizing the time to achieve network convergence. A router records the interface over which it received a particular route and does not propagate its information about the route back over the same interface.

spoofing. For data links, a technique in which a protocol initiated from an end station is acknowledged and processed by an intermediate node on behalf of the final destination. In IBM 6611 data link switching, for example, SNA frames are encapsulated into TCP/IP packets for transport across a non-SNA wide area network, unpacked by another IBM 6611, and passed to the final destination. A benefit of spoofing is the prevention of end-to-end session timeouts.

SSAP. Source service access point.

static route. The route between hosts, networks, or both that is manually entered into a routing table.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

StreetTalk. In the VIrtual NEtworking System (VINES), a unique network-wide naming and addressing system that allows users to locate and access any resource on the network without knowing the network topology. See also *Internet Control Protocol (ICP)* and *RouTing update Protocol (RTP).*

Structure of Management Information (SMI). (1) In the Simple Network Management Protocol (SNMP), the rules used to define the objects that can be accessed by means of a network management protocol. (2) In OSI, the set of standards relating to management information. The set includes the *Management Information Model* and the *Guidelines for the Definition of Managed Objects*.

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the Internet address. (2) Synonym for *subnetwork*.

subnet address. In Internet communications, an extension to the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use `$AA` as their service access point (SAP) value.

subnetwork mask. Synonym for *address mask*.

SVC. Switched virtual circuit.

switched connection. A mode of operating a data link in which a circuit or channel is established to switching facilities as, for example, in a public switched network. (T)

switched line. A telecommunication line in which the connection is established by dialing. Contrast with *nonswitched line*.

switched virtual circuit (SVC). An X.25 circuit that is dynamically established when needed. The X.25 equivalent of a switched line.

synchronous. (1) Pertaining to two or more processes that depend upon the occurrence of specific events such as common timing signals. (T) (2) Occurring with a regular or predictable time relationship.

Synchronous Data Link Control (SDLC). A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I) Contrast with *binary synchronous communication (BSC)*.

SYNTAX. In the Simple Network Management Protocol (SNMP), a clause in the MIB module that defines the abstract data structure that corresponds to a managed object.

system. In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions. (I) (A)

system configuration. A process that specifies the devices and programs that form a particular data processing system.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the end users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol.

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

TG. Transmission group.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a "threshold exceeded" occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

throughput class. In packet switching, the speed at which data terminal equipment (DTE) packets travel through the packet switching network.

tick. The measurement of time that the Internetwork Packet Exchange (IPX) Routing Information Protocol (RIP) takes to reach its destination.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

translational bridging. A bridging method that allows frames to be bridged between ports configured to support source route bridging and ports configured to support transparent bridging. Frame translation is performed, as appropriate, to accommodate differences between Ethernet and token-ring frames bridged across LANs.

Note: Translational bridging on the 6611 emulates function provided by the IBM 8209 LAN Bridge product.

Transmission Control Protocol (TCP). A communications protocol used in Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet Protocol is the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission group (TG). (1) A connection between adjacent nodes that is identified by a transmission group number. See also *parallel transmission groups*. (2) In a subarea network, a single link or a group of links between adjacent nodes. When a transmission group consists of a group of links, the links are viewed as a single logical link, and the transmission group is called a *multilink transmission group (MLTG)*. A *mixed-media multilink transmission group (MMMLTG)* is one that contains links of different medium types (for example, token-ring, switched SDLC, nonswitched SDLC, and frame-relay links). (3) In an APPN network, a single link between adjacent nodes.

transmission header (TH). Control information, optionally followed by a basic information unit (BIU) or a BIU segment, that is created and used by path control to route message units and to control their flow within the network. See also *path information unit*.

transparent bridging. In LANs, a method for tying individual local area networks together through the medium access control (MAC) level. A transparent bridge stores the tables that contain MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

trusted router. A router that can supply what is considered, by other routers in the network, valid routing information and network destination feasibility information.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The European version (E1) transmits 2.048 Mbps. The Japanese version (J1) transmits 1.544 Mbps.

U

UA. Unnumbered acknowledgment.

UDP. User Datagram Protocol.

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with *locally administered address*.

User Datagram Protocol (UDP). In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

V.24. In data communications, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

V.28. In data communications, a specification of the CCITT that defines the electrical characteristics for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at rates below 20 kilobits per second.

V.35. In data communications, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

V.36. In data communications, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at rates of 48, 56, 64, or 72 kilobits per second.

variable. In the Simple Network Management Protocol (SNMP), a match of an object instance name with an associated value.

version. A separately licensed program that usually has significant new code or new function.

VINES. VIrtual NEtworking System.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit*. Contrast with *physical circuit*. (2) A logical connection established between two DTEs.

virtual link. In Open Shortest Path First (OSPF), a point-to-point interface that connects border routers that are separated by a non-backbone transit area. Because area routers are part of the OSPF backbone, the virtual link connects the backbone. The virtual links ensure that the OSPF backbone does not become discontinuous.

VIrtual NEtworking System (VINES). The network operating system and network software from Banyan Systems, Inc. In a VINES network, virtual linking allows all devices and services to appear to be directly connected to each other, when they may actually be thousands of miles apart. See also *StreetTalk*.

virtual route (VR). In SNA, either a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). See also *explicit route (ER)*, *path*, and *route extension (REX)*.

vital product data (VPD). Information that uniquely defines system, hardware, software, and microcode elements of a processing system.

VPD. Vital product data.

VR. Virtual route.

W

WAN. Wide area network.

well-known port. In Internet communications, one of a set of preassigned protocol port numbers that address specific functions used by transport level protocols (for example, TCP and UDP).

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. Contrast with *local area network (LAN)* and *metropolitan area network (MAN)*.

wildcard character. Synonym for *pattern-matching character*.

X

X.21. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for a general-purpose interface between data terminal equipment and data circuit-terminating equipment for synchronous operations on a public data network.

X.25. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. See also *packet switching*.

Xerox Network Systems (XNS). The suite of internet protocols developed by the Xerox Corporation. Although similar to TCP/IP protocols, XNS uses different packet formats and terminology. See also *Internetwork Packet Exchange (IPX).*

XID. Exchange identification.

Xmodem Protocol. A public-domain asynchronous data link control protocol that provides packet numbering and checksum error control for the transfer of binary files. The Xmodem Protocol is used widely for microcomputer systems.

XNS. Xerox Network Systems.

Z

ZIP. Zone Information Protocol.

ZIT. Zone information table.

zone. In AppleTalk networks, a subset of nodes within an internet.

Zone Information Protocol (ZIP). In AppleTalk networks, a protocol that provides zone management service by maintaining a mapping of the zone names and network numbers across the internet on the session layer.

zone information table (ZIT). A listing of network numbers and their associated zone name mappings in the internet. This listing is maintained by each internet router in an AppleTalk internet.

Bibliography

IBM 6611 Network Processor and Multiprotocol Network Program Publications

The IBM 6611 Network Processor and the Multiprotocol Network Program library includes the:

Multiprotocol Network Program Configuration Guide, SC31-6691

Multiprotocol Network Program Operations and Problem Management, SC31-6692

6611 Network Processor Cable Labels, GX27-3910

6611 Network Processor Connectivity Poster, SX75-0096

6611 Network Processor Customer Setup Guide, GA27-3993

6611 Network Processor Introduction and Planning Guide, GK2T-0334

6611 Network Processor Maintenance Information, GA27-3941

6611 Network Processor Network Management Reference, GC30-3567

6611 Network Processor Operations Pocket Guide, GX27-3909

6611 Network Processor Translated Safety Information, GA27-3954

Related IBM Product Publications

The following list of publications contains information concerning IBM products related to the use of the IBM 6611 Network Processor and the Multiprotocol Network Program:

AIX NetView/6000 Administration Reference, SC31-6196

AIX NetView/6000 at a Glance, GC31-6175

AIX SystemView NetView/6000 Concepts, GC31-6179

AIX SystemView NetView/6000 User's Guide, SC31-7024

AIX SystemView NetView/6000 Problem Determination, SC31-7021

AIX SystemView NetView/6000 Installation and Configuration, SC31-7020

Getting Started with LAN Network Manager, SC31-7104

LAN Cabling System Planning and Installation Guide, GA27-3361

LAN Network Manager Reference, SC31-7106

LAN Station Manager User's Guide, SC31-7108

Local Area Network Manager Reference, SC31-7106

NetBIOS Application Development Guide, S68X-2270

IBM Remote Token-Ring Bridge/DOS Version 1.0.1, part number P71G9347 includes publications and diskettes

Systems Network Architecture Concepts and Products, GC30-3072

Systems Network Architecture Formats, GA27-3136

Systems Network Architecture Management Services Reference, SC30-3346

Systems Network Architecture Technical Overview, GC30-3073

Systems Network Architecture Type 2.1 Node Reference, SC30-3422

TCP/IP Tutorial and Technical Overview, GG24-3376

Token-Ring Network Introduction and Planning Guide, GA27-3677

Token-Ring Network Architecture Reference, SC30-3374

Token-Ring Network Bridge Program Version 2.2.4 User's Guide (shipped with the product)

Token-Ring Network Introduction and Planning Guide, GA27-3677

The IBM Network Processor, GG24-3870

Using LAN Network Manager, SC31-7105

Using the IBM Cabling System and Communication Products, GA27-3620

8209 LAN Bridge: Attachment Module Guide for Ethernet and IEEE 802.3 LANs, GA27-3891

6611 Network Processor folder, SX75-0102, which includes these brochures:

- *6611 Network Processors and the IBM Multiprotocol Network Program*, G325-6503
- *6611 SNA/NetBIOS Internetworking*, G325-6504
- *6611 World-Class Multiprotocol Support*, G325-6505
- *6611 Network Management and the AIX Router and Bridge Manager/6000*, G325-6506
- *6611 Configuration Program and System Manager*, G325-6507

Other Publications

The following list is of known publications that contain information about internetworking, network design, and the protocols that the IBM 6611 supports. Other useful publications may already exist or may be published after the date of this book.

Internet Activities Board (IAB)

Internet Official Protocol Standards, Request for Comments 1600, Jon Postel (editor), March 1994

Internet Activities Board, Request for Comments 1160, Vinton G. Gerf, DDN Network Information Center, SRI International, May 1990

Internetworking

FYI on "What Is the Internet?", Request for Comments 1462, Krol, E., Hoffman, E, May 1993

FYI on Introducing the Internet–A Short Bibliography of Introductory Internetworking Readings for the Network Novice, Request for Comments, 1463, Hoffman, E., Jackson, L., May 1993

Internetworking: A Guide to Communications, Mark A. Miller, M&T Books, 1991

Internetworking Computer Systems: Interconnecting Networks and Systems, John McConnell, Prentice Hall, 1988.

Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture, Second Edition, Douglas E. Comer, Prentice Hall, 1991

Network Design

IBM Multisegment LAN Design Guidelines, GG24-3398

The IBM 6611 Network Processor as an IP Router, GG24-4064

Protocols

ANSI T1.617-1991, *Telecommunications — Digital Subscriber Signaling Service 1—Signaling Specification for Frame Relay Bearer Service*, June 18, 1991

Banyan VINES-The Professional Reference, Jim Krochmal, New Riders Publishing, 1994

CCITT Recommendation I.122 — Framework for Providing Additional Packet-Mode Bearer Services

CCITT Recommendation Q.922 — ISDN Data Link Layer Specification for Frame Mode Bearer Services, April 19, 1991

CCITT Recommendation X.21, Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Synchronous Operation on Public Data Networks (Geneva, 1984)

CCITT Recommendation X.25, Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks (Geneva, 1976; amended Geneva, 1980)

DECnet Digital Network Architecture (Phase IV): General Description, AA-N149A-TC, Digital Equipment Corporation, 1982

DECnet Digital Network Architecture (Phase IV): Ethernet Data Link Functional Specification, AA-Y298A-TK, Digital Equipment Corporation, 1983

DECnet Digital Network Architecture (Phase IV): Routing Layer Functional Specification, AA-X435A-TK, Digital Equipment Corporation, 1983

DECnet Digital Network Architecture (Phase IV): Token Ring Data Link and Node Product Functional Specifications, EK-DNAP4-TR-001, Digital Equipment Corporation, 1992

Inside AppleTalk, Second Edition, Gursharan Sidhu, Richard Andrews, Alan Oppenheimer, Addison-Wesley Publishing Company, Inc., 1990

Internet Transport Protocols, XNSS 028112, Xerox Corporation, 1981

Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture, Second Edition, Douglas E. Comer, Prentice Hall, 1991

IPX Router Specification, Part Number 107-000029-001, Novell, Inc., October 16, 1992

NetWare Communications Processes, Paul Turner, Novell Corporation, 1990

Novell NetWare Link Services Protocol Specification, Revision 1, Novell part number 100-001708-002, February 1994

VINES Protocol Definition, Order Number 003673, Banyan Systems Incorporated, June 1993

VINES Architecture Definition, Order Number 002645, Banyan Systems Incorporated, April 1993

Network Management

IEEE 802.1D-1990, IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, The Institute of Electrical and Electronics Engineers, Inc., May 1990

Interconnections: Bridges and Routers, Perlman, Radia, Addison-Wesley Publishing Company, Inc., 1992

Networking with Banyan VINES, Laubach, Edwin G., McGraw-Hill, Inc., 1991

Specification of Abstract Syntax Notation One (ASN.1), Information technology–Open Systems Interconnection, International Standard ISO/IEC 8824, December 1991

The IBM LAN Bridge, Latif, A., Rowlance, E.J., Adams, R. Holt, IEEE Network, Volume 6 Number 3, May 1992

The Simple Book: An Introduction to Management of TCP/IP-based Internets, Marshall T. Rose, Prentice Hall, 1991

Internet Requests for Comments (RFCs)

Obtaining RFCs

This section describes three methods for obtaining copies of Internet RFCs.

Electronic Copies via FTP: If you have FTP running on a workstation that is connected to the Internet, you may retrieve RFCs from the Network Information Center by following this procedure:

1. Use FTP to connect to host ds.internic.net.
2. Issue the command **user anonymous** to identify yourself to the host.
3. When prompted for a password, type **guest**.
4. Type the command **cd rfc** to change to the RFC directory.
5. Type the command **get rfc.nnn.txt**, where *nnn* represents the requested RFC number.

Electronic Copies via Electronic Mail:

The Network Information Center provides an automated service called service@ds.internic.net. This service allows you to access RFCs (and other documents) via ordinary electronic mail. This is especially useful for users who do not have access to the Network Information Center via a direct Internet link. Follow this procedure to obtain an RFC via electronic mail:

1. Send a mail message to service@ds.internic.net.
2. In the Subject field, type **rfc.nnn.**, where *nnn* is the RFC number. To obtain a list of all of the RFCs available, substitute the word *index* for *nnn*.

Large files will be broken into smaller separate messages. The information you request will be sent back to you as soon as possible.

Printed Copies: Printed copies of RFCs are available for a fee from:

SRI International, Room EJ291
333 Ravenswood Avenue
Menlo Park, CA 94025
(415) 859-3695
(415) 859-6387
FAX (415) 859-6028

RFCs Implemented by the IBM 6611 and the IBM Multiprotocol Network Program

This section provides a list of Internet RFCs and drafts that relate to the IBM 6611 and the IBM Multiprotocol Network Program.

RFC	Title
768	*User Datagram Protocol*, Postel, J.B., August 1980
791	*Internet Protocol*, Postel, J.B., September 1981
792	*Internet Control Message Protocol*, Postel, J.B., September 1981
793	*Transmission Control Protocol*, Postel, J.B., September 1981
826	*Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48 Bit Ethernet Address for Transmission on Ethernet Hardware*, D.C. Plummer, November 1982
854	*Telnet Protocol Specification*, Postel, J.B.; Reynolds J.K., May 1983

855 *Telnet Option Specifications*, Postel, J.; Reynolds J., May 1983

862 *Echo Protocol*, Postel, J., May 1983

868 *Time Protocol*, Postel, J.; Harrenstien, K., May 1983

877 *Standard for the Transmission of IP Datagrams over Public Data Networks*, Korb, J.T., September 1983

891 *DCN Local-Network Protocols*, Mills, D.L., December 1983

894 *Standard for the Transmission of IP Datagrams over Ethernet Networks*, Hornig, C., April 1984

904 *Exterior Gateway Protocol Formal Specification*, Mills, D.L., April 1984

919 *Broadcasting Internet Datagrams*, Mogul, J., October 1984

922 *Broadcasting Internet Datagrams in the Presence of Subnets* , Mogul, J., October 1984

950 *Internet Standard Subnetting Procedure*, Mogul, J; Postel, J., August 1985

951 *Bootstrap Protocol*, Croft, W., Gilmore, J., September 1985

959 *File Transfer Protocol*, Postel, J.B.; Reynolds J.K., October 1985

1009 *Requirements for Internet Gateways*, Braden, R.; Postel, J., June 1987

1042 *Standard for the Transmission of IP Datagrams over IEEE 802 Networks*, Postel J.B.; Reynolds J.K., February 1988

1058 *Routing Information Protocol*, Hendrick, C., June 1988

1155 *Structure and Identification of Management Information for TCP/IP-Based Internets*, Rose, M.; McCloghrie, K., May 1990

1156 *Management Information Base for Network Management of TCP/IP-Based Internets*, McCloghrie, K; Rose, M.T., May 1990

1157 *Simple Network Management Protocol (SNMP)*, Case, J.D.; Fedor M.; Schoffstall, M.L.; Davin, C., May 1990

1171 *Point-to-Point Protocol for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*, Perkins, D., July 1990

1212 *Concise MIB Definitions*, Rose, M.T. & McCloghrie, K. (editors), March 1991

1213 *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*, McCloghrie, K. & Rose, M.T. (editors), March 1991

1219 *On the Assignment of Subnet Numbers*, Tsuchiya, P, April 1991

1220 *Point-to-Point Protocol Extensions for Bridging*, Baker, F. (editor), April 1991

1229 *Extensions to the Generic-Interface MIB*, McCloghrie, K. (editor), May 1991

1231 *IEEE 802.5 Token-Ring MIB*, McCloghrie, K.; Fox, R.; Decker, E., May 1991

1232 *Definitions of Managed Objects for the DS1 Interface Type*, Baker, F. & Kolb, C. (editors), May 1991

1243 *AppleTalk Management Information Base*, Waldbusser, S. (editor), July 1991

1245 *OSPF Protocol Analysis*, Moy, J. (editor), July 1991

1247 *OSPF Version 2*, Moy, J., July 1991

1253 *OSPF Version 2: Management Information Base*, Baker, F.; Coltun, R., August 1991

1267 *A Border Gateway Protocol 3 (BGP-3)*, Lougheed, K.; Rekhter, Y., October 1991

1268 *Application of the Border Gateway Protocol in the Internet*, Rekhter, Y. & Gross, P. (editors), October 1991

1269 *Definitions of Managed Objects for the Border Gateway Protocol (Version 3)*, Willis, S.; Burruss, J.W., October 1991

1284 *Definitions of Managed Objects for the Ethernet-Like Interface Types*, Cook, J. (editor), December 1991

1289 *DECnet Phase IV MIB Extensions*, Saperia, J., December 1991

1293 *Inverse Address Resolution Protocol*, Brown, C., January 1992

1294 *Multiprotocol Interconnect over Frame Relay*, Bradley, T.; Brown, C.; Malis, A., January 1992

1315 *Management Information Base for Frame Relay DTEs*, Brown, C.; Baker, F.; Carvalho, C., April 1992

1331 *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*, Simpson, W., May 1992

1332 *The PPP Internet Protocol Control Protocol (IPCP)*, McGregor, G., May 1992

1333 *PPP Link Quality Monitoring*, Simpson, W., May 1992

1340 *Assigned Numbers*, Reynolds, J.; Postel, J., July 1992

1354 *IP Forwarding Table MIB*, Baker, F., July 1992

1356 *Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode*, Malis, A.; Robinson, D.; Ullman, R., August 1992

1370 *Applicability Statement for OSPF*, Internet Architecture Board, October 1992

1376 *The PPP DECnet Phase IV Control Protocol (DNCP)*, Senum, S., November 1992

1378 *The PPP AppleTalk Control Protocol (ATCP)*, Parker, B., November 1992

1388 *RIP Version 2-Carrying Additional Information*, Malkin, G., January 1993

1389 *RIP Version 2 MIB Extension*, Malkin, G., January 1993

1397 *Default Route Advertisement in BGP2 and BGP3 Versions of the Border Gateway Protocol*, Haskin, D., January 1993

1403 *BGP OSPF Interaction*, Varadhan, K., January 1993

1434 *Data Link Switching: Switch-to-Switch Protocol*, Dixon. R.; Kushi, D., March 1993

1490 *Multiprotocol Interconnect over Frame Relay*, Bradley, T; Brown, C.; Malis, A., July 1993

1493 *Definitions of Managed Objects for Bridges*, Decker, E.; Langille, P.; Rijsinghani, A.; McCloghrie, K., July 1993

1525 *Definitions of Managed Objects for Source Route Bridges*, Decker, E.; McCloghrie, K.; Langille, P.; Rijsinghani, A., September 1993

1548 *The Point-to-Point Protocol (PPP)*, Simpson, W., December 1993

1549 *PPP in HDLC Framing*, Simpson, W. (editor), December 1993

1551 *Novell IPX over Various WAN Media (IPXWAN)*, Allen, M., December 1993

1570 *PPP LCP Extensions*, Simpson, W. (editor), January 1994

1600 *Internet Official Protocol Standards*, Postel, J. (editor), March 1994

1638 *PPP Bridging Control Protocol (BCP)*, Baker, F., Bowen, R., June 1994

Index

Numerics

D

E

K

L

M

T

Communicating Your Comments to IBM

Multiprotocol Network Program
Configuration Guide
Version 1 Release 3

Publication No. SC31-6691-01

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:

  United States and Canada: **1-800-227-5088**

- If you prefer to send comments electronically, use this network ID:
  - IBM Mail Exchange: **USIB2HPD at IBMMAIL**
  - IBMLink: **CIBMORCF at RALVM13**
  - Internet: **USIB2HPD@VNET.IBM.COM**

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies.

Help us help you!

Multiprotocol Network Program
Configuration Guide
Version 1 Release 3

Publication No. SC31-6691-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

Specific Comments or Problems:

Please tell us how we can improve this book:

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name

Address

Company or Organization

Phone No.

Help us help you!
SC31-6691-01

Cut or F
Along Li

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

Information Development
Department E15
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape | **Please do not staple** | Fold and Tape

SC31-6691-01

Cut or I
Along L

Part Number: 73G6427

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber

The IBM 6611 Network Processor and Multiprotocol Network Program Library

IBM Multiprotocol Network Program Configuration Guide, SC31-6691
IBM Multiprotocol Network Program Operations and Problem Management, SC31-6692
IBM 6611 Network Processor Cable Labels, GX27-3910
IBM 6611 Network Processor Connectivity poster, SX75-0096
IBM 6611 Network Processor Customer Setup Guide, GA27-3993
IBM 6611 Network Processor Introduction and Planning Guide, GK2T-0334
IBM 6611 Network Processor Maintenance Information, GA27-3941
IBM 6611 Network Processor Network Management Reference, GC30-3567
IBM 6611 Network Processor Operations Pocket Guide, GX27-3909
IBM 6611 Network Processor Translated Safety Information, GA27-3954

73G6427

SC31-6691-01