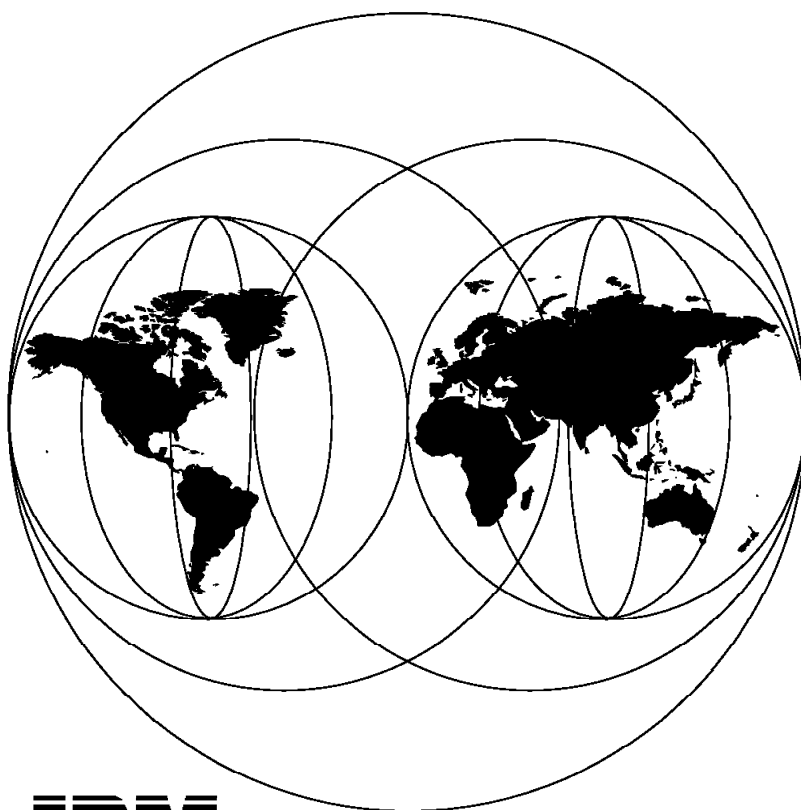


IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios - Volume I

June 1997



**International Technical Support Organization
Raleigh Center**



International Technical Support Organization

SG24-4446-02

**IBM 2210 Nways Multiprotocol Router Description
and Configuration Scenarios - Volume I**

June 1997

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix A, "Special Notices" on page 763.

Third Edition (June 1997)

This edition applies to Version 1 Release 1 of the Nways Multiprotocol Routing Services, 5765-B86, for use with the IBM 2210 Nways Multiprotocol Router.

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

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

© **Copyright International Business Machines Corporation 1995 1997. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Preface	ix
The Team That Wrote This Redbook	ix
Comments Welcome	xii
 Chapter 1. IBM 2210 Introduction	 1
1.1 Models of the IBM 2210	1
1.2 Indicators on the IBM 2210	9
1.3 The Reset Button on the IBM 2210	9
1.4 Networks Supported by the IBM 2210	10
1.5 Software Package	10
1.6 Accessing the IBM 2210	14
1.6.1 Local Access	14
1.6.2 Remote Access	15
1.6.3 Examples	15
 Chapter 2. MRS Overview	 19
2.1 Introduction	19
2.2 Boot Files and Boot Processes	19
2.3 2210 Configuration	20
2.4 MRS User Interface	22
2.4.1 Configuring User Access	22
2.4.2 Nways MRS Process Structure	24
2.4.3 QUICK CONFIG Process	25
2.4.4 CONFIG ONLY Process	28
2.4.5 OPCON Process	29
2.4.6 CONFIG Process	30
2.4.7 GWCON Process	35
2.4.8 MONITR Process	36
2.4.9 MOSDDT Process	37
2.4.10 BOOT CONFIG Process	37
2.5 The Event Logging System (ELS)	38
2.5.1 Controlling Message Display	42
2.6 The IBM 2210 Configuration Program	42
2.6.1 Hardware and Software Requirements	42
2.6.2 Anonymous FTP Site for the IBM 2210 Multiprotocol Router	43
2.6.3 Installing the Configuration Program	44
2.6.4 Migration Support for Down-Level Configuration Files	46
2.6.5 An Overview of the IBM 2210 Configuration Program	47
2.6.6 The 2210 Navigation Window	47
2.6.7 Configure Pull-Down Menu (on the Navigation Window)	51
2.6.8 Options Pull-Down Menu (on the Navigation Window)	52
2.6.9 Validating Configuration Files	52
2.6.10 Sending/Retrieving the Configuration File	53
2.7 IBM 2210 PROM Load/Dump Program	54
2.7.1 Loading the PROM Load/Dump Program	55
 Chapter 3. Interfaces	 57
3.1 The LAN Interfaces	57
3.1.1 The Ethernet Interface	57
3.1.2 The Token-Ring Interface	58
3.2 Configure the LAN Interfaces	60

3.2.1	Configuring the Ethernet Interface	60
3.2.2	Configuring the Token-Ring Interface	64
3.3	Monitoring the LAN Interfaces	74
3.3.1	Monitoring the Ethernet Interface	74
3.3.2	Monitoring the Token-Ring Interface	76
3.4	Configuring Serial Interfaces	77
3.4.1	The X.25 Interface	78
3.4.2	X.25 Implementation	78
3.4.3	Configuring X.25	79
3.4.4	X.25 Configuration Commands	79
3.4.5	X.25 Configuration Steps	83
3.4.6	Monitoring X.25	83
3.4.7	The Frame Relay Interface	84
3.4.8	Configuring Frame Relay	85
3.4.9	Frame Relay Configuration Steps	86
3.4.10	Monitoring Frame Relay	87
3.4.11	The Point-to-Point Interface	88
3.4.12	Configuring PPP	88
3.4.13	PPP Configuration Steps	88
3.4.14	Monitoring Point-to-Point	89
3.4.15	The SDLC Interface	89
3.4.16	Configuring SDLC	92
3.4.17	SDLC Configuration Steps	92
3.4.18	Monitoring SDLC	93
3.4.19	The SDLC Relay Interface	94
3.4.20	Configuring SDLC Relay	94
3.4.21	SDLC Relay Configuration Steps	95
3.4.22	Monitoring SDLC Relay	96
3.4.23	The V.25bis Network Interface	96
3.4.24	Configuring V.25bis	100
3.4.25	V.25bis Configuration Steps	101
3.4.26	Monitoring V.25bis and Dial Circuits	102
3.5	The ISDN Interface	102
3.5.1	ISDN Driver Support	103
3.5.2	ISDN Implementation	103
3.5.3	ISDN Configuration Commands	105
3.5.4	ISDN Configuration Steps	105
3.5.5	Frame Relay over ISDN Configuration	108
3.5.6	Monitoring ISDN and Dial Circuits	108
Chapter 4.	Bridging	111
4.1	Introduction to Bridging	111
4.2	Bridging Methods	112
4.2.1	Transparent Bridging (STB)	113
4.2.2	Source Route Bridging (SRB)	114
4.2.3	Source Route Transparent Bridging (SRT)	116
4.2.4	Source Route-Translational Bridge (SR-TB)	116
4.2.5	Tunnel Bridge	117
4.2.6	Bridging Methods Supported by the IBM 2210	119
4.2.7	Bridging Methods Supported between the 2210 and the 6611	121
4.3	Bridging Configuration Commands	122
4.3.1	Basic Bridging Configuration Commands	124
4.3.2	Configuration Commands for SRB Bridging	126
4.3.3	Configuration Commands for Spanning Tree Protocol	127
4.3.4	Configuration Commands for the Filtering Database	129

4.3.5 Configuration Commands for the SR-TB Bridging	130
4.3.6 Configuration Commands for the Protocol Filtering	132
4.3.7 Configuration Commands for the Tunnel Bridging	132
4.3.8 Configuration Commands for the TCP/IP Host Services	135
4.4 Bridging Scenarios and Configurations	138
4.4.1 Scenario 1: STB Implementation	139
4.4.2 Scenario 2: STB Interoperability with the 6611	149
4.4.3 Scenario 3: SRB Implementation	160
4.4.4 Scenario 4: SRB Interoperability with the IBM 6611 Network Processor	180
4.4.5 Scenario 5: SRT Bridge Implementation and Interoperability	196
4.4.6 Scenario 6: SR-TB Implementation with NetBIOS Facilities	209
4.4.7 Scenario 7: SR-TB Interoperability with the IBM 6611 Network Processor	233
4.4.8 Scenario 8: IP Tunnel Bridge Implementation via X.25 Network	247
4.4.9 Scenario 9: SRB Source Routing Bridge with Frame Relay	263
Chapter 5. Frame Relay Boundary Access Node	275
5.1 About the Boundary Access Node Feature	275
5.2 Benefits of BAN	276
5.3 How BAN Works	277
5.4 Bridged versus DLSw BAN	277
5.4.1 Which Method Should You Use	279
5.5 Using the BAN Feature	279
5.6 Using Multiple DLCIs for BAN Traffic	280
5.7 BAN Scenario	280
Chapter 6. LAN Network Manager Support	289
6.1 LNM Implementation in IBM 2210	289
6.2 LNM Configurations Commands	290
6.2.1 LNM Scenarios and Configuration	290
6.2.2 LNM Considerations	293
Chapter 7. IP Routing Protocols	295
7.1 Interior and Exterior Gateway Protocols	295
7.2 Routing Algorithms	296
7.2.1 Static Routing	296
7.2.2 Distance Vector Routing	297
7.2.3 Link State Routing	302
7.3 Routing Information Protocol (RIP)	303
7.3.1 Protocol Description	303
7.4 Open Shortest Path First (OSPF)	305
7.4.1 OSPF Terminology	305
7.4.2 Protocol Description	309
7.5 Border Gateway Protocol (BGP4)	320
7.5.1 Protocol Description	320
7.6 ARP Subnet Routing	325
7.6.1 The Concept of ARP Subnet Routing	326
7.7 IP Multicasting	326
7.7.1 IGMP	327
7.7.2 Multicast OSPF (MOSPF)	327
7.7.3 Distance Vector Multicast Routing Protocol (DVMRP)	328
Chapter 8. The IBM 2210 as an IP Router	329
8.1 IP Implementation	329

8.1.1	General IP Parameters	330
8.1.2	Interface Address Assignments	331
8.1.3	RIP Implementation in IBM 2210	331
8.1.4	OSPF Implementation	332
8.1.5	MOSPF	335
8.1.6	DVMRP	335
8.1.7	BGP4 Implementation	335
8.1.8	Static Route Implementation	336
8.1.9	IP Filters	337
8.1.10	IP Source Routing	337
8.1.11	Access Controls	337
8.1.12	BootP Implementation	338
8.1.13	Telnet Implementation	338
8.1.14	SNMP Implementation	339
8.1.15	TFTP Implementation	340
8.1.16	ARP-Subnet Routing	340
8.2	Configuring IP on the IBM 2210	341
8.2.1	IP Configuration Commands	341
8.2.2	IP Configuration Steps	343
8.2.3	IP Monitoring	348
8.3	Configuring Dynamic Routing Using RIP	348
8.3.1	RIP Configuration Commands	349
8.3.2	RIP Configuration Steps	350
8.3.3	RIP Monitoring	352
8.4	Configuring Dynamic Routing Using OSPF	352
8.4.1	OSPF Configuration Commands	352
8.4.2	OSPF Configuration Steps	353
8.4.3	OSPF Monitoring	355
8.5	Configuring BGP4	356
8.5.1	BGP Configuration Commands	357
8.5.2	BGP4 Configuration Steps	357
8.5.3	BGP4 Monitoring	358
8.5.4	Configuring SNMP	359
8.5.5	SNMP Configuration Steps	359
8.5.6	Monitoring SNMP	360
8.5.7	Configuring DVMRP	361
8.5.8	Monitoring DVMRP	362
8.6	Scenarios and Configuration Examples	362
8.6.1	Scenario 1: Configuring IP RIP over a PPP	362
8.6.2	Scenario 2: Configuring IP RIP over a PPP (ISDN)	371
8.6.3	Scenario 3: Configuring OSPF with 6611 Interoperability over a PPP	381
Chapter 9.	IPX Routing and Configuration	405
9.1	RIP Overview	405
9.1.1	RIP Packet Format	406
9.1.2	Route Selection	407
9.2	SAP Overview	408
9.2.1	SAP Packet Format	409
9.2.2	Get Nearest Server Request Handling	410
9.3	IPXWAN Overview	410
9.3.1	IPXWAN Packet Format	411
9.4	IPX Configuration on the IBM 2210	413
9.4.1	IPX Configuration Commands	413
9.4.2	IPX Configuration Overview	414
9.4.3	Further IPX Configuration Considerations	416

9.5 Enhancements to IPX with MRS V1R1	417
9.6 IPX Configuration Scenarios	418
9.6.1 Scenario 12: Routing IPX over X.25	418
9.6.2 Scenario 2: Routing IPX over PPP, between an IBM 2210 and an IBM 6611 Network Processor	440
Chapter 10. Data Link Switching	449
10.1 Data Link Switching Overview	449
10.1.1 DLSw Circuit Establishment	449
10.2 DLSw on the IBM 2210	451
10.2.1 Data Link Switching Supported Topology	452
10.2.2 Local Data Link Switching	452
10.2.3 Remote Data Link Switching	452
10.2.4 DLSw Using MOSPF	453
10.3 DLSw Configuration on the IBM 2210	453
10.3.1 DLSw Configuration Commands	453
10.3.2 DLSw Configuration Overview	454
10.3.3 Further DLSw Configuration Considerations	456
10.4 DLSw Enhancements with V1R2 of Nways MRNS Software	456
10.5 DLSw Enhancements with V1R1 of Nways MRS Software	458
10.6 DLSw Configuration Scenarios	459
10.6.1 Scenario 1: DLSw between Two 2210s over PPP	460
10.6.2 Scenario 2: DLSw between Two 2210s and 6611 over Frame Relay	484
10.7 DLSw RFC 1795 Implementation in IBM 2210	508
10.8 DLSw and NetBIOS Commands	510
10.8.1 DLSw and NetBIOS Scenarios and Configuration	510
Chapter 11. Features and Facilities	525
11.1 EasyStart Feature	525
11.2 EasyStart Scenario and Configuration	525
11.2.1 EasyStart Scenario and Configuration with RS/6000	525
11.3 Bandwidth Reservation (BRS)	530
11.3.1 Introduction to Bandwidth Reservation (BRS)	530
11.3.2 Bandwidth Reservation (BRS) Configuration Commands	533
11.3.3 Scenario 1: Bandwidth Reservation (BRS) with IP, IPX and Bridging	536
11.4 MAC Filtering (MCF)	566
11.4.1 Introduction to MAC Filtering (MCF)	566
11.4.2 Sliding Window Filter	570
11.4.3 MAC Filtering (MCF) Configuration Commands	570
11.4.4 Scenario 2: MAC Filtering (MCF)	574
11.5 WAN Restoral (WRS)	599
11.5.1 Introduction to WAN Restoral (WRS)	599
11.5.2 WAN Restoral Configuration	600
11.5.3 Scenario 3: WAN Restoral (WRS) Implementation with IP, DLSw and Bridging	608
11.5.4 Scenario 4: WAN Restoral (WRS) Implementation with IP, DLSw and Bridging using ISDN	641
11.6 WAN Reroute Feature	665
11.7 WAN Reroute Implementation in the IBM 2210	665
11.8 Frame Relay Enhancements	666
11.9 WAN Reroute Commands	667
11.9.1 Scenario 5: WAN Reroute Implementation	667
11.9.2 Scenario 6: WAN Reroute Implementation Using ISDN	672
11.9.3 Additional Configuration for 2210B and 2210C	682
11.10 Dial-on-Demand	683

11.10.1	Introduction to Dial-on-Demand	683
11.10.2	Dial-on-Demand Configuration Commands	685
11.10.3	Scenario 7: Dial-on-Demand Implementation over IP	690
11.10.4	Scenario 8: Dial-on-Demand Implementation over IP Using ISDN	701
11.11	NetBIOS Facilities	713
11.11.1	The NetBIOS Name Caching Facility	713
11.11.2	NetBIOS Filtering Facility	723
11.12	Data Compression for PPP Interface	731
11.12.1	Introduction to Data Compression	731
11.12.2	Data Compression Configuring Commands	733
11.12.3	Scenario 9: PPP Data Compression with Bridging	734
11.13	PPP Authentication Protocols	747
11.13.1	Introduction to PPP Authentication Protocols	747
11.13.2	Password Authentication Protocol (PAP)	748
11.13.3	Challenge-Handshake Authentication Protocol (CHAP)	748
11.13.4	PPP Authentication Protocols Configuration Commands	748
11.13.5	Scenario 10: PPP Authentication Protocol with Bridging	750
Appendix A. Special Notices		763
Appendix B. Related Publications		767
B.1	International Technical Support Organization Publications	767
B.2	Redbooks on CD-ROMs	767
B.3	Other Publications	767
How to Get ITSO Redbooks		769
How IBM Employees Can Get ITSO Redbooks		769
How Customers Can Get ITSO Redbooks		770
IBM Redbook Order Form		771
Index		773
ITSO Redbook Evaluation		775

Preface

This redbook describes the IBM 2210 Nways Multiprotocol Router and its operating software, the Nways Multiprotocol Routing Services (MRS). It provides a technical overview of functions implemented by the IBM 2210 such as bridging, multiprotocol routing, data link switching, frame-relay boundary access node and LAN Network Manager support. One chapter is dedicated to the important special features implemented by the IBM 2210, such as WAN Restoral, WAN Reroute, Dial-on-Demand, Bandwidth Reservation, and EasyStart. The redbook also contains descriptions of practical scenarios and implementations, including topology details and console commands for the IBM 2210.

This redbook will help you build a routing environment using the IBM 2210 Nways Multiprotocol Router. With detailed step-by-step implementation of various scenarios, this redbook can be used as a sample when configuring not only the basic routing but also all the additional special features available in this product.

Some knowledge of networking architectures and protocols is assumed.

The Team That Wrote This Redbook

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

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

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

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

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

Mohammad Shabani is a program manager for the Early Support Program in EMEA for networking hardware division products such as ATM, routers, Intelligent Hubs, etc. in Hursley Park, Winchester (UK).

Noboru Umenai is an I/T Engineer in Japan. He has two years of experience in the multiprotocol network field. His areas of expertise include IP networks. He has written extensively on ISDN Interface, WRS, DOD, PAP and CHAP, and PPP data compression.

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

The first edition of this book was designed and managed by:

Mohammad Shabani
Systems Management and Networking ITSO Center, Raleigh.

The authors of the first edition were:

Jan Maarten De Klein
IBM Netherlands

Jerome Mareau
IBM France

John Sutch
IBM UK

The second edition was designed and managed by:

Mohammad Shabani
Ricardo Haragutchi

The authors of the second edition were:

Arthur Alexiou
IBM Australia

Denise Citti de Lauro
IBM Brazil

Enio Cervelini
IBM Brazil

Hans Mattsson
IBM Sweden

Thanks to the following people for the invaluable advice and guidance provided in the production of earlier editions:

Aroldo Yuji Yai
Barry Nusbaum
Carla Sadtler
David Boone
Gail Wojton

John Parker
Martin Murhammer
Mick Lugton
Paul Brown
Shawn Walsh
Volkert Kreuk
Systems Management and Networking ITSO Center, Raleigh.

Acee Lindem
Adel Fahmy
Don Page
Ellen Cybrynski
Ellen Niemitalo
Eric Walls
Frank Pita
Gerry Graham
Hank Schuwarzell
John Baxter
Jon Houghton
Julia Holloway
Julio Vazquez
Karen Heron
Mark Townsley
Peter Gayek
Pramod Patel
Rich Reid
Sallie Everette
Steve Klein
Steve Worley
Terri Davis
IBM Research Triangle Park (2210)

Bill McCauley
Bruce Gillooly
Dave Jacobson
Don Boston
Doug Flint
Gwen Adams
Imre Szabo
Isaac Allen
Janet Andersen
Jason Cornpropst
Jerry Sents
Jim Ayres
Keith Karlsson
Kevin McClain
Paul Shoytush
Pete Andrews
Rainer Jenke
Randy Worzella
Rosemary Cook
Skip Wilder
Szabo Imre
Timothy Smith
Wayne Taylor

Wes Moorehead

IBM Research Triangle Park (2216)

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

Comments Welcome

Your comments are important to us!

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

- Fax the evaluation form found in "ITSO Redbook Evaluation" on page 775 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Home Pages at the following URLs:

For Internet users <http://www.redbooks.ibm.com>

For IBM Intranet users <http://w3.itso.ibm.com/redbooks>

- Send us a note at the following address:

redbook@vnet.ibm.com

Chapter 1. IBM 2210 Introduction

This chapter provides an introduction to the IBM 2210, including a description of the hardware and an overview of the software package. Further information can be found in *IBM 2210 Nways Multiprotocol Router Maintenance Information* and *IBM 2210 Nways Multiprotocol Router Planning and Setup Guide*.

1.1 Models of the IBM 2210

The IBM 2210 is available in several models to accommodate the types of networks you want to support. Keep in mind that there are two memory choices that you must evaluate before deciding on which model best meets your needs. Each type of memory has a specific purpose and should be considered separately:

1. **Flash memory.** Flash memory is used to store a compressed version of the executable program product, IBM Nways Multiprotocol Routing Services (MRS, product number 5765-B86 V1R1), as well as one or more configuration images. Customers often desire to store more than one release of the code and multiple configuration images in flash as part of their management strategy.

The chart below shows the amount of flash memory consumed by each MRS V1R1 software code load.

Please note that only the x4x models have expandable flash memory. All the other models have a fixed amount of flash memory (either 2 MB or 4 MB, depending on the model).

Table 1. Flash Memory Consumption - Models 1X4, 1X8

Model	Amount of flash	Total number of banks	Number of banks consumed by one code load			
			Software preload feature code number			
			5121	5122	5123	5124
1s4	2 MB	32	20	22	24	N/A
1u4	2 MB	32	20	22	24	N/A
1s8	4 MB	64	20	22	24	27
1u8	4 MB	64	20	22	24	27

Note: Each configuration takes one bank.

Table 2. Flash Memory Consumption - Models 12T, 12E

Model	Amount of flash	Total number of banks	Number of banks consumed by one code load				
			Software preload feature code number				
			5002	5003	5005	5007	5008
12T	4 MB	64	20	22	25	42	48
12E	4 MB	64	20	22	25	42	48

Note: Each configuration takes one bank.

<i>Table 3. Flash Memory Consumption - Models 127, 128</i>						
Model	Amount of flash	Total number of banks	Number of banks consumed by one code load			
			Software preload feature code number			
			5023	5024	5026	5027
127	4 MB	64	24	27	44	50
128	4 MB	64	24	27	44	50
Note: each configuration takes one bank.						

<i>Table 4. Flash Memory Consumption - Models X4X without Adapter or with WAN concentration adapter</i>						
Model	Amount of flash	Total number of banks	Number of banks consumed by one code load			
			Software preload feature code number			
			5043	5044	5046	5047
14T	4 MB *	14 *	6	7	11	13
24T	4 MB *	14 *	6	7	11	13
24E	4 MB *	14 *	6	7	11	13
24M	4 MB *	14 *	6	7	11	13
Note: * double for 8 MB calculations. Each configuration takes one bank.						

<i>Table 5. Flash Memory Consumption - Models X4X with ISDN BRI Adapter</i>						
Model	Amount of flash	Total number of banks	Number of banks consumed by one code load			
			Software preload feature code number			
			5063	5064	5066	5067
14T	4 MB *	14 *	7	7	11	13
24T	4 MB *	14 *	7	7	11	13
24E	4 MB *	14 *	7	7	11	13
24M	4 MB *	14 *	7	7	11	13
Note: * double for 8 MB calculations. Each configuration takes one bank.						

<i>Table 6. Flash Memory Consumption - Models X4X with ISDN PRI Adapter</i>						
Model	Amount of flash	Total number of banks	Number of banks consumed by one code load			
			Software preload feature code number			
			5083	5084	5086	5087
14T	4 MB *	14 *	7	7	12	13
24T	4 MB *	14 *	7	7	12	13
24E	4 MB *	14 *	7	7	12	13
24M	4 MB *	14 *	7	7	12	13
Note: * double for 8 MB calculations. Each configuration takes one bank.						

<i>Table 7. Flash Memory Consumption - Models X4X with ATM Adapter</i>						
Model	Amount of flash	Total number of banks	Number of banks consumed by one code load			
			Software preload feature code number			
			5103	5104	5106	5107
14T	4 MB *	14 *	8	9	13	14
24T	4 MB *	14 *	8	9	13	14
24E	4 MB *	14 *	8	9	13	14
24M	4 MB *	14 *	8	9	13	14
Note: * double for 8 MB calculations. Each configuration takes one bank.						

2. **DRAM.** Dynamic random access memory provides the working memory for the 2210. The router code and router tables both run from DRAM. The amount of DRAM in a given 2210 will determine the size and complexity of the network it can support. There are three sizes of DRAM available for the x2x models: 4 MB, 8 MB, and 16 MB. There are four sizes of DRAM available for the x4x models: 4 MB, 8 MB, 16 MB, and 32 MB. Four megabytes (4 MB) of DRAM is the default for all models. The other DRAM sizes are available by the addition of the respective memory expansion feature. These memory expansion features are available as both factory- or field-installed features. Field-installed memory expansion features on the x2x models must be installed by trained service personnel. Field-installed memory expansion features on x4x models are customer-installable features. DRAM on models 1Sx and 1Ux is not upgradeable.

Use of the 2210STOR EXEC is recommended prior to each machine order to ensure the correct configuration is ordered. The following chart is provided as a guideline:

<i>Table 8. DRAM Requirement Estimates Per Software Load</i>			
Models	Software Description	Minimum DRAM Required	Preload Feature Code Number
1x4	IP+ISDN BRI	4	5121
	IP+IPX+ISDN BRI	4	5122
1x8	IP+DLSw+ISDN BRI	8	5123
	IP+IPX+DLSw+ISDN BRI	8	5124
12T	IP+IPX	4	5002
12E	IP+IPX	4	5003
	IP+IPX+DLSw	8	5005
	IP+DLSw+APPN	16	5007
	All Protocol+APPN	16	5008
127	IP+DLSw+ISDN BRI	8	5023
128	IP+IPX+DLSw+ISDN BRI	8	5024
	IP+DLSw+APPN+ISDN BRI	16	5026
	All Protocol+APPN+ISDN BRI	16	5027
x4x Empty or with WAN Connection Adapter	IP+DLSw	8	5043
	IP+IPX+DLSw	8	5044
	IP+DLSw+APPN	16	5046
	All Protocol+APPN	16	5047
x4x with ISDN BRI Adapter	IP+DLSw+ISDN BRI	8	5063
	IP+IPX+DLSw+ISDN BRI	8	5064
	IP+DLSw+APPN+ISDN BRI	16	5066
	All Protocol+APPN+ISDN BRI	16	5067
x4x with ISDN PRI Adapter	IP+DLSw+ISDN PRI	8	5083
	IP+IPX+DLSw+ISDN PRI	8	5084
	IP+DLSw+APPN+ISDN PRI	16	5086
	All Protocol+APPN+ISDN PRI	16	5087
x4x with ATM Adapter	IP+DLSw+ATM	8	5103
	IP+IPX+DLSw+ATM	8	5104
	IP+DLSw+APPN+ATM	16	5106
	All Protocol+APPN+ATM	16	5107
Note: All Protocol includes DLSw and LNM.			

Table 9 shows the different models and the offerings of the IBM Nways Multiprotocol Routing Services that are available.

Note: Certain models of the IBM 2210 support ISDN. You cannot use one of the standard WAN ports for ISDN. Software support for ISDN must be ordered separately.

Table 9. IBM 2210 Models							
Model	Replaced by model	LAN	No. of WANs (See Note)	ISDN BRI Port	Flash Memory (base/max)	DRAM (base/max)	Adapter Slot ²
1S4	-	Ethernet	1 ³	1 ³	2 MB/2 MB	4 MB/4 MB	No
1S8	-	Ethernet	1 ³	1 ³	4 MB/4 MB	8 MB/8 MB	No
1U4	-	Ethernet	1 ³	1 ³	2 MB/2 MB	4 MB/4 MB	No
1U8	-	Ethernet	1 ³	1 ³	4 MB/4 MB	8 MB/8 MB	No
121 ¹	12T	Token-Ring	2	0	2 MB/2 MB	4 MB/16 MB	No
122 ¹	12E	Ethernet	2	0	2 MB/2 MB	4 MB/16 MB	No
123 ¹	12T	Token-Ring	2	0	4 MB/4 MB	8 MB/16 MB	No
124 ¹	12E	Ethernet	2	0	4 MB/4 MB	8 MB/16 MB	No
12T	-	Token-Ring	2	0	4 MB/4 MB	4 MB/16 MB	No
12E	-	Ethernet	2	0	4 MB/4 MB	4 MB/16 MB	No
125 ¹	127	Token-Ring	2	1	2 MB/2 MB	4 MB/16 MB	No
126 ¹	128	Ethernet	2	1	2 MB/2 MB	4 MB/16 MB	No
127	-	Token-Ring	2	1	4 MB/4 MB	4 MB/16 MB	No
128	-	Ethernet	2	1	4 MB/4 MB	4 MB/16 MB	No
14T	-	Token-Ring	4	opt	4 MB/12 MB	4 MB/32 MB	Yes
24T	-	2 (two) Token-Ring	4	opt	4 MB/12 MB	4 MB/32 MB	Yes
24E	-	2 (two) Ethernet	4	opt	4 MB/12 MB	4 MB/32 MB	Yes
24M	-	1 (one) Token-Ring, 1 (one) Ethernet	4	opt	4 MB/12 MB	4 MB/32 MB	Yes

¹ Discontinued models.

² Support for ISDN BRI, ISDN PRI, ATM, 4 and 8 serial port adapters.

³ Only one of the two ports (either WAN or ISDN BRI) can be configured/used at any given time on these models.

Note: The standard WAN ports on the IBM 2210 will support any of these physical interfaces:

- EIA RS 232-D/V.24
- V.35
- V.36
- X.21

The ISDN BRI port on the 1Sx models provides a four-wire twisted pair S/T interface with a RJ-45 connector. The ISDN BRI port will support the same signaling specifications as the other 2210 models, namely EuroISDN in Europe, INS-64 in Japan, National ISDN-1 and -2, AT&T 5ESS and Nortel DMS-100 in North America, and TS 013 in Australia.

The 1Ux models include a fully-integrated NT-1, incorporating the "U" interface. This support is provided at no additional cost compared with the S/T interface models. This saves customers the expense and inconvenience of having to purchase and configure a standalone NT-1.

Table 10. Features Supported by Model

Model	Integrated Modem Feature FC #2814	Second Service Port FC #2832	Adapter Enable Feature FC#3001/2	8 MB DRAM Memory FC #4008	16 MB DRAM Memory FC #4016	32 MB DRAM Memory FC #4032	4 MB Flash Memory FC #4104	8 MB DRAM Memory FC #4048/49	16MB DRAM FC #4056/577	ISDN BRI Adapter FC #3101	ISN PRI-T1/J1 Adapter FC #3107	ISN PRI-E1 Adapter FC #3108	25 Mbps ATM Adapter FC #3901	4-port WAN conc Adapter FC #3120	8-port WAN conc Adapter FC #3121	8 MB DRAM Memory FC #4108
1S4	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no
1S8	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no
1U4	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no
1U8	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no
121	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no	no	no
122	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no	no	no
123	no	no	no	no	no	no	no	n/a	yes	no	no	no	no	no	no	no
124	no	no	no	no	no	no	no	n/a	yes	no	no	no	no	no	no	no
12T	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no	no	no
12E	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no	no	no
125	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no	no	no
126	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no	no	no
127	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no	no	no
128	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no	no	no
14T	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes	yes	yes	yes	yes
24T	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes	yes	yes	yes	yes
24E	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes	yes	yes	yes	yes
24M	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes	yes	yes	yes	yes

Note: Serial/LAN cables and power cords are common across all models.

The ports of the different models are shown in Figure 1 on page 7 through Figure 8 on page 8. The two models shown in each figure differ only in the amount of DRAM and flash memory they contain, as described above.

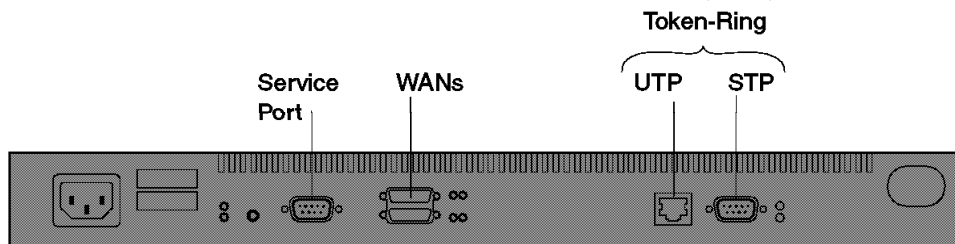


Figure 1. Models 121 and 12T

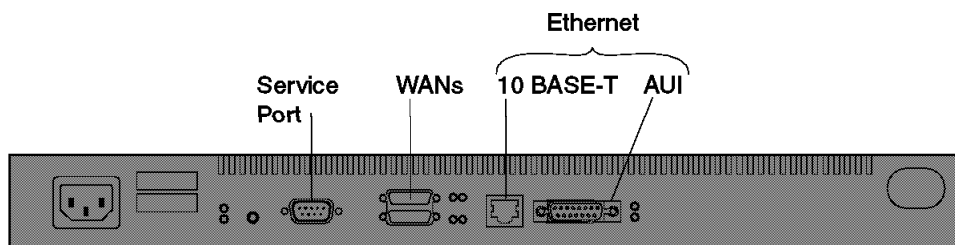


Figure 2. Models 122 and 12E

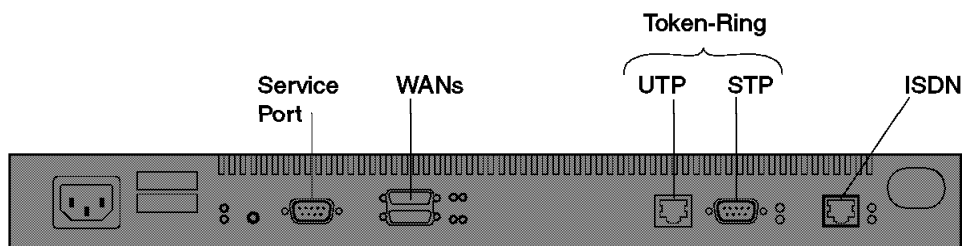


Figure 3. Models 125 and 127

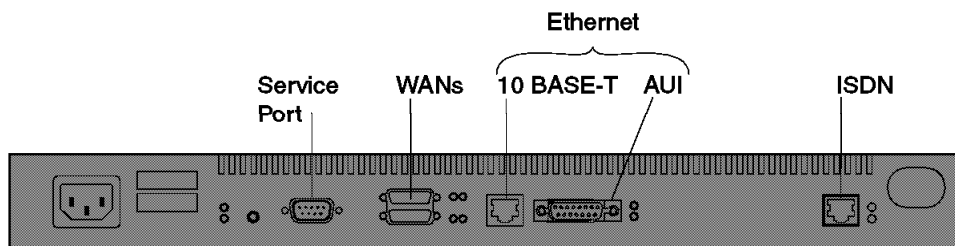


Figure 4. Models 126 and 128

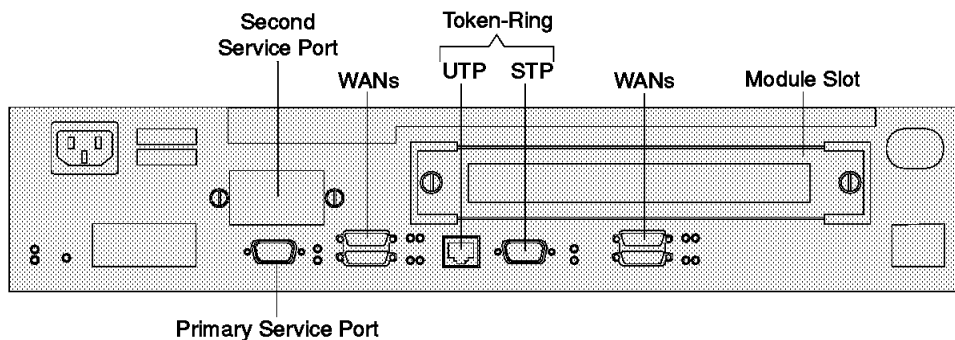


Figure 5. Models 14T

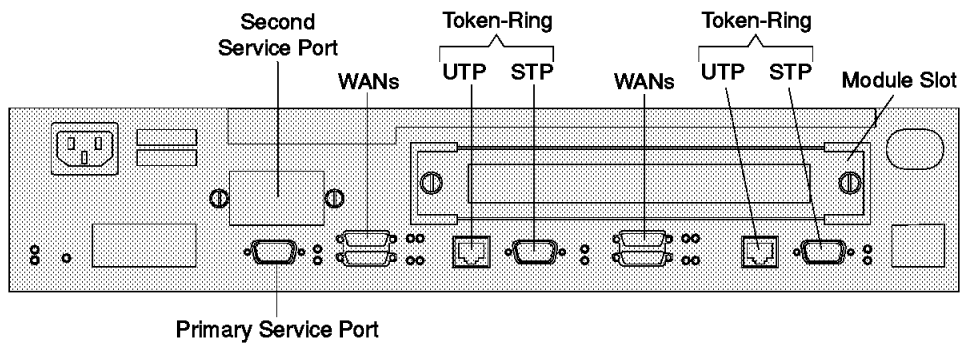


Figure 6. Models 24T

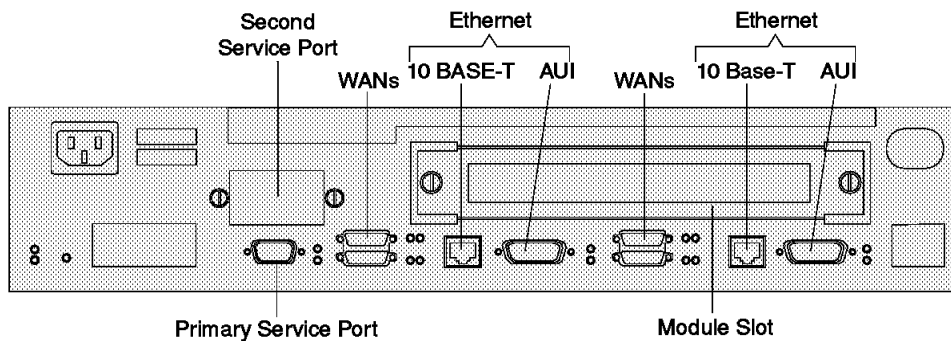


Figure 7. Models 24E

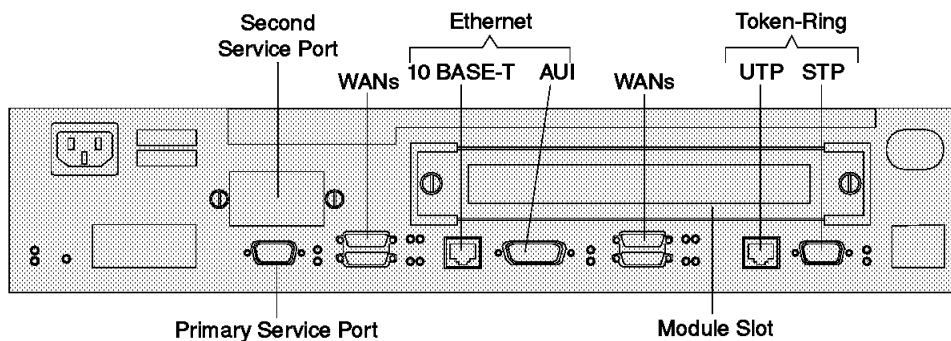


Figure 8. Models 24M

The double-density models support an additional service port and an adapter slot that can support ISDN basic rate, ISDN primary rate and ATM. The availability of these adapter cards is defined in the announcement letter.

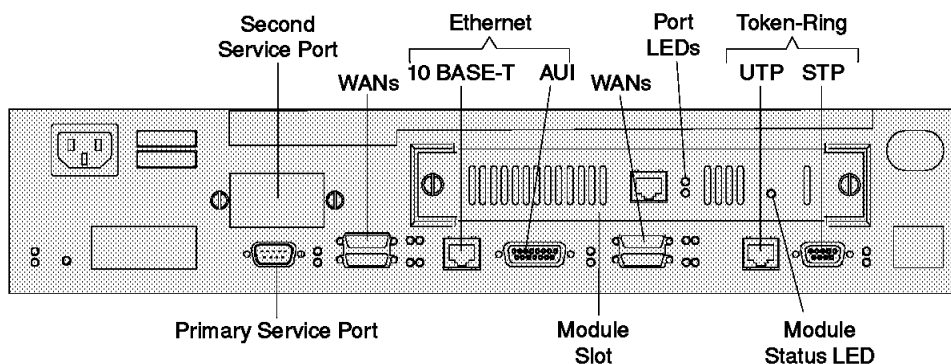


Figure 9. Model 24M with the ISDN Adapter

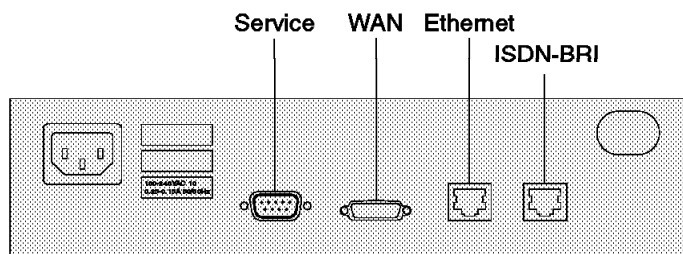


Figure 10. Model 1Sx and 1Ux

1.2 Indicators on the IBM 2210

The IBM 2210 has green and amber LEDs that indicate the status of the system and of individual ports. Green indicates normal operation; amber indicates a problem.

The LEDs are on both the front and the back of the IBM 2210, so you can place it with either side facing forward. This is shown in Figure 11 and Figure 12.

Note: The figures shown are for Models 121 and 12T. The port LEDs are specific to each model.

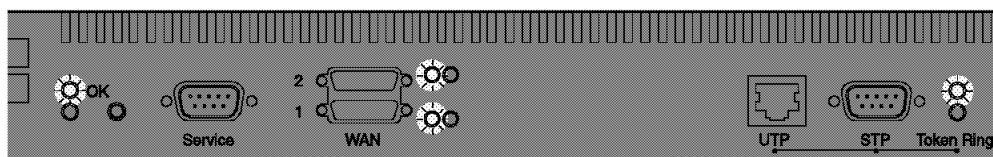


Figure 11. LEDs on the Port Side of Models 121 and 12T

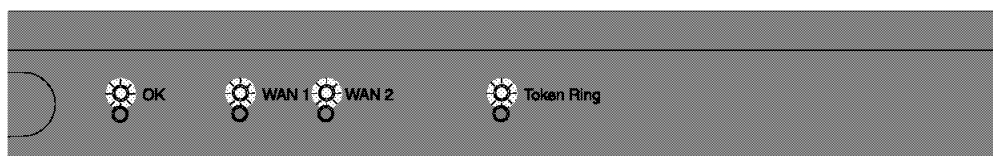


Figure 12. LEDs on the Side Opposite the Ports for Models 121 and 12T

1.3 The Reset Button on the IBM 2210

If you press the reset button, it will re-load the operational code. Also, if you press this button within 10 seconds of powering on, the 2210 will enter the extended power-on self-test (POST). Extended POST allows you to test memory more extensively than POST.

The reset button on the IBM 2210 is recessed to prevent accidental activation and is shown in Figure 13 on page 10.

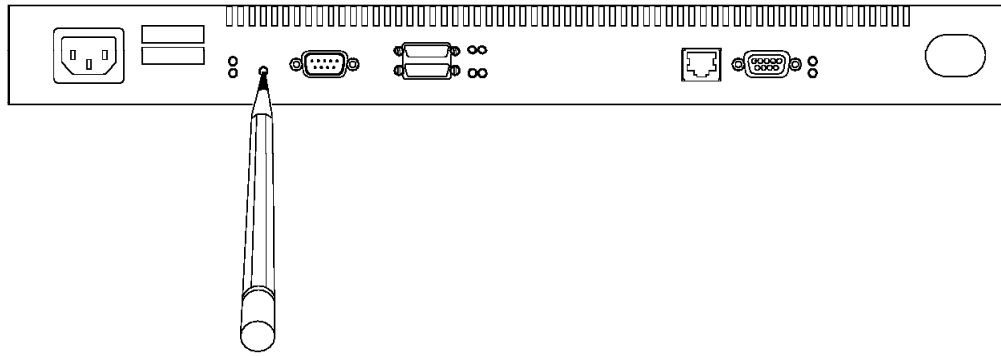


Figure 13. Reset Button on the IBM 2210 (Models 121, 122, 12T, 12E, 125, 126, 127 and 128)

For Models 14T, 24T, 24E and 24M the reset button is located below the AC power socket.

1.4 Networks Supported by the IBM 2210

The IBM 2210 supports the following LAN connections:

- Token-ring (IEEE 802.5) with STP or UTP connection
- Ethernet (IEEE 802.3) with AUI or 10BASE-T connection

Every IBM 2210 supports the following serial connections:

- EIA 232D/V.24
- V.35
- V.36
- X.21

Note: RS449 is also supported, using the V.36 cable available for the IBM 2210.

In addition to these serial connections, you can order optional support for ISDN.

1.5 Software Package

Nways Multiprotocol Routing Services (MRS, product number 5765-B86 V1R1) is the software that runs on the IBM 2210 and it comes as a base suite package, plus four separately orderable packages. It extends the function of IBM 2210 Nways Multiprotocol Routing Network Services (MRNS) Release 3 Enhanced.

In addition to current MRNS Release 3, the new MRS provide:

- APPN NN/ HPR /DLUR support
- ISDN BRI and PRI adapter and worldwide ISDN switch support
- ATM support including LAN emulation client and Classical IP
- Broad range of LAN, WAN and ATM network connectivity options
- Compatibility between products supported by the multiprotocol service software
- Many protocol enhancements

- Easy configuration, installation, and maintenance

1.5.1.1 MRS Base Suite versus Additional Routing Suite Contents

The *base suite* contains the following functional capabilities from a price/packaging perspective:

- TCP/IP, including OSPF
- Bridging (SR, TB, SRT and SR-TB)
- MAC filtering
- Data link controls (PPP, FR, X.25 and SDLC)
- AIW Version 1 DLSw(RFC 1795), including NetBIOS
- NetBIOS name caching/filtering
- SDLC primary and secondary support
- SDLC relay
- APPN/HPR/DLUR
- V.25bis
- Bandwidth reservation system
- EasyStart (with MRS)
- WAN reroute
- Specific device drivers where appropriate, that is, to support ISDN BRI or PRI and ATM

The Base + Additional Routing Suite includes the following additional protocols available in specific package options noted below. IPX is included in several package options; the other protocols listed are contained only where All Protocol is noted.

- IPX
- AppleTalk Phase 2
- Banyan VINES
- DECnet IV
- DECnet V/OSI
- BGP-4

The following table is a matrix of the MRS Release 1 software options available for pre-load and their designated OTC (one-time charge/cost) feature codes.

Note: Backup media diskettes will no longer be shipped with basic license orders. Only the configuration program diskettes and CD-ROM containing the documentation files will be provided (hard copy of software documents may be selected as optional deliverables).

In addition, a letter is included with instructions on how to retrieve the specific code option from the pre-loaded 2210 itself or from the appropriate 2210 Internet-accessible server. The IBM 2210 home page can be accessed at the following URL:

<http://www.raleigh.ibm.com/220/220prod.html>

<i>Table 11. OTC (One Time Charge/Cost)</i>						
Code Load Description	Media Feature Codes			Charge Feature Codes (US), (AP, LA, Canada)		
	12x	x4x	1Sx, 1Ux	12x	x4x	1Sx, 1Ux
Base Suite Options						
Base Program	5805	5805	5805	4000 A7RT	4003 A7RW	4006 A7TC
Additional Routing Suite Options						
Base + Additional Routing	5815	5815	5815	4001 A7RU	4004 A7TA	4007 A7TD
Field Install Additional Routing	5825	5828	5825	4002 A7RV	4005 A7TB	4008 A7TE

Table 11 is a matrix of the MRS Release 1 software options available for pre-load and their designated DSLO feature codes. Note that with DSLO (distributed systems license option), customers receive no media; only the appropriate discounted charge applies.

<i>Table 12. DSLO (Distributed Systems License Option)</i>						
Code Load Description	Media Feature Codes			Charge Feature Codes (US), (AP, LA, Canada)		
	12x	x4x	1Sx, 1Ux	12x	x4x	1Sx, 1Ux
Base Suite Options						
Base Program				4009 A7TF	4012 A7TJ	4015 A7TN
Additional Routing Suite Options						
Base + Additional Routing				4010 A7TG	4013 A7TK	4016 A7TN
Field Install Additional Routing				4011 A7TH	4014 A7TL	4017 A7TP

Chapter 2, “MRS Overview” on page 19 gives a more detailed description of Nways MRS.

Current licenses of IBM Nways Multiprotocol Routing Network Services (5765-368) for the IBM 2210 Nways Multiprotocol Router are entitled to migrate to the new IBM Nways Multiprotocol Routing Services for the 2210 at no additional charge. This may be done via the normal MES process. Current licenses of the charge feature codes listed below, both Basic and DSLO, must specify the associated Upgrade Feature Code shown when ordering the MES to transfer to the respective new IBM Nways Multiprotocol Routing Services license.

The following is a matrix of the MRS Release 1 software options available for pre-load and their designated OTC (one time charge/cost) feature codes (upgraded from MRNS 5765-368 basic licenses).

<i>Table 13. OTC (One Time Charge/Cost)</i>						
Code Load Description	Basic License Feature Code		Upgrade Feature Code		Basic License Feature Code 1	
	12x	x4x	12x	x4x	12x	x4x
Base Suite Options						
Base Program	4432 3391	4000 A4UU	4018 A7UV	4021 A7VB	4000	4003
Additional Routing Suite Options						
Base + Additional Routing	4433 3392	4001 A4UV	4019 A7UW	4022 A7VC	4001	4004
Base + ISDN	4434 4493		4018 A7UV		4000 2	
Base + Additional Routing + IPX	4764		4019 A7UW		4001 2	
Field Install Additional Routing	4765	4002 A4UW	4020 A7VA	4023 A7VD	4002	4005
Field Install Additional Routing + ISDN	4766		4020 A7VA		4002 2	

The following table is a matrix of the MRS Release 1 software options available for pre-load and their designated DSLO feature codes. Note that with DSLO (distributed systems license option), customers receive no media; only the appropriate discounted charge applies (upgraded from MRNS 5765-368 basic licenses).

Table 14. DSLO						
Code Load Description	DSLO License Feature		Upgrade Feature Code		DSLO License Feature Code 1	
	12x	x4x	12x	x4x	12x	x4x
Base Suite Options						
Base Program	4435	4003 A4VA	4024 A7VE	4027 A7VH	4009	4012
Additional Routing Suite Options						
Base + Additional Routing	4436	4004 A4VB	4025 A7VF	4028 A7VJ	4010	4013
Base + ISDN	4737		4024 A7VE		4009 2	
Base + Additional Routing + IPX	4767		4025 A7VF		4010 2	
Field Install Additional Routing	4768	4005 A4VC	4026 A7VG	4029 A7VK	4011	4014
Field Install Additional Routing + ISDN	4769		4026 A7VG		4011 2	

1 Yielded by upgrade feature code.

2 Since ISDN no longer is an additional charge feature, this migration will yield a standard Base or Base + Additional Routing license respectively.

1.6 Accessing the IBM 2210

You can access the IBM 2210 using the following methods:

- An ASCII terminal or ASCII terminal emulator attached directly to the IBM 2210 service port
- An ASCII terminal (or emulator) attached via a modem to the IBM 2210 service port
- A Telnet session

1.6.1 Local Access

You can access the IBM 2210 locally through its service port, using an ASCII terminal or emulator. The DEC VT100 terminal is supported, as well as devices that are configured to emulate it. The settings should be:

- No parity
- 8-bit word length
- 1 stop bit
- 300 bps-38.4 kbps bit rate

There are two possibilities of making the direct attachment to the IBM 2210:

- ASCII terminal (or emulator) - Standard RS-232 cable (25pin-to-25pin) - null modem - 25pin-to-9pin adapter - IBM 2210 Service Port connector.
- ASCII terminal (or emulator) - Crossover cable (wired internally to act as a null modem) - IBM 2210 service port connector. Note that if your crossover cable is a 25pin-to-25pin cable, you will need a 25pin-to-9pin adapter.

Some information:

The IBM part number for the null modem is p/n 10H5570.

The IBM part number for the 25pin-to-9pin adapter is p/n 74G0687.

When using an ASCII asynchronous terminal (or emulator), please refer to the emulator's manufacturer documentation to set the required parameters (8 bit, no parity, 1 stop bit, speed, computer communication port).

The IBM 3101, 3151 and 3161 Display Stations are also supported. For further information on these, please refer to *The IBM 2210 Nways Multiprotocol Router Planning and Setup Guide*.

1.6.2 Remote Access

You can access the IBM 2210 remotely using either Telnet or a terminal attached to the service port via a modem.

The modem must use asynchronous operation and support the AT command set.

The connection (modem to IBM 2210 service port) will be made through a standard RS-232 cable, either 25pin-to-9pin or 25pin-to-25pin with 25pin-to-9pin adapter.

The modem connected to the IBM 2210 must be set to auto-answer mode. The auto-answer mode is set through S register, which is on most asynchronous modems. For example, ATS0=2 means that the modem must detect two telephone rings before it auto-answers. Please refer to the modem's manufacturer documentation for information about the AT commands required to set your modem to operate in auto-answer mode.

1.6.3 Examples

This section provides examples of how to use TFTP and Zmodem to transfer the configurations to the routers.

1.6.3.1 Using TFTP

In this example, you will load your configuration yourfile.cfg from the workstation over the IP network and restart the router to use the newly loaded configuration as the current 2210 configuration. The router ID is 8.8.8.2 and the IP address of the remote workstation on is 8.8.8.1.

From an AIX or OS/2 window, type the following:

```
telnet 8.8.8.2
```

From the 2210 user interface:

1. Type yourid at the login prompt.
2. Type yourpassword at the password prompt.
3. Press Ctrl-p to return to the * prompt if necessary.
4. Press Enter whenever an expected prompt does not appear.
5. Type talk 6 to go to the Config> prompt.
6. Type boot to go to the Boot config> prompt.
7. Type tftp get and press Enter. Give the local file name (CONFIG).
8. Type 8.8.8.1 as the remote host.

9. Type `c:\cfg2210\yourfile.cfg` as the OS/2 full path and name if your file is on an OS/2 server **OR**
10. Type `/home/student/cfg2210/yourfile.cfg` as the AIX full path and name if your file is on an RS/6000 server.

Wait until you have received a message indicating a successful TFTP file transfer. You should see the following messages:

```
TFTP transfer complete, status: OK
Got hostname "xxxxx" - is this okay ? (Yes or (No)): Answer yes if correct.
Updating CONFIG; Do Not Interrupt!
Boot config>
```

The configuration changes must be applied for them to take effect. To do this restart the router as follows:

1. Press `Ctrl+p` to exit.
2. Type `restart` to activate new configuration.
3. Answer `yes` when asked "Are you sure?".

You will lose your telnet session when the router restarts.

1.6.3.2 Using Zmodem to Transfer a Configuration File

This session provides instruction to transfer configuration files to a 2210 router via Zmodem over the following modems:

1. Connect a Hayes-Compatible modem to the router

Note: One modem should already be connected to the remote workstation. You will connect a second modem to the router as described below.

Material Needed:

- Hayes-compatible modem
- RJ11 phone cable
- 9pin to 25pin adapter

Note: The modem should already be configured correctly.

2. Connect the modem as follows:
 - a. Disconnect the RS-232 cable from the IP workstation.
 - b. Use the 9pin-to-25pin adapter to connect the RS-232 cable from the 2210 to the modem.
 - c. Connect the RJ11 phone cable from the modem to the remote phone outlet.
 - d. Plug the power cord from the modem into the power outlet.
 - e. Turn on the modem power switch.
 - f. Plug the Router into the electrical outlet.
3. Dial into the router

Use ProComm Plus from the remote workstation to dial as follows:

- a. Press `Ctrl-Alt-Delete` to reboot the remote workstation.
- b. Select **DOS (No Network Drivers)**, from the menu within 30 seconds.
- c. Type `cd \pcplus` at the `c:\>` prompt to change to the ProComm Plus directory.
- d. Type `pcplus` to start ProComm Plus communications software.
- e. Follow directions to press any key after ProComm Plus initializes:

- 1) Press Alt+z for menu.
 - 2) Press Alt+d for Dialing Directory.
 - 3) Type m to dial manually.
 - f. Type AT and press Enter. AT must be uppercase.
 - g. Type ATDTnnnnn where nnnnn is the local phone extension listed on the wall in your lab.
- Note:** If the modems do not connect, try switching the remote modem off and on before retrying the dial sequence.
4. When connected, press Enter and log in to the 2210.

Note: After pressing Enter if you do not receive the login prompt or *, there may be a baud rate mismatch. The modems are 2400 baud. Send a break character to the router: press Alt+b in ProComm Plus, then b, then Enter.
 5. Transfer the new configuration file to the router using Zmodem software.

Note: Experience has shown that Zmodem in some software packages has problems when the file is on floppy disk that it does not have when the same file is on the hard drive.
 6. From the router user interface, do the following:
 - a. Press Ctrl+p to return to the * prompt, if necessary.
 - b. Type reload to begin reload.
 - c. Answer y when asked "Are you sure?".
 - d. Press Ctrl+c to interrupt load to go to Bootstrap Monitor.
 - e. Type ? to look at the Bootstrap Monitor menu.
 - f. Type zc to begin the Zmodem configuration process to send configuration file.
 - g. Answer y when asked "Are you sure?".
 7. From the ProComm Plus panel, do the following:
 - a. Press Alt+z to look at menu.
 - b. Press Page Up to choose Send files.
 - c. Type z to choose Zmodem.
 - d. Type c:\yourfile.cfg as the path and file name of your file.
 - e. Press Enter to get the Watch Progress window.
 8. When config transfer is complete, reload to exit Bootstrap Monitor and to pick up the new configuration, as follows:
 - a. Answer y when asked "Okay?".
 - b. Type ? to look at the Bootstrap Monitor menu.
 - c. Type b to boot using new config
 9. Re-establish the remote 2210 session after the reload, if necessary.
 10. Log into the router, as follows:
 - Login = yourid
 - Password = yourpassword

Chapter 2. MRS Overview

This chapter provides an overview of the Nways Multiprotocol Routing Services (MRS) software for the IBM 2210. It includes descriptions of the boot process, the user interface and the event logging system (ELS). Further information can be found in the *Nways MRS Software User's Guide*.

2.1 Introduction

The Nways MRS is the software that supports the IBM 2210. The Nways MRS has two components:

- The code that provides the routing, bridging, data link switching, and SNMP agent functions for the IBM 2210
- The configuration program, which offers a graphical user interface that allows you to configure the IBM 2210 from a workstation

2.2 Boot Files and Boot Processes

The IBM 2210 does not have a hard drive like the IBM 6611 Network Processor, so it needs another method to load its operating system (referred to here as the boot file).

The boot file can be loaded (booted) from the following sources:

- Flash memory (referred to here as the integrated boot device or simply IBD).
- An external server that supports the TFTP server function. This could be another router which supports the TFTP server function (such as another IBM 2210).
- The console port using Zmodem.

Note: The IBM 2210 is delivered pre-loaded with a boot file in the IBD.

The IBM 2210 has a boot configuration database that holds information on all the available boot files. Each entry in the database contains the host server's location where the boot file resides and the path, file name, and a timeout value for the boot file. You can add entries to the database by issuing the following command:

Boot Config>**add boot-entries**

The BOOT CONFIG prompt is accessed via the CONFIG process discussed in 2.4.6, "CONFIG Process" on page 30.

On startup, the IBM 2210 will normally load itself with the boot file stored in the IBD, but it can use the boot configuration database to obtain a copy from a TFTP server, should this boot file become corrupted or unusable.

The IBM 2210 may also use the Boot Protocol (Bootp) to obtain its boot file, and uses the Bootp client function to do so. The IBM 2210 will use Bootp to learn its own IP address and the location (TFTP server) from which the boot file can be obtained. It will then use TFTP to load the boot file from the TFTP server.

In order to cause the IBM 2210 to act as a Bootp client, the interfaces, over which the Bootp packet should be broadcasted, are indicated by issuing the following command:

Boot Config>**add bp-device**

Note

When the IBM 2210 obtains its boot file at boot time from an external source, it loads the boot file into executable memory, but does not save a copy in the IBD. If you want to save a copy into the IBD, issue one of the following commands:

Boot Config>**Store**

or

Boot Config>**TFTP get**

Both commands use the TFTP protocol. The only difference is the format in which you specify the location of the file to be transferred.

The IBM 2210 does not allow you to initiate a transfer from another device to the IBM 2210, so you will need to start the transfer from the router's operator console.

For further information, see 2.4.10, "BOOT CONFIG Process" on page 37.

The Zmodem boot allows you to load router code through the console port, using an ASCII terminal emulator package that supports the Zmodem protocol. To load the code via this method enter:

>zb

The > prompt (the Boot prompt) is accessed by pressing Ctrl+C while the IBM 2210 is reloading.

Your Zmodem software documentation explains the commands required to start the upload.

2.3 2210 Configuration

The configuration process customizes the IBM 2210 for both the network in which you intend to run it and the equipment being used. The configuration file may be created via the Nways MRS Configuration Program and then transferred to the IBM 2210, or via commands entered at the operator console.

The configuration data resides in IBM 2210's non-volatile RAM (NVRAM) and is combined with the boot file when the IBM 2210 is restarted or reloaded, creating the operating environment of the IBM 2210. NVRAM is the only place from which the IBM 2210 will obtain the configuration information during a restart or reload process.

Reloading the IBM 2210 causes the router to reload the boot file into RAM. At the same time, it customizes the operating environment using the configuration file stored on NVRAM.

To reload the IBM 2210, issue the Reload command from the OPCON prompt (*).

Restarting the IBM 2210 does not cause the router to reload the boot file. It simply takes the configuration file on NVRAM and feeds it into the operating environment.

To restart the IBM 2210, issue the Restart command from the OPCON prompt (*).

Changes made from the operator console configuration process (CONFIG) are immediately saved in NVRAM and, in most cases, will take effect once the IBM 2210 is restarted or reloaded. However, there are a few changes that will take effect immediately, without the need to restart or reload. The CONFIG process is discussed further in 2.4.6, "CONFIG Process" on page 30.

Changes made from the operator console monitoring process (GWCON) take effect immediately. However, once the router is restarted or reloaded, these changes are lost. This facility could be useful if you wish to test some changes prior to making them permanent.

Note: The parameters that can be changed from the GWCON process are a subset of the parameters that can be changed from the CONFIG process.

The GWCON process is discussed further in 2.4.7, "GWCON Process" on page 35.

The Nways MRS Configuration Program may also be used to configure the IBM 2210. The Nways MRS Configuration Program runs under AIX, OS/2 and Windows and uses a GUI interface. When configuring via the Nways MRS Configuration Program, create a configuration file on the workstation, which can be saved in two formats:

- An archive format that is stored in the workstation configuration database and is readable by the Nways MRS Configuration Program
- A 2210-readable format for transferring to the IBM 2210 via TFTP

Note: The 2210-readable format cannot be reloaded into the Nways MRS Configuration Program, so it is highly recommended that you save an archive copy before creating and sending a 2210-readable file to the router. The 2210-readable file must be manually transferred to the IBM 2210 using *one* of the following commands:

- Boot Config>**Copy Config**
- Boot Config>**TFTP get**
- **>zc**

If you choose to create your configuration on the IBM 2210 console, you should save a copy of it on an external server in case the NVRAM fails or the file becomes corrupted. To do this, use either of the following commands:

Boot Config>**Copy Config**

Boot Config>**TFTP put**

The >zc command allows you to load a configuration file via the console port, using an ASCII terminal emulator that supports the Zmodem protocol.

To access the > prompt, press Ctrl+C while the router is reloading.

Your Zmodem software documentation explains the commands required to start the upload.

2.4 MRS User Interface

Access the Nways MRS user interface through an ASCII console or emulator, as mentioned in 1.6, “Accessing the IBM 2210” on page 14.

By default, when you connect to the IBM 2210 you will not be required to enter a user ID or password, and you will have access to all router functions and commands.

However, for security reasons, you may want users to enter a user ID and password when they connect to the router. Enabling this function is described in 2.4.1, “Configuring User Access.”

2.4.1 Configuring User Access

To add user access to the router, enter the `Config>add user` command.

When you add a user, you are prompted for their password and their permission level, which can be one of the following:

- Administration

This level gives access to all router commands and functions, including configuration and user administration.

- Operations

This level allows you to view the configuration parameters and network statistics, use the GWCON commands to make dynamic configuration changes, and to restart the router.

- Monitor

This level allows you only to view the configuration parameters and network statistics.

Note: User IDs can contain a maximum of eight characters, passwords can contain a maximum of eighty characters, and both user IDs and passwords are case-sensitive.

When you add the very first user, the IBM 2210 automatically enables console login, which is the function that causes you to be prompted for an user ID and password. Console login can also be enabled and disabled using the following commands respectively:

`Config>enable console-login`

`Config>disable console-login`

Also, when you add the very first user, you are asked whether you wish to add technical support access. If you reply yes, a user ID called 2210I3 is created with a password known by IBM service personnel. This user ID has administrator privileges and is available for use by IBM service personnel. However, you can change the password and permission level of this user if you wish, using the following command:

`Config>change user`

An example of adding users for the first time is shown in Figure 14 on page 23.

```

Config>add user
Enter user name: []? admin
Password: 1
Enter password again: 2
Enter permission: (A)dmin, (O)perations, or (M)onitor [A]? a
User 'admin' has been added
Enabling console login 3
Do you want to add Technical Support access?(Yes or [No]): y
Config>list user
  USER      PERMISSION
  admin      Admin
  221013     Tech Support
Console login is enabled

Config>add user hdesk 4
Password:
Enter password again:
Enter permission: (A)dmin, (O)perations, or (M)onitor [A]? o
User 'hdesk' has been added
Config>list user
  USER      PERMISSION
  admin      Admin
  221013     Tech Support
  hdesk      Operations
Console login is enabled

Config>add user Hdesk 4
Password:
Enter password again:
Enter permission: (A)dmin, (O)perations, or (M)onitor [A]? o
User 'Hdesk' has been added
Config>list user
  USER      PERMISSION
  admin      Admin
  221013     Tech Support
  hdesk      Operations
  Hdesk      Operations
Console login is enabled

```

Figure 14. Adding Users to the IBM 2210

Notes:

- 1** The password field is hidden when entered.
- 2** You are required to verify the password.
- 3** Console login is automatically enabled.
- 4** An example to show that user IDs are case-sensitive.

2.4.2 Nways MRS Process Structure

The user interface to the Nways MRS consists of a main process, called OPCON, and several secondary processes that allow you to control and monitor the operation of the IBM 2210.

The more commonly used processes and their structure are shown in Figure 15.

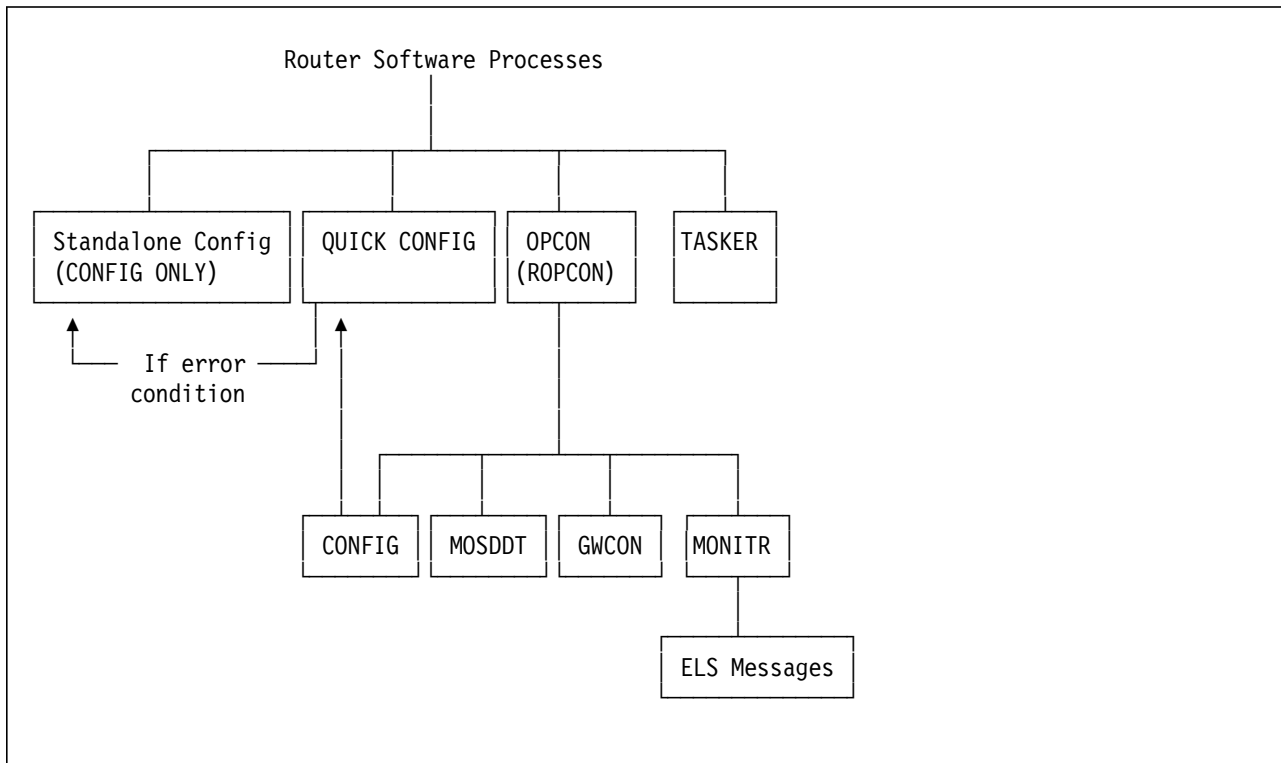


Figure 15. Nways MRS Processes

Table 15 gives a brief description of each process.

Table 15 (Page 1 of 2). Process Description		
Process	Description	Prompt
OPCON	Functions as the main operator control program. It provides service for one directly connected console.	Asterisk (*)
ROPCON	Provides OPCON service for two remotely attached (Telnet) consoles.	Asterisk (*)
EZSTART	Provides the router's user interface during automatic configuration download. Commands that run in OPCON will also run in EasyStart but may or may not be useful. Functionally, OPCON and EasyStart are the same.	EasyStart>
GWCON	Provides monitoring of the software components.	Plus sign (+)
CONFIG	Provides online configuration ability.	Config>
MONITR	Performs message printing services.	None
TASKER	Runs the router's main networking software and performs the internetwork data transfer operations.	None
MOSDDT	Used as the MOS runtime debugging tool.	Dollar sign (\$)
QUICK CONFIG	Provides a simple way to configure devices and some protocols.	None

<i>Table 15 (Page 2 of 2). Process Description</i>		
Process	Description	Prompt
CONFIG-ONLY	Provides the same function as the CONFIG process with the addition of the Restart and the Reload commands.	Config (only)>

2.4.3 QUICK CONFIG Process

When you initially load, start or restart the router with no configuration, you automatically enter the Quick Configuration (QUICK CONFIG) process. This provides a quick and simple way to configure interfaces, bridging and routing protocols, and boot records. Be aware, however, that this option chooses many defaults, some of which may not be appropriate to your installation. It is, therefore, advisable to:

1. Configure the interfaces and boot records using QUICK CONFIG
2. Restart the router
3. Complete a full configuration

Quick configuration is also available by issuing the `Config>qconfig` command.

Output from a sample configuration using QCONFIG is shown in Figure 16 on page 26.

This configuration would allow you to restart the router and configure it fully from a TCP/IP station using Telnet, and attached via a LAN (provided the workstation is in the same IP subnet).

```

Config>qconfig

Router Quick Configuration for the following:
o  Interfaces
o  Bridging
    Spanning Tree Bridge (STB)
    Source Routing Bridge (SRB)
    Source Routing/Transparent Bridge (SR/TB)
    Source Routing Transparent Bridge (SRT)
o  Protocols
    IP (including OSPF, RIP and SNMP)
    IPX
o  Booting

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

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

Type 'Yes' to Configure Interfaces
Type 'No' to skip Interface Configuration
Type 'Quit' to exit QUICK CONFIG

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


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

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

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

This is all configured device information:

Intf 0 is Token Ring, Speed 4 Mb/sec, Connector UTP
Intf 1 is WAN 1 with PPP Encapsulation, RS-232 modem cable
Intf 2 is WAN 2 with PPP Encapsulation, RS-232 modem cable

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

Device configuration saved

```

Figure 16 (Part 1 of 3). An Example of Using QUICK CONFIG


```

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

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit QUICK CONFIG

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

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

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit QUICK CONFIG

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

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

Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes] yes
IP Address: [] 9.67.46.148
Address Mask: [255.0.0.0] 255.255.255.240

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

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

Per-Interface IP Configuration complete

Configuring IP Routing Information
Enable Dynamic Routing? (Yes, No): [Yes] no

Only Static Routing Enabled

Routing Configuration Complete

SNMP will be configured with the following parameters:
    Community: public
    Access:     READ-ONLY

```

Figure 16 (Part 2 of 3). An Example of Using QUICK CONFIG

```

This is the information you have entered:

      Interface #      IP Address      Address Mask
          0          9.67.46.148      255.255.255.240

Only STATIC Routing present

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

IP configuration saved

Configure IPX? (Yes, No): [Yes] no

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

Type 'Yes' to Configure Booting
Type 'No' to skip Booting Configuration
Type 'Quit' to exit QUICK CONFIG

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

Previous Boot information

Booting Method:      IBD Boot
IBD Load Name:      led.ldc

Create an IBD boot record using this information? (Yes, No): [Yes] yes

Boot configuration saved
Enable Console Modem-Control? (Yes, No, Quit): [No] no

QUICK CONFIG Done
Restart the router for this configuration to take effect

Restart the router? (Yes, No): [Yes] yes

```

Figure 16 (Part 3 of 3). An Example of Using QUICK CONFIG

2.4.4 CONFIG ONLY Process

The CONFIG ONLY process is used for making configuration changes without the normal operational router software running. In this state the router is not active in the network.

There are two ways to enter CONFIG ONLY mode:

- Operational failure: The router encounters a problem during operation and automatically comes up in CONFIG ONLY mode. This can occur if, for example, static RAM is corrupted.
- You deliberately enter CONFIG ONLY mode by issuing the `bc` command from the `>` prompt. This prompt is the boot prompt and is accessed by pressing Ctrl+C while the router is reloading.

2.4.5 OPCON Process

The OPCON process handles the communication between the user and the other processes. To communicate with those other processes issue the `talkpid` command from the OPCON prompt (*), where `pid` is the process ID of the process you wish to talk to. The process ID can be obtained by issuing the `status` command from the OPCON prompt. You would normally expect to see the following output:

```
*status
Pid  Name      Status TTY  Comments
1    COpCon    RDY   TTY0
2    Monitr    DET   --
3    Tasker    RDY   --
4    MOSDDT    DET   --
5    CGWCon    IOW   --
6    Config    DET   --
7    EZstrt    IDL   --
8    COpCon    IOW   TTY1
9    ROpCon    IDL   TTY2
10   ROpCon    IDL   TTY3
```

To return to the OPCON process from any other use the intercept character which is set to `Ctrl+P` by default. To change the intercept character, issue the `Intercept` command from the OPCON prompt.

The OPCON process also allows you to restart or reload the router, and among other things, display memory usage information. The commands available under OPCON are listed in Table 16.

Note

You can abbreviate most of the commands entered at any of the process prompts to the least number of letters that still make the command unique.

For example, the `Talk` command can be shortened to `t`.

Table 16 (Page 1 of 2). OPCON Commands

Command	Function
? (Help)	Lists all the OPCON commands.
Breakpoint	Enters the MOSDDT debugging tool.
Divert	Sends the output from a process to a console or other terminal.
Flush	Discards the output from a process.
Halt	Suspends the output from a process.
Intercept	Sets the OPCON default intercept character.
Logout	Logs out a remote console.
Memory	Reports the router's memory usage.
Restart	Restarts (but does not reload) the router software.
Reload	Reloads the router software.
Status	Shows information about all router processes.

Table 16 (Page 2 of 2). OPCON Commands	
Command	Function
Talk	Connects to another router process and enables the use of its commands.
TELNET	Connects to another router.

2.4.6 CONFIG Process

The CONFIG process is accessed by issuing the `*talk 6` command.

It is from this process that most of your configuration will be done unless you choose to use the Nways MRS Configuration Program. CONFIG is fully described in the *Nways MRS Software User's Guide*. Using CONFIG commands, you can:

- Enter the QUICK CONFIG mode
- Enter the BOOT CONFIG mode
- Clear, list or update configuration information, both for interfaces and protocols
- Enable or disable console login

The commands available under CONFIG are shown in Table 17.

Table 17 (Page 1 of 2). CONFIG Commands	
Command	Function
? (Help)	Lists the CONFIG commands or lists the options associated with specific commands.
Add	Adds an interface to the router configuration, or a user to the router.
Boot	Enters BOOT CONFIG command mode.
Change	Changes the current interface's device type configuration, or a user's password.
Clear	Clears configuration information.
Delete	Deletes an interface from the router's configuration or a configured user.
Disable	Disables login from a remote console, remote access using a modem, or a specified interface.
Enable	Enables login from a remote console or remote access using a modem, or enables a specified interface.
Event	Enters the ELS configuration command mode.
Feature	Provides access to configuration commands for WRS (WAN Restoral), BRS (Bandwidth Reservation), and MCF (MAC Filtering).
List	Displays the system parameters or the hardware configuration.
Network	Enters the configuration environment of the specified network (interface).
Patch	Modifies the patch variables, changing the router configuration.
Protocol	Enters the command environment of the specified protocol.
Qconfig	Enters the QUICK CONFIG process.
Set	Sets various systemwide parameters, plus the data-link type for the serial interfaces.
Time	Sets and displays the system time.
Unpatch	Restores patch variables to their default values.

Table 17 (Page 2 of 2). CONFIG Commands	
Command	Function
Update	Updates the current version of the configuration.

The example configuration scenarios in this book show the commands used from the CONFIG process, along with the relevant Nways MRS Configuration Program panels.

The structure of the configuration process for Nways MRS is shown in Figure 17.

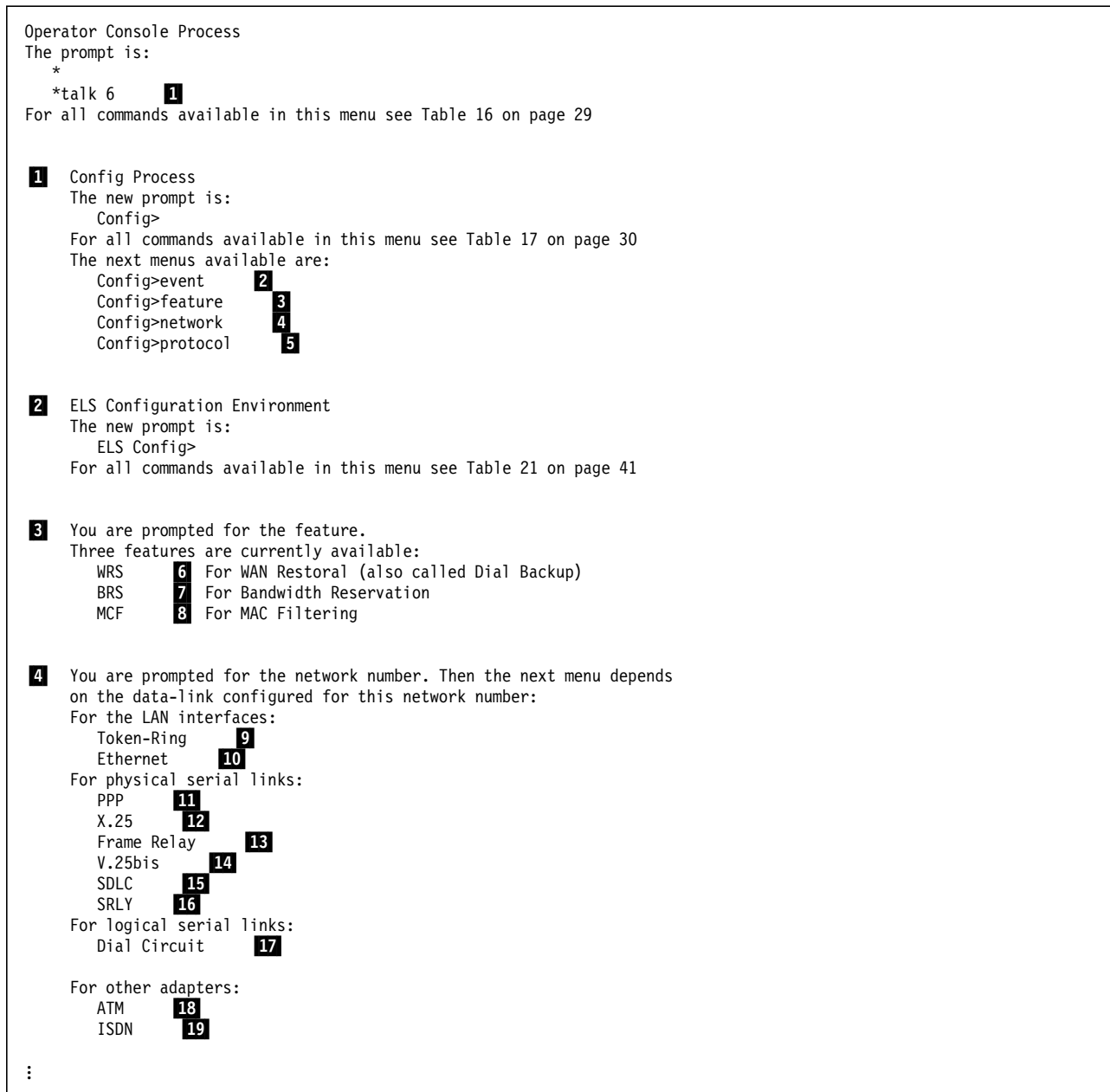


Figure 17 (Part 1 of 5). Structure of the CONFIG Process for Nways MRS Program

:

- 5** You are prompted for the protocol.
Here are the protocols currently available:
- | | | |
|-------|-----------|--|
| IP | 20 | For TCP/IP protocol |
| ARP | 21 | For ARP protocol for TCP/IP only |
| IPX | 22 | For IPX Novel protocol |
| DVMRP | 23 | For Distance Vector Multicast Routing Protocol for TCP/IP networks |
| SNMP | 24 | For Simple Network Management Protocol for TCP/IP networks |
| OSPF | 25 | For OSPF routing protocol on TCP/IP networks |
| DN | 26 | For DNA Phase IV |
| SDLC | 27 | For SDLC Relay protocol over TCP/IP networks |
| AP2 | 28 | For Appletalk 2 protocol |
| ASRT | 29 | For Bridging and NetBIOS facilities |
| HST | 30 | For TCP/IP Host services on bridges only |
| DLSw | 31 | For Data Link Switching protocol for TCP/IP networks |
| VIN | 35 | For Banyan VINES |
| OSI | 36 | For ISO CLNP/ISIS/ISIS |
| BGP | 37 | For Border Gateway Protocol |
| APPN | 38 | For Advanced Peer-to-Peer Networking |
| LNM | 39 | For Lan Net work manager |

- 6** WAN Restoral user configuration
The new prompt is:
WRS Config>
For all commands available in this menu see Table 74 on page 607

- 7** Bandwidth Reservation user configuration
The new prompt is:
Reservation Config>
For all commands available in this menu see Table 70 on page 534

- 8** MAC Filtering user configuration
The new prompt is:
Filter Config>
For all commands available in this menu see Table 72 on page 571

- 9** Token-Ring interface configuration
The new prompt is:
TKR config>
For all commands available in this menu see Table 23 on page 65

- 10** Ethernet interface configuration
The new prompt is:
ETH config>
For all commands available in this menu see Table 22 on page 61

- 11** Point-to-Point user configuration
The new prompt is:
PPP Config>
For all commands available in this menu see Table 34 on page 88

:

Figure 17 (Part 2 of 5). Structure of the CONFIG Process for Nways MRS Program

```

:
12 X.25 user configuration
   The new prompt is:
     X.25 Config>
   For all commands available in this menu see Table 25 on page 80

13 Frame Relay user configuration
   The new prompt is:
     FR Config>
   For all commands available in this menu see Table 32 on page 86

14 V.25bis Data Link Configuration
   The new prompt is:
     V.25bis Config>
   For all commands available in this menu see Table 41 on page 100

15 SDLC user configuration
   The new prompt is:
     SDLC # Config> (Where # is the network number.)
   For all commands available in this menu see Table 36 on page 92

16 SDLC relay interface user configuration
   The new prompt is:
     SRLY Config>
   For all commands available in this menu see Table 38 on page 95

17 Circuit configuration
   The new prompt is:
     Circuit Config>
   For all commands available in this menu see Table 42 on page 101

18 ATM configuration
   The new prompt is:
     ATM Config>
   For all commands available in this menu see Chapter 41 of
   Multiprotocol Routing Services Software User's guide
   Version 1 Release 1 documentation.

19 ISDN configuration
   The new prompt is:
     ISDN Config>
   For all commands available in this menu see Table 45 on page 105.

20 Internet protocol user configuration
   The new prompt is:
     IP config>
   For all commands available in this menu see Table 55 on page 341

:

```

Figure 17 (Part 3 of 5). Structure of the CONFIG Process for Nways MRS Program

:

- 21** ARP user configuration
The new prompt is:
ARP config>
For all commands available in this menu see Chapter 18 of *Nways MRS Protocol Configuration and Monitoring Reference Volume 1 Version 1 Release 1* documentation.
- 22** IPX protocol user configuration
The new prompt is:
IPX config>
For all commands available in this menu see Table 67 on page 413
- 23** Distance Vector Multicast Routing Protocol config console
The new prompt is:
DVMRP Config>
For all commands available in this menu see Table 65 on page 361
- 24** SNMP user configuration
The new prompt is:
SNMP Config>
For all commands available in this menu see Table 63 on page 359
- 25** Open SPF-Based Protocol configuration console
The new prompt is:
OSPF Config>
For all commands available in this menu see Table 59 on page 353
- 26** DN protocol user configuration
The new prompt is:
NCP config>
For all commands available in this menu see Chapter 10 of *Nways MRS Protocol Configuration and Monitoring Reference Reference Volume 2 Version 1 Release 1* documentation
- 27** SDLC relay protocol user configuration
The new prompt is:
SDLC config>
For all commands available in this menu see Table 39 on page 95
- 28** AP2 protocol user configuration
The new prompt is:
AP2 config>
For all commands available in this menu see Chapter 26 of *Nways MRS Protocol Configuration and Monitoring Reference* documentation

Figure 17 (Part 4 of 5). Structure of the CONFIG Process for Nways MRS Program

- 29** Adaptive Source Routing Transparent Bridge user configuration
 The new prompt is:
 ASRT config>
 For all commands available in this menu see Table 51 on page 123
 The next menus available are:
 ASRT config>name-caching **32**
 ASRT config>netbios-filtering **33**
 ASRT config>tunnel **34**
- 30** TCP/IP Services user configuration
 The new prompt is:
 TCP/IP-Host config>
 For all commands available in this menu see Table 53 on page 136
- 31** DLSw protocol user configuration
 The new prompt is:
 DLSw config>
 For all commands available in this menu see Table 68 on page 454
- 32** NetBIOS Name Caching facility configuration
 The new prompt is:
 Name Cache Config>
 For all commands available in this menu see Table 76 on page 719
- 33** NetBIOS Filtering facility configuration
 The new prompt is:
 NETBIOS Filter config>
 For all commands available in this menu see Table 77 on page 727
- 34** Tunnel interface configuration
 The new prompt is:
 TNL config>
 For all commands available in this menu see Table 52 on page 133
- 35** Vines Protocol configuration
 The new prompt is:
 Vines config>
 For all commands available in this menu see Chapter 8 of *Nways MRS Protocol Configuration and Monitoring Reference Reference Volume 2 Version 1 Release 1* documentation
- 36** OSI/DECnet for phase V
 The new prompt is:
 OSI config>
 For all commands available in this menu see Chapter 11 of *Nways MRS Protocol Configuration and Monitoring Reference Reference Volume 2 Version 1 Release 1* documentation
- 37** BGP Protocol configuration
 The new prompt is:
 BGP>
 For all commands available in this menu see Table 61 on page 357
- 38** APPN Protocol configuration
 The new prompt is:
 APPN>
 For all commands available in this menu see *2210/2216 APPN/ATM Red Book* documentation

Figure 17 (Part 5 of 5). Structure of the CONFIG Process for Nways MRS Program

2.4.7 GWCON Process

The GWCON process is accessed by issuing the *talk 5 command.

You can use this process to monitor the current router configuration, monitor router utilization, and make temporary configuration changes.

Using GWCON commands you can:

- List the interfaces and protocols currently configured
- Display memory and network statistics
- Set some current configuration parameters
- Set current ELS parameters
- Test, enable or disable a network interface

This process is also discussed fully in the *Nways MRS Software User's Guide*.

The commands available under GWCON are shown in Table 18.

Table 18. GWCON Commands	
Command	Function
? (Help)	Lists the GWCON commands.
Boot	Displays boot information for the router.
Buffer	Displays information about packet buffers assigned to each interface.
Clear	Clears statistics.
Configuration	Lists the currently configured protocols and interfaces.
Disable	Disables the specified interface.
Environment	
Error	Displays error counts.
Event	Enters the ELS event logging.
Fault	Displays information about a router crash.
Feature	Enters the WRS, BRS, or MCF environment.
Interface	Displays network hardware statistics, or statistics for the specified interface.
Log	Sets or displays the logging level for events not included in ELS.
Memory	Displays memory, packet, and buffer data.
Network	Enters the console environment of the specified network (interface).
Protocol	Enters the console environment of the specified protocol.
Queue	Displays buffer statistics for a specified interface.
Statistics	Displays statistics for a specified interface.
Test	Enables a disabled interface or tests the specified interface.
Uptime	Displays time statistics for the router.

2.4.8 MONITR Process

The MONITR process receives messages from the event logging system (ELS) and displays them on the console. It is accessed by issuing the `*talk 2` command.

There is no prompt associated with MONITR and you cannot enter any commands. To exit MONITR use the OPCON intercept character (Ctrl+P by default).

2.4.9 MOSDDT Process

This is a special process used by software specialists to examine and change the contents of the router's memory and registers. It is used only for debugging purposes and is not discussed here.

2.4.10 BOOT CONFIG Process

The BOOT CONFIG process is accessed by entering boot from the Config> prompt.

The BOOT CONFIG process is accessed by issuing the *talk 6 command.

It allows you to:

- Add, modify or delete entries from the boot configuration database
- Enable or disable dumping of the IBM 2210
- View the current boot and dump configuration database
- Transfer configuration information between router memory and remote hosts, using TFTP
- Retrieve the boot file from a local or remote source
- Store boot file images in the IBD
- List the contents of the IBD
- Delete files from the IBD

From the Boot Config> prompt, you have the following commands available:

Table 19. BOOT CONFIG Commands	
Command	Function
? (Help)	Displays a list of the commands available from this prompt level.
Add	Adds a boot interface IP address to a specified interface, host boot entry, or host dump entry.
Change	Changes the boot interface IP address, network boot entry data, or network dump entry data.
Copy config	Copy boot files and configuration files from remote routers and hosts.
Describe	Displays information about the stored images in the IBD.
Delete	Deletes a network boot interface, a host boot entry, host dump entry, or boot interface IP address.
Disable	Disables memory dump or unique naming of the dump files.
Enable	Enables memory dump and allows unique naming of the dump files.
Erase	Erases a stored image or an IBD bank.
List	Displays all network boot addresses, all boot and dump configuration data, the contents of the IBD, and name settings.
Load	Copies the boot file from the IBD to RAM or copies the boot file from a remote host.
Store	Copies the boot file from RAM to the IBD.
TFTP	Initiates TFTP file transfers between router memory and remote hosts.
Exit	Leaves the BOOT CONFIG environment and returns to the CONFIG process.

2.5 The Event Logging System (ELS)

ELS is a monitoring system that manages messages logged as a result of router activity. Using ELS commands, you can configure the system such that you only see the messages that you need. ELS uses the concepts of *subsystem*, *event number*, *message text*, *logging level*, and *group* to help you manage the messages you see.

Subsystem is a predefined name for a router component, such as an interface or protocol. For example, IP is the subsystem name for the IP protocol, and TKR is the subsystem name for the token-ring interface.

The ELS Config process is accessed by issuing the `Config>event` command.

You can obtain a complete list of the subsystem names by issuing the ELS `Config>list subsystem` command as shown in Figure 18 on page 39.

The output shows the subsystem name, the number of events for the subsystem, and a description of the subsystem.

```
ELS config>list subsystem
```

Name	Events	Description
ALL		All subsystems
APPN	78	Advanced Peer-to-Peer Networking
GW	77	Router base and network library
FLT	7	Filter Library
BRS	4	Bandwidth Reservation
ARP	17	Address Resolution Protocol
IP	86	Internet Protocol
ICMP	20	Internet Control Message Protocol
TCP	55	TCP
UDP	4	User Datagram Protocol
BTP	5	Bootp relay agent
RIP	19	IP Routing Information Protocol
OSPF	60	Open SPF-Based Routing Protocol
MSPF	15	OSPF Multicast extensions
TFTP	24	TFTP Protocol
SNMP	20	Simple Network Management Protocol
DVM	21	DVMRP Multicast Routing Protocol
IPX	89	Internetwork Packet Exchange Protocol
CLNP	58	ISO 8473 - CLNP
ESIS	24	ISO 9542 - ESIS Protocol
ISIS	58	ISO 10589 - ISIS Protocol
DNAV	26	DNA Phase V
AP2	68	AppleTalk Phase 2
ZIP2	51	Appletalk Phase 2 Zone Information Protocol
R2MP	38	Appletalk Phase 2 Routing Table Management Protocol
VIN	79	Banyan VINES
SRT	83	Source Routing Transparent Bridge
STP	31	Spanning Tree Protocol
BR	29	Bridge/Routing
SRLY	28	SDLC Relay
ETH	47	Ethernet Handler
SL	33	Serial Line Handler
TKR	45	Token Ring Handler
X25	50	X.25 Protocols
ILMI	6	Interim Local Management Interface
SDLC	91	IBM SDLC
FRL	45	Frame Relay
PPP	93	Point-to-Point
X251	16	X.25-Physical-Layer
X252	34	X.25-Frame-Layer
X253	39	X.25-Packet-Layer
XTP	58	X.25 Transport
IPPN	4	IP Protocol Net
WRS	22	WAN Restoral

Figure 18 (Part 1 of 2). Output from the List Subsystem Command

LNK	60	LNK
LLC	33	Logical Link Control
MCF	9	MAC Filtering
DLS	327	Data Link Switching
V25B	28	CCITT/ITU V.25bis
EZ	9	EasyStart
AI	1	Auto-device Install
BAN	29	Boundary Access Mode
COMP	18	Data Compression Engines
NBS	50	NetBIOS Support Subsystem
NOT	15	Forwarder messages not loaded
ATM	13	Asynchronous Transfer Mode
LEC	7	ATM LAN Emulation Client
SVC	5	ATM Signalling

Figure 18 (Part 2 of 2). Output from the List Subsystem Command

Event number is a predefined number assigned to each message within a subsystem. You can obtain a complete list of events for a particular subsystem by issuing the ELS Config>**list subsystem** *subsys* command, where *subsys* is the name of the particular subsystem you are interested in. For example:

ELS Config>**list subsystem udp**

This command will list all possible events in the UDP subsystem, as shown in Figure 19. The output shows the event number, the logging level and the message text.

```
ELS config>list subsystem udp

Event      Level      Message
UDP.001    P-TRACE    pkt %I -> %I port %d no srvr
UDP.002    U-INFO     pkt %I -> %I port %d no srvr
UDP.003    UE-ERROR    dsc pkt frm %I bd len %d
UDP.004    UE-ERROR    bd cksum clc %o rcv %o
```

Figure 19. Output from the List Subsystem UDP Command

Message text is the actual text related to the event that has occurred and is used along with the subsystem and event number when the message is displayed by the MONITR process.

Logging level is a predefined category that each event will belong to, and which indicates the importance of the event. Note, whenever you issue the ELS Config>**list subsystem** *subsys* command to list all the events within a subsystem, the logging level for each event is displayed.

The complete list of logging levels is shown in Table 20.

Table 20 (Page 1 of 2). Logging Levels	
Level	Description
UI ERROR	Unusual internal errors
CI ERROR	Common internal errors

<i>Table 20 (Page 2 of 2). Logging Levels</i>	
Level	Description
UE ERROR	Unusual external errors
CE ERROR	Common external errors
ERROR	Includes all error levels above
UINFO	Unusual informational comment
CINFO	Common informational comment
INFO	Includes all informational comment levels above
STANDARD	Includes all error levels and all informational comment levels above
PTRACE	Per packet trace
UTRACE	Unusual operation trace message
CTRACE	Common operation trace message
TRACE	Includes all trace levels above
ALL	Includes all logging levels

Group is a user-defined collection of events that is given a name. A group can consist of events from different subsystems and of different logging levels. Once you have created a group, you can use the group name to manipulate the events in the group as a whole.

The *Nways MRS Event Logging System Messages Guide* also contains a complete list of all events for all subsystems and includes the logging level for each event.

A summary of the commands available under the ELS Config> prompt are listed in Table 21.

<i>Table 21. ELS Configuration Commands</i>	
Command	Function
? (Help)	Lists the ELS configuration commands or lists the options associated with specific commands.
Add	Adds an event to an existing group or creates a new group.
Clear	Clears all ELS Configuration information.
Default	Resets the display or trap setting of an event, group, or subsystem.
Delete	Deletes an event number from an existing group or deletes an entire group.
Display	Enables message display on the console monitor (MONITR).
Exit	Exits the ELS configuration process.
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Notrap	Prevents messages from being trapped and sent out over SNMP.
Set	Sets the pin parameter to the maximum number of traps per second.
Trap	Allows messages to be trapped and sent out over SNMP.

2.5.1 Controlling Message Display

To control the display of messages in MONITR, use the display and nodisplay commands. These can be issued from within one of the following:

- The CONFIG process, where the changes will become part of the configuration when the IBM 2210 is restarted
- The GWCON process, where the effect will be immediate, but will only last until the router is restarted (unless an ELS>**save** command is issued).

For example, to display the standard level messages associated with the TKR subsystem, you would issue:

```
ELS>display subsystem TKR standard
```

To prevent all TKR messages being displayed, issue the following:

```
ELS>nodisplay subsystem TKR all
```

You would now need to switch to the MONITR process to see the effects of your command, after restarting if necessary.

2.6 The IBM 2210 Configuration Program

The IBM Nways Multiprotocol Routing Network Services Configuration Program allows you to perform a complete configuration of an IBM 2210 Nways Multiprotocol Router. The Configuration Program is run on a workstation and has a graphical user interface.

Before using the Configuration Program you must perform an initial configuration on the 2210 to allow you to transfer these settings across to the IBM 2210 Router. The minimum requirement is that IP Routing is enabled to use the Trivial File Transfer Protocol (TFTP) or IP and SNMP are enabled to use the Communication option within the configuration program.

2.6.1 Hardware and Software Requirements

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

- IBM AIX 3.2.5 or higher with Transmission Control Protocol/Internet Protocol (TCP/IP) enabled
- IBM AIXwindows
- 16 MB of memory (32 MB recommended)
- A 3.5-inch diskette drive that can read and write 1.44 MB formatted diskettes
- 14 MB of available space on the fixed disk drive
- A graphics display that supports 640x480 resolution and 16 colors or gray scales (1024x768 resolution and 256 colors recommended)
- A mouse

The following hardware and software are required to use the Configuration Program on a PC workstation using an Intel 80386 or higher processor or a compatible system that has an Intel 80386 or higher processor (486 DX2-50 is the minimum recommended processor).

For workstations running the Microsoft Windows program, you need the following:

- IBM DOS 5.0 or higher, MS-DOS 5.0 or higher
- Microsoft Windows 3.1 or later versions
 - Win32s, included with the MRS Configuration Program diskettes (not needed by Windows 95)
 - WinSock 2.0 DLL (included with Win32s)
- TCP/IP application that uses WinSock 2.0 (This is only required for using the Configuration function.)
- 16 MB of memory (32 MB recommended)
- 3.5-inch diskette drive that can read and write 1.44 MB formatted diskettes
- 14 MB of available space on the fixed disk drive
- A graphics display that supports 640x480 resolution and 16 colors or gray scales (1024x768 resolution and 256 colors recommended)
- A mouse
- If you encounter problems with windows not updating properly, ensure that you have installed the latest BIOS and video drivers provided by the manufacturer.

For workstations running the IBM Operating System/2 (OS/2) Program, you need the following:

- OS/2 2.1 or Warp 3.0
- IBM TCP/IP 1.2.1 or OS/2 or later (This is only required for using the Configuration function.)
- 16 MB of memory (32 MB recommended)
- 3.5-inch diskette drive that can read and write 1.44 MB formatted diskettes
- 14 MB of available space on the fixed disk drive
- 10 MB of available swapper disk space on the swapper fixed disk drive partition
- A graphics display that supports 640x480 resolution and 16 colors or gray scales (1024x768 resolution and 256 colors recommended)
- A mouse
- If you encounter problems with windows not updating properly, ensure that you have installed the latest BIOS and video drivers provided by the manufacturer.

2.6.2 Anonymous FTP Site for the IBM 2210 Multiprotocol Router

IBM has established an anonymous FTP site for providing information and configuration program updates (and other program updates in the future) relating to the 2210.

The hostname for the anonymous FTP site is `ftp.mways.raleigh.ibm.com`. If you have trouble resolving this name, the IP address is 204.146.167.70. After connecting to the machine, specify anonymous as the user ID and your e-mail address as your password. Check the README file on the anonymous FTP site in the `/pub` directory for the latest information.

The subdirectories where the Configuration Programs reside are as follows:

- /pub/config/2210/MRS/1.1.0.0/GA/diskettes for the diskette images
- /pub/config/2210/MRS/1.1.0.0/GA/runtime for the RISC System/6000 files

There is also a 2210 Configuration Program Web page for users with Web browsers at the following URL:

<http://www.raleigh.ibm.com/220/220fix.html>

2.6.3 Installing the Configuration Program

The IBM 2210 Multiprotocol Routing Services Configuration Program Version 1.0 Release 1.0 (hereafter referred to as the Configuration Program) is shipped on eight diskettes.

- Diskettes 1-6 contain the Configuration Program
- Diskettes 7-8 contain the WIN32s specific program

This chapter provides instructions for installing the Configuration Program.

2.6.3.1 Installation on a RISC System/6000

To install the Configuration Program on a RISC System/6000 workstation (requires AIX 3.2.5 or higher):

1. Log in to AIX as a non-root user.
2. Place diskette 1 in the 3.5-inch diskette driver.
3. At the AIX prompt, type the following command:

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`

4. Type `chmod 550 INSTALL.AIX` at the AIX prompt:

Where

`chmod` Change 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.

5. At the AIX prompt, type `INSTALL.AIX` and press Enter.

6. Follow the prompts that appear on the panel to complete the installation.

2.6.3.2 Installation on a PC

To install the Configuration Program on a PC workstation running OS/2 2.1 or 3.0, follow these steps:

1. Place diskette 1 in the diskette drive.
2. At the OS/2 prompt, type A:OS2INST and press Enter.
3. Follow the prompts that appear on the panel.

The Configuration Program will install itself on the system and will prompt you to enter the installation drive and directory. An IBM 2210 folder will be created with the Configuration Program icon inside.

Note: The Configuration Program will not currently work on OS/2 WARP 4.0. Compatibility with OS/2 WARP 4.0 is considered a priority and is being addressed.

To install the Configuration Program on a PC workstation running Windows, type WIN A:INSTALL beside the DOS prompt or follow these steps for Windows 95:

1. Start Windows 95.
2. Place diskette 1 in the diskette drive.
3. Double-click on the **Mycomputer** icon.
4. Double-click on the **3 1/2 Floppy [A:]** icon.
5. Double-click on the **Install.exe** icon.
6. Follow the prompts that appear on the panel.

Figure 20 shows the window when installing configuration for Windows 95.

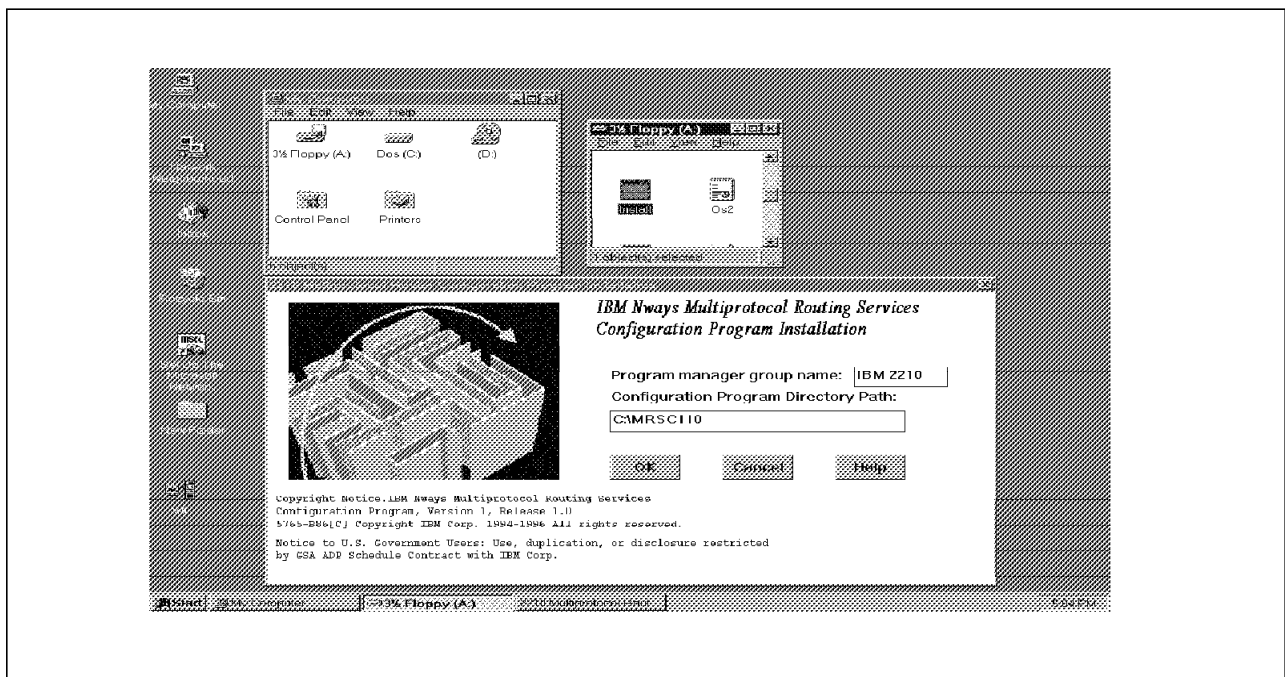


Figure 20. Install the Configuration Program for Windows 95

For Windows 3.1x:

Note: If you have not installed the WIN32s diskettes (required for Windows only), you must do so *before* installing the Configuration Program.

1. Start Windows.
2. Place diskette 1 in the diskette drive.
3. Select **File** from the menu bar icon.
4. Select **Run** from the pull-down window.
5. Type A:INSTALL on the command line and select **OK** to start the installation.
6. Follow the prompts that appear on the panels.

The Configuration Program will install itself on the system disk drive and will prompt you to enter the installation directory, group box name and any other details necessary to complete the installation.

After a successful installation, an icon labeled MRS V1R1.0 Config will be added to the program group you specify using the installation program or, by default, to the IBM 2210 program group. In addition, an icon is now provided for the README file as well.

For WIN32s:

1. Stop all Windows applications.
2. In Windows Program Manager, select **File**, then **Run**.
3. Put diskette 7 of 8 in diskette drive A:.
4. On the command line (of **Run**) enter A:SETUP and choose **OK**.
5. Note the message to add SHARE.EXE to AUTOEXEC.BAT file. (SHARE is part of DOS; the AUTOEXEC.BAT file can be modified after this install.)
6. At the next prompt for the WIN32s Setup diskette, insert 8 of 8.
7. Expect message WIN32s files successfully installed.
8. Optional FREECELL program is on diskette 7 of 8.
9. Clicking on **Setup** will restart Windows to complete the installation.

2.6.4 Migration Support for Down-Level Configuration Files

To use the configuration files created by earlier versions of the configuration program, you must migrate to the new release format. If the only copy of the configuration is either in the router or in binary format, you must use the version of the configuration program that created the configuration to create the configuration database file.

2.6.4.1 Creating Configuration Database File

To create the configuration database file:

1. Start the previous version of the configuration program.
2. Select **Read Router Configuration** to read the existing configuration into the configuration program. Another way to load an existing configuration into the program is to select **Communication, Single**, and then **Retrieve** from the Configuration menu.
3. Select **Save Configuration** from the File menu.
4. Save the configuration into a file with file extension .CBD.

2.6.4.2 Converting a Configuration Database File

Configurations already in a configuration database may be migrated to the new release format by doing the following:

1. Start the current version of the configuration program.
2. Select **Open Configuration** from the File menu. Select the old configuration from within the .cdb file you created in "Creating Configuration Database File." The configuration program will then ask if you wish to convert the configuration to the new format.
3. Select **Save Configuration As** to save the configuration to a new file with a new name, which allows you to keep the existing configuration file for future use.

2.6.4.3 Router Configuration Format (Readable by 2210)

If you did not save .cdb files using the previous versions of the Configuration Programs, you will still be able to read the configuration files created by the 2210 router command line or by the MRNS V1R3.0 2210 Configuration Programs. Use the Read router configuration (for a .cfg file) or clicking on **Communicate>Retrieve** to perform the read. Note that migration is not performed on files read using these functions. The preferred migration method uses the .cdb files and the Open function of the Configuration Program.

2.6.5 An Overview of the IBM 2210 Configuration Program

The IBM 2210 Configuration Program consists of two main windows:

- The Navigation Window
- The configuration window

The Navigation Window displays a directory tree consisting of the various components that you can configure.

To select any particular configuration window, click the left mouse button on the item you are interested in. The configuration window will now display the configuration window you have selected.

Help is available for each field within a panel. You may access the help by pressing PF1.

If the field requires you to enter a value, ensure you press Enter/Return after entering your value. If you don't do this, the value may not be saved.

Specific configurations using the Nways MRS Configuration Program are included in the scenarios shown in this book.

2.6.6 The 2210 Navigation Window

The 2210 Navigation Window lists the configuration windows grouped by function (for example, Devices, IP, IPX, and so on). When you select a panel in the Navigation Window, the presentation window will display the configuration questions for the selected panel.

This Navigation Window is a method of presenting information hierarchically.

An example of a hierarchical structure is as follows:

Routers

Devices Interfaces

Note that folder icons are displayed by certain items in the navigation list. These items in the navigation tree group windows by function. Also note that there can be other nested folders within a given folder. The first time you start the configuration program, the entire navigation list is presented. However, the navigation list can be contracted (and later on expanded) by selecting items that have folder icons.

The way to expand or contract the navigation list is by pressing and holding the middle button (on a three-button mouse) or the right button (on a two-button mouse) and selecting the appropriate choice from the displayed pop-up menu.

The Router category (at the top of the navigation list) is considered the root of the navigation tree. The next level of functions are as follows:

- Router
 - Devices
 - System
 - Protocols
 - Bridging
 - Features

The complete Navigation Window is shown in Figure 21 on page 49.

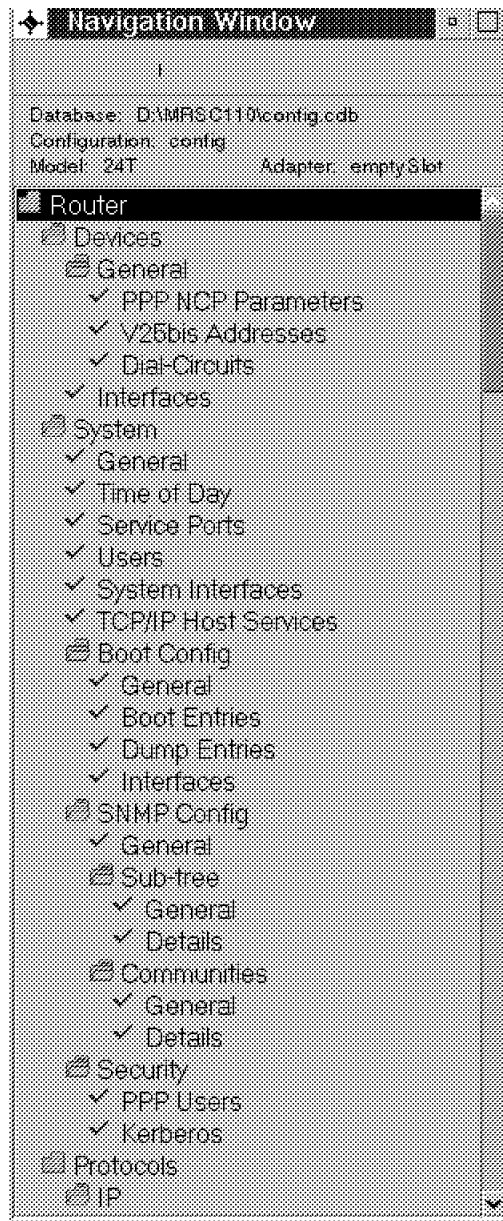


Figure 21 (Part 1 of 2). The IBM 2210 Configuration Program Navigation Window



Figure 21 (Part 2 of 2). The IBM 2210 Configuration Program Navigation Window

A sample panel is shown in Figure 22 on page 51. All panels within the Nways MRS Configuration Program will look similar to this one.

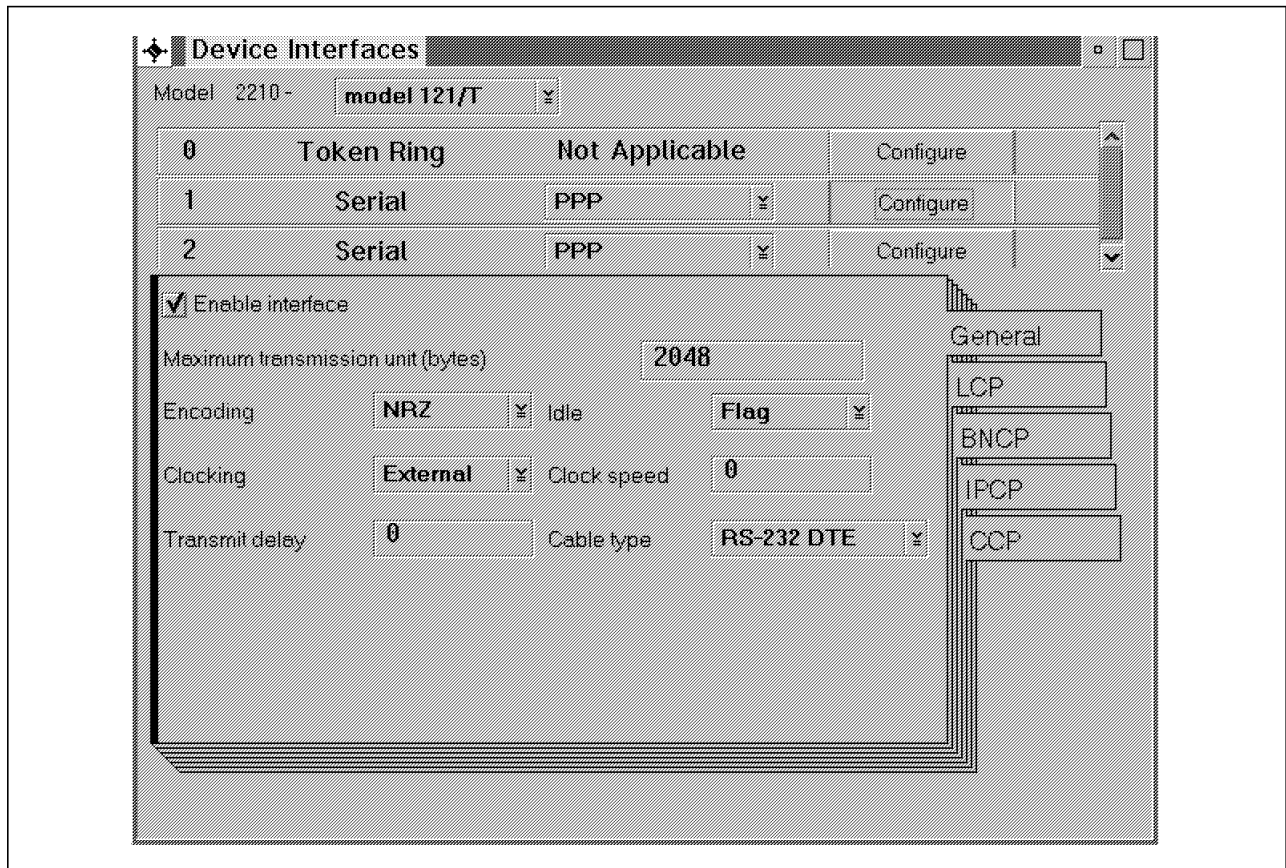


Figure 22. Device Interfaces Configuration Window

2.6.7 Configure Pull-Down Menu (on the Navigation Window)

The following options are available by clicking on the **Configure** menu bar choice of the Navigation Window.

- New Configuration

This option initializes a new configuration. This means that you are starting a clean configuration from scratch for the model you choose from the submenu.

- Save Configuration As

This option saves the working configuration in the configuration database. A single database can hold multiple configurations.

Configurations saved in the configuration program are readable only by the Configuration Program. The router only understands configurations that are created by the Create Router Configuration option.

- Read Router Configuration

This option is not available at this stage.

- Create Router Configuration

This option creates a configuration file that you may send to the router.

- Open Configuration

This option reads configurations from configuration databases that were previously saved by the configuration program.

- Delete Configuration

This options deletes configurations from the configuration databases.

- Communications

This option allows you to send configurations to the 2210. You can send a single configuration to a 2210 by selecting the Single Router option, or you can send multiple configurations to multiple 2210s by selecting the Multiple Routers option.

- ASCII File

This option is for creating an ASCII version of the configuration file. Release 2 now allows you to print the file to obtain a hardcopy report.

2.6.8 Options Pull-Down Menu (on the Navigation Window)

- Font

This option allows you to select the fonts that are on your workstation.

- Color

This option works by dialing a color with the three sliders that represent the RGB values of the color. Once the desired color is displayed, click on either the **Warning** or **Error** color box to use that color. Currently, only the error color is used within the program.

- Message Prompting

Message prompting filters out those types of messages that are turned on in the message prompting customization window. When the configuration is validated, only those classes of messages selected by the user will be displayed. Currently, some of the validation code ignores the filters and displays the messages anyway.

- Default Model

This option allows you to select a model type as the default. On the next activation of the Configuration Program, the values associated with the model type become the initialized values.

2.6.9 Validating Configuration Files

In the Navigation field, check marks or question marks are displayed next to each screen or function name. Check marks indicate that the configuration data associated with the field or function has been validated by the configuration program and can be sent to the 2210.

Question marks indicate that some parameter is not valid for this configuration to be used on the 2210.

Invalid configurations can be saved to database files, but you should not create router configuration files or attempt to send them to the 2210 unless they have been validated by the configuration program.

2.6.10 Sending/Retrieving the Configuration File

Using the Configuration Program, you can send configuration files to the IBM 2210 via SNMP SETs.

Using this option, you can send router formatted configuration data for the working (currently opened) configuration. This feature uses SNMP SETs and is the preferred method of transporting configuration data to the router's configuration memory. Multiple router's may be configured in this manner with one SEND MULTIPLE action.

The Communication function will communicate with routers using the SNMP protocol. The router must be set up with an IP address and have an SNMP community with access defined as WRITE_READ_TRAP for send and restart. For retrieve and query, the community access can be READ_TRAP or WRITE_READ_TRAP.

You *must* make sure that TCP/IP is installed and *running* before using the Communications Single and/or Communications Multiple functions.

The single send will send the configuration that is currently open. The IP destination and community fields will default to what is defined in the configuration. The timeout value is the maximum number of seconds the send function will wait for a response. Select the appropriate actions:

1. Send the configuration to the router
2. Restart the router immediately or later
3. Send the configuration and then restart the router
4. Query the router for the system description
5. Retrieve the configuration from the router

The multiple send/retrieve will act on configurations that are saved in the configuration database. The send lists (.CDB files) contain groups of configuration names and parameters to be sent and/or retrieved. For each configuration, the names and parameters are: IP destination, community, timeout, send, restart, date, time, query, and retrieve. The configurations can also be retrieved from several routers into one or more configuration databases.

An example of how to configure SNMP Community Name access rights prior to using the IBM 2210 communication utilities is shown in Figure 23 on page 54.

```

Config>protocol snmp
SNMP Config>add community
Community name: []? 2210a
SNMP Config>set community access write
Community name: []? 2210a
SNMP Config>list community access

```

Community Name	Access
public	Read, Trap
2210a	Read, Write, Trap

```

SNMP Config>

```

Figure 23. Configuring SNMP Community Name Access Rights

A simple example of restarting the router via the IBM 2210 Configuration Program is shown in Figure 24.

Note: To access the window shown, you must select **Configure**, **Communications**, and then **Single router** from the IBM 2210 Configuration Program menu options.

The dialog box titled "Send..." contains the following fields and options:

- IP Address or name:** 9.67.46.30
- Community:** 2210c1g
- Timeout (in seconds):** 10
- ☐ Send configuration to router
- ☒ Restart router
- Date:** 9/28/1995
- Time:** 11:31:01 am
- ☐ Query router information
- Buttons:** OK, Cancel, Help

Figure 24. Communication to the IBM 2210 via SNMP

2.7 IBM 2210 PROM Load/Dump Program

The PROM Load/Dump program is the program that performs boot operations and diagnostics on the IBM 2210. This program is kept in Boot Flash and can be replaced as necessary to support new adapters or install corrective services. In order to use the ISDN BRI adapter, ISDN PRI adapter, 25MBPS ATM interface adapter or the 4/8 port WAN concentration adapters, the IBM 2210's PROM Load/Dump program must be at Version 2.20 or higher.

2.7.1 Loading the PROM Load/Dump Program

The IBM 2210 PROM Load/Dump program is kept in Boot Flash, which is only accessible by the PROM Load/Dump program. The only way to load the PROM Load/Dump Program into Boot Flash is to load the PROM Load/Dump program, prom_2.20, from the diskette included with this shipment into the IBM 2210 DRAM and allow it to execute. During execution, it will load itself into Boot Flash.

There are various ways to load the IBM 2210 Load/Dump program into the IBM 2210 DRAM. The methods are listed below:

1. Loading using Zmodem
2. Loading using tftp get
3. Loading using boot manual

Please refer to the readme file that comes with the prom_2.20 diskette.

We found there is a problem when we used tftp get to load the IBM 2210 Load/Dump program. When using the LOAD LOCAL option via a Telnet session, the tool that writes the new code into the Flash causes the router to load IBD image prom_2.20 and writes it to the Flash into an endless loop, instead loading the IBD load image as MRS.XXX. The loop can only be stopped by attaching a terminal to the service port and pressing a Ctrl+C. If power is removed while the program is writing the Flash during the loop, the boot code in Flash will be corrupted and cause the system board to have to be replaced.

The other two options, boot manual and Zmodem, using the service port are OK. So *do not* use the LOAD LOCAL option to upgrade the BOOT code to V2.20 until you get a fix.

Chapter 3. Interfaces

This chapter describes the LAN and WAN interfaces provided by the IBM 2210.

3.1 The LAN Interfaces

There are two types of LAN interfaces:

- Ethernet
- Token-ring

For both interfaces, we list the different protocols used, and look at the frame layout for all these protocols.

In each frame of each protocol, the *destination MAC address* is the workstation MAC address where the frame is going to, and the *source MAC address* is the workstation MAC address where the frame has been sent from.

3.1.1 The Ethernet Interface

The Ethernet interfaces support both Ethernet II and the IEEE 802.3 protocol.

In Ethernet segments, the MAC addresses are in canonical format. It means that the bytes of the MAC address begin with the least significant bit (LSB) from left to right.

Both Ethernet II and 802.3 protocols can be used on the same physical network simultaneously. However, stations using one protocol cannot interoperate with stations using the other protocols.

The layout of the Ethernet II frame is shown in Figure 25.

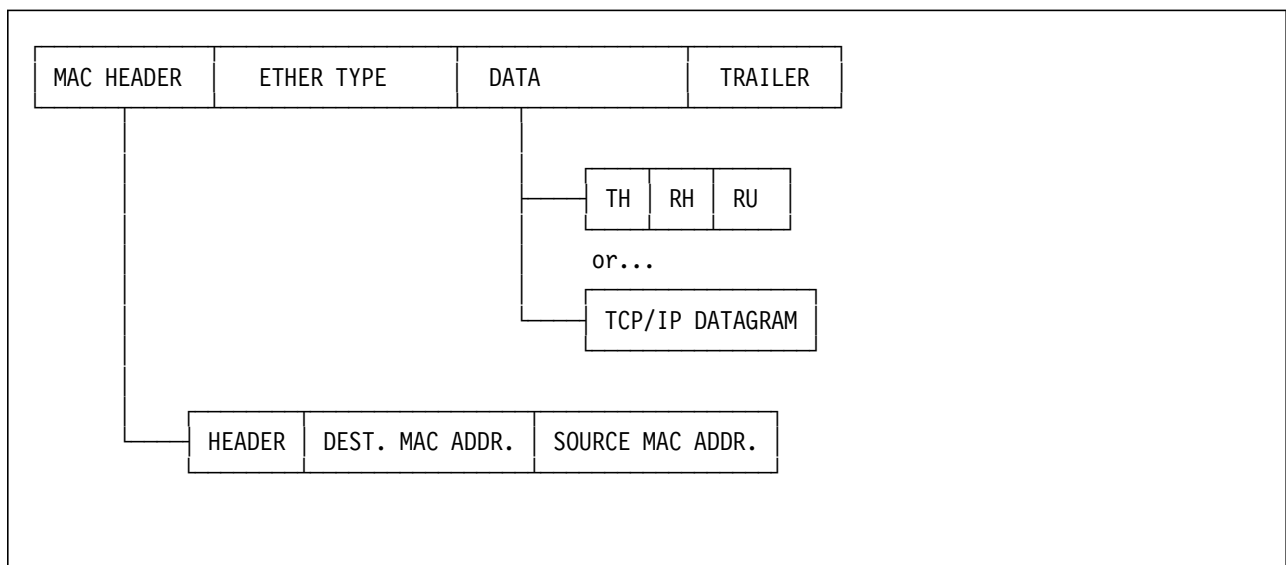


Figure 25. Layout of the ETHERNET II Protocol

In Ethernet II, the Ether Type identifies the protocol carried in the upper layer. For example, the Ether Type used to identify IP is 0800.

The layout of the IEEE 802.3 protocol is shown Figure 26 on page 58.

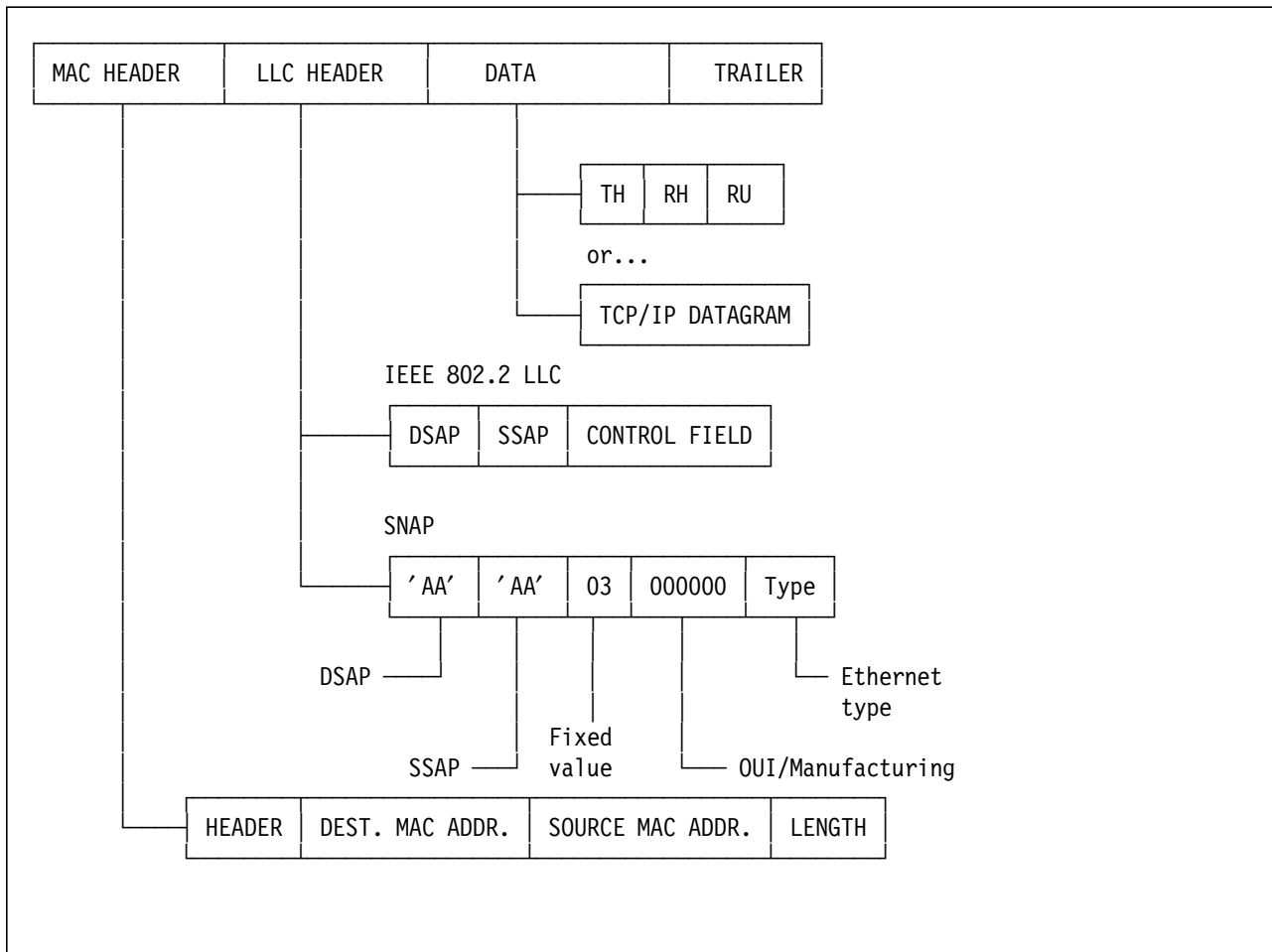


Figure 26. Layout of the IEEE 802.3 Protocol

The IEEE 802.3 format may use SNAP or 802.2 LLC layout.

With 802.2 LLC, the protocol of the network layer is identified by the SAP. There are two SAPs in an LLC 802.2 frame: the destination SAP (DSAP) and the source SAP (SSAP). For example, the SAP used to identify NetBIOS is F0.

With SNAP, both DSAP and SSAP = AA, and the protocol of the network layer is identified by the Type field in the SNAP header. The Type field has the same value as the Ether Type field of the Ethernet II protocol.

3.1.2 The Token-Ring Interface

The token-ring interface supports the IEEE 802.5 protocol.

In token-ring segments, the MAC addresses are in non-canonical format. It means that the bytes of the MAC address begin with the most significant bit (MSB) from left to right.

The layout of the IEEE 802.5 is shown in Figure 27 on page 59.

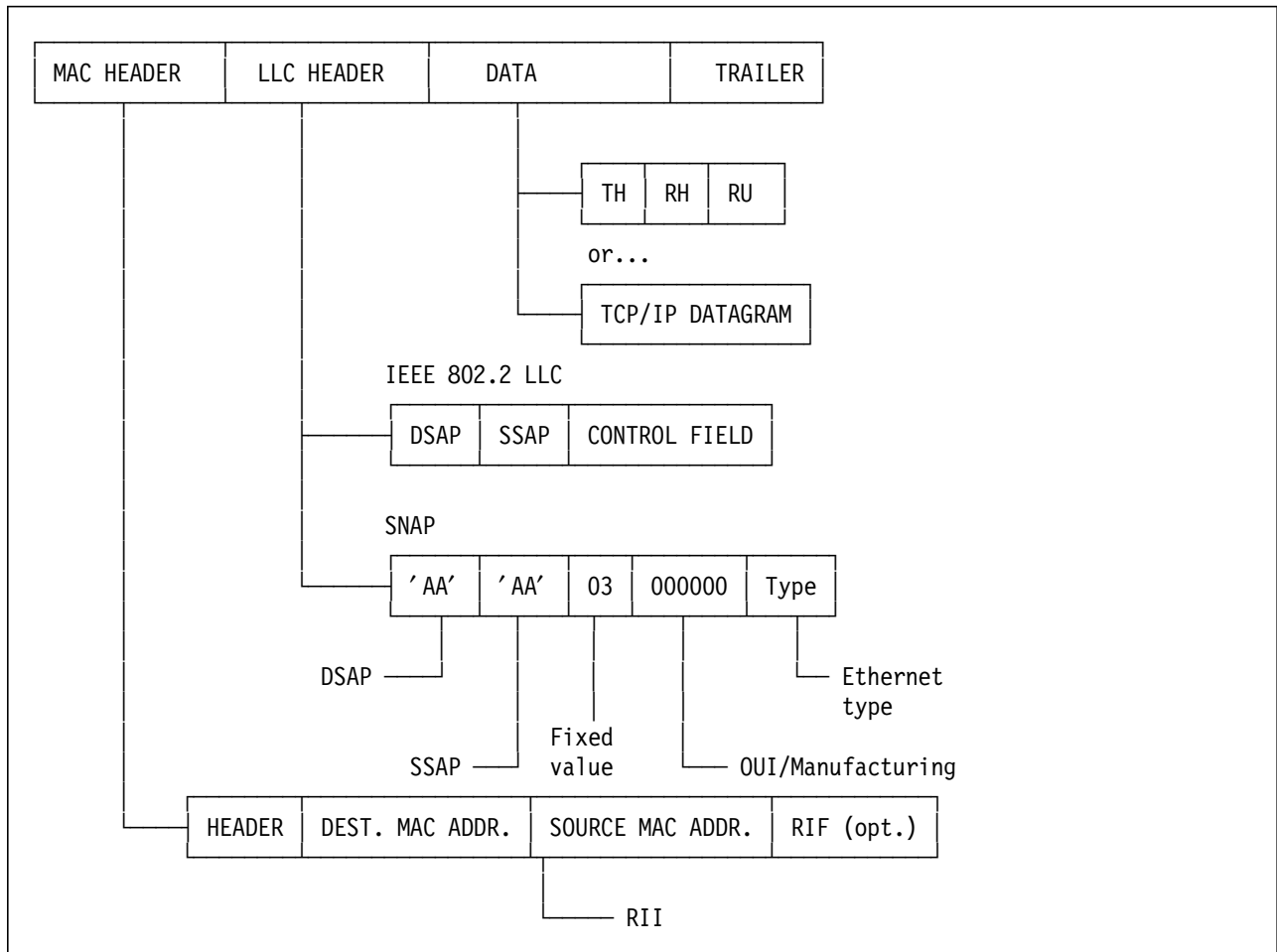


Figure 27. Layout of the IEEE 802.5 Protocol

The IEEE 802.5 format may contain SNAP or 802.2 LLC layout.

As explained previously for the IEEE 802.3 protocol, for the IEEE 802.5 protocol with 802.2 LLC the protocol of the network layer is identified by the SAP. There are two SAPs in an LLC 802.2 frame: the destination SAP (DSAP), and the source SAP (SSAP). For example, SAP F0 is used for NetBIOS. With SNAP, both DSAP and SSAP are set to AA.

When the source route bridging is enabled on the interface, the IEEE 802.5 frame contains a routing information indicator (RII) that is the first bit of the source MAC address. This bit indicates that the frame contains a routing information field (RIF) that lists the path between the source MAC address and the destination MAC address.

The layout of the RIF is shown Figure 28 on page 60.

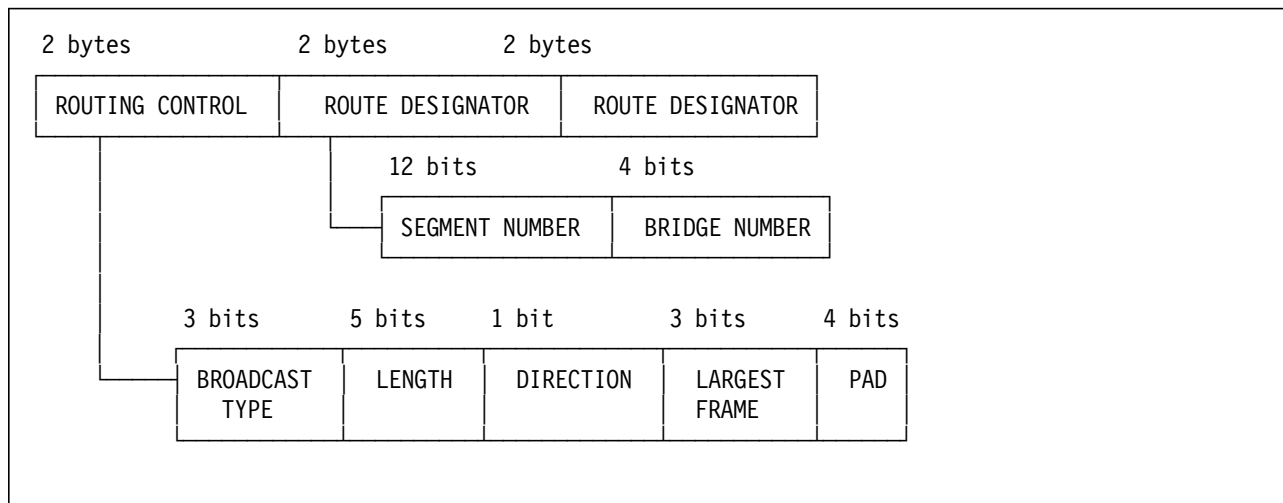


Figure 28. Routing Information Field Layout

The path is shown in the RIF by the route designator. The route designators contain the segment numbers and the bridge numbers that the frame has to go through to get from the source MAC address to the destination MAC address.

If the frame does not contain the RII bit, it means the frame is not bridged via source route bridges, but the frame could be bridged via transparent bridges.

3.2 Configure the LAN Interfaces

An IBM 2210 has only one LAN interface; it can be either an Ethernet LAN or a token-ring LAN. It depends on the model of the IBM 2210. Models 121, 12T, 125 and 127 have a token-ring LAN. Models 122, 12E, 126 and 128 have an Ethernet LAN. The LAN interface is always the network number 0 for the IBM 2210.

3.2.1 Configuring the Ethernet Interface

In this section we describe the different parameters for the Ethernet interface.

Table 22 on page 61 shows you the available commands to configure the Ethernet interface customization.

The *Nways MRS Software User's Guide* documentation covers these commands in detail.

<i>Table 22. Ethernet Configuration Commands</i>	
Command	Function
? (Help)	Displays all the Ethernet commands, or lists the subcommand options for specific commands.
Connector-Type	Sets the connector type plugged in the 2210.
Frame	Sets the type of IPX frames used.
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type 8137) or IEEE 802.3 (with or without 802.2, with or without SNAP).
List	Displays the current Ethernet configuration.
Exit	Exits the Ethernet configuration, and comes back to CONFIG Process.

For the Ethernet, you can set up the following parameters:

- Connector-Type
- Frame
- IP-Encapsulation

The following references are made to the examples given in Figure 29 on page 63 (for ASCII console configuration) and Figure 30 on page 64 (for Nways MRS Configuration Program).

On an ASCII console, you can always issue a question mark (?) to have all possible commands shown. **3**

- Enabling the Ethernet interface **1**

The Ethernet interface must be enabled to work properly. With an ASCII console configuration, the Ethernet is enabled by default.

With Nways MRS, you must select **Enable Interface** for the Ethernet interface from the Devices directory.

- Access the Ethernet configuration **2**

To access the Ethernet LAN configuration of your IBM 2210, type network 0 in the CONFIG process from the ASCII console.

For Nways MRS Configuration Program, select **Interfaces** from the Devices directory. In the Device Interface window, specify the model of the 2210. Then, select **Configuration** for the Ethernet interface.

- Connector-type parameter **4**

The connector-type parameter could be RJ45 for the 10Base-T, or AUI for the 10Base-5. You could also set it as AUTO-CONFIG. This will let the IBM 2210 automatically sense the type of connector that is plugged in.

You must select either AUTO-CONFIG or the type of cable actually plugged in the IBM 2210.

Note

On the Nways MRNS Configuration Program, the connector-type parameter could be BNC. BNC is not provided with the IBM 2210. You should not select this value.

- IP-encapsulation parameter **5**

The IP-encapsulation parameter can be Ethernet or IEEE-802.3. The default setting is Ethernet.

- Frame parameter **6**

The frame or framing type parameter has four possible values:

- Ethernet 802.3
- Ethernet II
- Ethernet 802.2
- Ethernet SNAP

This parameter applies only for the IPX frames.

In the Nways MRNS Configuration Program, this parameter is on the interfaces panel of the IPX subdirectory. This panel is called IPX-Interfaces.

- View the current configuration setting **7**

On Nways MRNS Configuration Program, you can directly see the value set for each parameter in the corresponding panel.

In ASCII console customization, you must issue the list command to see the current setting of these parameters.

In the given example, to show you the different settings for these parameters, we have changed each of them, followed by a new list command.

In the output from the list command, the frame parameter is called NetWare IPX encapsulation.

For an example of how the above commands are used, refer to Figure 29 on page 63 (for ASCII console configuration) and to Figure 30 on page 64 (for Nways MRNS Configuration Program).

```

*
*talk 6

Config>enable interface 0      1
Config>network 0               2
Ethernet interface configuration
ETH config>?                   3
CONNECTOR-TYPE
IP-ENCAPSULATION
LIST
FRAME
EXIT
ETH config>connector-type ?    4
AUTO-CONFIG
AUI (10Base-5)
RJ45 (10Base-T)
ETH config>ip-encapsulation ?  5
ETHERNET
IEEE-802.3
ETH config>frame ?             6
ETHERNET_II (Ethernet type 8137)
ETHERNET_8023 (IEEE 802.3 'raw' without 802.2)
ETHERNET_8022
ETHERNET_SNAP
ETH config>list                7
Connector type:                AUTO-CONFIG
NetWare IPX encapsulation:    ETHERNET_802.3
IP Encapsulation:             ETHER

ETH config>frame ethernet_snap
ETH config>list
Connector type:                AUTO-CONFIG
NetWare IPX encapsulation:    ETHERNET_SNAP
IP Encapsulation:             ETHER

ETH config>connector-type rj45
ETH config>list
Connector type:                RJ45 (10Base-T)
NetWare IPX encapsulation:    ETHERNET_SNAP
IP Encapsulation:             ETHER

ETH config>ip-encapsulation ieee-802.3
ETH config>list
Connector type:                RJ45 (10Base-T)
NetWare IPX encapsulation:    ETHERNET_SNAP
IP Encapsulation:             IEEE-802.3

ETH config>exit
Config>Ctrl+p
*

```

Figure 29. Ethernet Configuration via ASCII Console

```

On 2210 Navigation window:
  Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window:
  Select MODEL
    Select MODEL 126
  Select CONFIGURATION of Ethernet line 2
  ENABLE INTERFACE 1
  Select CONNECTOR TYPE 4
    Select AUTO-CONFIG
    or AUI
    or RJ45
  Do not select BNC
  Select IP ENCAPSULATION 5
    Select ETHERNET
    Select 802.3

On 2210 Navigation window:
  Select INTERFACES panel of IPX subdirectory of PROTOCOL directory

On IPX - INTERFACES Window:
  Select CONFIGURATION of Ethernet line
    Select FRAMING TYPE 6
    Select Ethernet 802.3
    or Ethernet II
    or Ethernet 802.2
    or Ethernet SNAP

```

Figure 30. Ethernet Configuration via Nways MRNS Configuration Program

3.2.2 Configuring the Token-Ring Interface

In this section, we describe the different parameters for the token-ring interface customization.

Table 23 on page 65 shows you the available commands to configure the token-ring interface.

The *Nways MRNS Software User's Guide* documentation covers these commands in detail.

<i>Table 23. Token-Ring Configuration Commands</i>	
Command	Function
? (Help)	Displays all the token-ring commands, or lists the subcommand options for specific commands.
Frame	Set the NetWare IPX encapsulation type.
List	Displays the current token-ring configuration.
LLC	Accesses the LLC configuration.
Media	Sets the media type plugged in the 2210 as shielded (STP) or unshielded (UTP).
Packet-size	Changes packet-size defaults for all token-ring networks.
Set	Sets the aging time of the RIF cache.
Source-Routing	Enables or disables source routing on the interface.
Speed	Sets the token-ring speed in MBps.
Exit	Exits the token-ring configuration, and returns to CONFIG process.

For the token-ring, you can set up the following parameters:

- Frame
- LLC
- Media
- Set
- Packet-size
- Source-Routing
- Speed

Note

Entering the LLC command, the IBM 2210 always responds: LLC CONFIG is not available for this network, even if DLSw is included in the software load.

The following references are made to the examples given in Figure 31 on page 68 (for ASCII console configuration) and Figure 32 on page 73 (for Nways MRNS Configuration Program).

On an ASCII console, you can always issue a question mark (?) to have all the possible commands shown. **3**

- Enabling the token-ring interface **1**

The token-ring interface must be enabled to work properly. With ASCII console configuration, the token-ring interface is enabled by default.

With Nways MRNS, you must select **Enable Interface** for the token-ring interface from the Devices directory.

- Accessing the token-ring configuration **2**

To access the token-ring LAN configuration of your IBM 2210, type network 0 in the CONFIG process for the ASCII console.

For Nways MRNS Configuration Program, select **Interfaces** from the Devices directory. In the Device Interface window, specify the model of the 2210. Then, select **Configuration** for the token-ring interface.

- Media or cable-type parameter **4**

The media parameter in ASCII console configuration corresponds to the cable-type parameter on Nways MRNS Configuration Program.

This can be unshielded (UTP) or shielded (STP).

This parameter should be set to the corresponding cable currently plugged into the IBM 2210 token-ring interface.

- RIF timer parameter **5**

The RIF timer parameter is the maximum amount of time (in seconds) that the information in the RIF is maintained before it is refreshed. The default is 120.

With the ASCII console customization, you should issue the command Set rif-timer to change it.

- MAC address or physical-address parameter **6**

This parameter is the locally administered address (LAA) of the token-ring interface. If you do not enter any value for this parameter, by default, the IBM 2210 token-ring MAC address will be the universally administered address (UAA).

With the ASCII console customization, this parameter is called physical-address. You should enter it in the following format:

40:00:22:10:A0:01

and in non-canonical format.

With Nways MRNS Configuration Program, this parameter is called MAC address. You should enter it in non-canonical format as follows:

40002210A001

- Packet-size parameter **7**

This parameter is the maximum size of the token-ring packets. The possible values depend on the speed of the token-ring.

For a token-ring of 4 Mbps, the possible values are:

- 1500
- 2052
- 4472

For a token-ring of 16 Mbps, the possible values are:

- 1470
- 2052
- 4399
- 8130
- 11407
- 17749

With the ASCII console customization, only the 16 Mbps values of the packet-size parameter are valid (regardless of the actual speed value). Consequently, with ASCII console customization, you could not enter a packet-size of 1500 or 4472, even with a token-ring speed of 4 Mbps.

Note

With the Nways MRNS Configuration Program, the *packet size* parameter is reset to 2052 value if you select the *speed* parameter.

- Source-routing or end node source routing parameter **8**

This parameter must be enabled if using source routing bridging on the token-ring interface. Otherwise, it should be disabled.

With ASCII console customization, this parameter is called source-routing and the default is ENABLED.

With the Nways MRNS Configuration Program, this parameter is called end node source routing and is DISABLED by default.

- Speed parameter **9**

This parameter must be the actual speed of the token-ring; otherwise, it may disrupt the network.

The two options are: 4 Mbps or 16 Mbps.

The default is 4 Mbps for both ASCII console customization and the Nways MRNS Configuration Program.

- The frame or framing-type parameter **10**

The frame parameter has four possible values:

- Token-Ring MSB
- Token-Ring LSB
- Token-Ring_SNAP MSB
- Token-Ring_SNAP LSB

This parameter applies only for the IPX frames.

In the Nways MRNS Configuration Program, this parameter is on the Interfaces panel of IPX subdirectory. This panel is called the IPX - Interfaces window.

- View the current configuration setting **11**

In the Nways MRNS Configuration Program, you can directly see the value set for each parameter in the corresponding window.

In ASCII console customization, issue the list command to see the current setting of these parameters.

To show you the different settings for these parameters, we changed each of them, followed by a new list command.

When IPX protocol is not ENABLED, there is no frame setting, and the output from the list command shows: IPX interface configuration missing. **12**

When IPX protocol is ENABLED, the output of the list command shows the frame parameter as NetWare IPX encapsulation. **13**

For more information about IPX configuration, see Chapter 9, “IPX Routing and Configuration” on page 405.

```

*
*talk 6

Config>enable interface 0      1
Config>network 0               2
Token-Ring interface configuration
TKR config>?                   3
EXIT
FRAME
LIST
LLC
MEDIA
SET
PACKET-SIZE bytes
SOURCE-ROUTING
SPEED Mb/sec
TKR config>media ?             4
SHIELDED twisted pair
UNSHIELDED twisted pair
TKR config>set ?
RIF-TIMER                      5
PHYSICAL-ADDRESS              6
TKR config>packet-size ?      7
Packet (MSDU) size (1470, 2052, 4399, 8130, 11407, 17749) [2052]?
TKR config>source-routing ?   8
ENABLED
DISABLED
TKR config>speed ?            9
Speed (4 or 16) [4]?
TKR config>frame ?            10
TOKEN-RING_SNAP
TOKEN-RING
TKR config>frame token-ring ? 10
MSB
LSB
TKR config>frame token-ring_snap ? 10
MSB
LSB
TKR config>list               11
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                     4 Mb/sec
Media:                     Shielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
IPX interface configuration record missing 12

:

```

Figure 31 (Part 1 of 5). Token-Ring Configuration via the ASCII Console

```

:
TKR config>media unshielded
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         120
Source Routing:          Enabled
MAC Address:              000000000000
IPX interface configuration record missing

TKR config>packet-size 1470
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 1470
Speed:                    4 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         120
Source Routing:          Enabled
MAC Address:              000000000000
IPX interface configuration record missing

TKR config>speed 16
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 1470
Speed:                    16 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         120
Source Routing:          Enabled
MAC Address:              000000000000
IPX interface configuration record missing

TKR config>set rif-timer 60
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 1470
Speed:                    16 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         60
Source Routing:          Enabled
MAC Address:              000000000000
IPX interface configuration record missing

:

```

Figure 31 (Part 2 of 5). Token-Ring Configuration via the ASCII Console

```

:
TKR config>source-routing disable
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 1470
Speed:                    16 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         60
Source Routing:          Disabled
MAC Address:              000000000000
IPX interface configuration record missing

TKR config>set physical-address 40:00:22:10:A0:01
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 1470
Speed:                    16 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         60
Source Routing:          Disabled
MAC Address:              40002210A001
IPX interface configuration record missing

TKR config>frame token-ring_snap msb
IPX interface configuration record missing
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 1470
Speed:                    16 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         60
Source Routing:          Disabled
MAC Address:              40002210A001
IPX interface configuration record missing

TKR config>exit
:

```

Figure 31 (Part 3 of 5). Token-Ring Configuration via the ASCII Console

```

:
Config>protocol ipx
IPX protocol user configuration
IPX config>?
DISABLE
ENABLE
EXIT
FRAME
LIST
SET
ADD
DELETE
MOVE access-control
IPX config>enable ipx
IPX config>list

IPX globally                enabled
Host number (serial line)   000000000000
Router Name (IPXWAN)
NodeID (IPXWAN)             0
Maximum networks            32
Maximum total alt. route entries 128
Maximum alt. routes per dest. network 3
Maximum services            32
Maximum Network Cache entries 64
Maximum Local Cache entries 64

No IPX interfaces enabled

IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.
IPX config>exit
Config>network 0
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 1470
Speed:                    16 Mb/sec
Media:                    Unshielded

RIF Aging Timer:          60
Source Routing:            Disabled
MAC Address:               40002210A001
NetWare IPX encapsulation: TOKEN-RING      MSB
:

```

13

Figure 31 (Part 4 of 5). Token-Ring Configuration via the ASCII Console

```
:
TKR config>frame token-ring_snap msb
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 1470
Speed:                    16 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         60
Source Routing:          Disabled
MAC Address:              40002210A001
NetWare IPX encapsulation: TOKEN-RING_SNAP MSB
TKR config>exit
Config>Ctrl+p
*
```

Figure 31 (Part 5 of 5). Token-Ring Configuration via the ASCII Console

On 2210 Navigation window :

- Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :

- Select MODEL
 - Select **MODEL 125**
- Select CONFIGURATION of Token-Ring line **2**
 - ENABLE INTERFACE** **1**
 - Select **CABLE TYPE** **4**
 - Select **UTP**
 - or **STP**
 - RIF TIMER = 120** **5**
 - MAC ADDRESS = 000000000000** **6**
 - Select **PACKET SIZE** **7**
 - For SPEED = 4 Mbps
 - Select **1500**
 - or **2052**
 - or **4472**
 - For SPEED = 16 Mbps
 - Select **1470**
 - or **2052**
 - or **4399**
 - or **8130**
 - or **11407**
 - or **17749**
 - Enable **END NODE SOURCE ROUTING** **8**
 - Select **SPEED** **9**
 - Select **4**
 - or **16**

On 2210 Navigation window :

- Select INTERFACES panel of IPX subdirectory of PROTOCOL directory

On IPX - INTERFACES Window :

- Select CONFIGURATION of Token-Ring line
 - Select **FRAMING TYPE** **10**
 - Select **Token-ring MSB**
 - or **Token-ring LSB**
 - or **Token-ring SNAP MSB**
 - or **Token-ring SNAP LSB**

Figure 32. Token-Ring Configuration via the Nways MRNS Configuration Program

3.3 Monitoring the LAN Interfaces

An IBM 2210 can have up to two LAN interfaces. It can be either an Ethernet LAN or a token-ring LAN, depending on the model of the IBM 2210. The LAN interface is always the network number 0 for the IBM 2210. On models with two LAN interfaces the network numbers are 0 and 5.

After the IPL of the IBM 2210, when the LAN interface is up, the LAN interface green LED on the 2210 panel should be on, not blinking. The amber LED interface should be off.

3.3.1 Monitoring the Ethernet Interface

In this section, we describe the different commands to monitor the Ethernet interface and to find its universally administered address.

Monitoring can only be done via an ASCII console plugged in the IBM 2210 or via a Telnet session to the IBM 2210. A sample is shown in Figure 34 on page 77.

- Access CGW Operator Console **1**

The CGW Operator Console (also called CGWCON) is the Gateway Console process. It will allow you to monitor your IBM 2210.

For more information about the GWCON process, see 2.4.7, "GWCON Process" on page 35.

To access the CGW Operator Console you must issue the Talk 5 command.

- Access the Ethernet statistics **2**

This shows you the statistics for the Ethernet interface for example, the physical MAC address of the Ethernet interface.

- Access Ethernet monitoring **3**

To access the monitoring of the Ethernet interface, issue the Network 0 command.

- The Collisions command **4**

This is the only command possible from the Ethernet configuration. It shows you the collision count of transmission for packets that had collisions before a successful transmission.

***talk 5** **1**

CGW Operator Console

+interface 0 **2**

Nt	Nt'	Interface	CSR	Vec	Self-Test Passed	Self-Test Failed	Maintenance Failed
0	0	Eth/0	81600	5E	1	0	0

Ethernet/IEEE 802.3 MAC/data-link on SCC Ethernet interface

Physical address 0000938080D0
PROM address 0000938080D0

Input statistics:

failed, frame too long	0	failed, FCS error	0
failed, alignment error	0	failed, FIFO overrun	0
internal MAC rcv error	0	packets missed	0

Output statistics:

deferred transmission	0	single collision	0
multiple collisions	0	total collisions	0
failed, excess collisions	0	failed, FIFO underrun	0
failed, carrier sense err	0	SQE test error	0
late collision	0	internal MAC trans errors	0

RISC Microcode Revision 1

+network 0 **3**

ETH>?

COLLISIONS

EXIT

ETH>**collisions** **4**

Transmitted with 1 collisions:	0
Transmitted with 2 collisions:	0
Transmitted with 3 collisions:	0
Transmitted with 4 collisions:	0
Transmitted with 5 collisions:	0
Transmitted with 6 collisions:	0
Transmitted with 7 collisions:	0
Transmitted with 8 collisions:	0
Transmitted with 9 collisions:	0
Transmitted with 10 collisions:	0
Transmitted with 11 collisions:	0
Transmitted with 12 collisions:	0
Transmitted with 13 collisions:	0
Transmitted with 14 collisions:	0
Transmitted with 15 collisions:	0

ETH>**exit**

+Ctrl+p

*

Figure 33. Ethernet Monitoring via the ASCII Console

3.3.2 Monitoring the Token-Ring Interface

In this section we describe the different commands to monitor the token-ring interface, and to find its universally administered address.

Monitoring can only be done via an ASCII console plugged in the IBM 2210 or via the Telnet session to the IBM 2210. References are to Figure 34 on page 77.

- Access CGW operator console **1**

The CGW operator console (also called CGWCON) is the Gateway Console process. It will allow you to monitor your IBM 2210.

For more information about the GWCON process, see 2.4.7, “GWCON Process” on page 35.

To access the CGW Operator Console, issue the Talk 5 command.

- Access the token-ring statistics **2**

This shows you the statistics for the token-ring interfaces. For example, it shows you the physical MAC address of the token-ring interface. This is the universally administered address of the token-ring interface, unless you have customized a locally administered address for the token-ring interface.

- Access token-ring monitoring **3**

To monitor the token-ring interface, issue the Network 0 command.

- The Dump command **4**

It shows you the RIF cache contents for each remote MAC address. See the RIF layout in Figure 28 on page 60.

Note

The SRT-STAT command is incorrectly listed in the *Nways MRNS Software User's Guide* documentation. This command is actually not available on the IBM 2210. It is a documentation error. See APAR II01165.

```

*talk 5 1

CGW Operator Console

+interface 0 2

Nt Nt' Interface      CSR  Vec      Self-Test  Self-Test  Maintenance
0  0  TKR/0          6000000  1C      Passed     Failed     Failed
                                1         0         0

Token-Ring/802.5 MAC/data-link on IBM Token-Ring interface
Microcode version: 000VL00A1 (052594)

Physical address      08005AC60015
Network speed         4 Mbps
Max packet size (INFO) 2052
Handler state         Ring open
Interface Restarts    0

# times Signal lost   0    # times Beaconsing      0
Hard errors           0    Lobe wire faults          0
Auto-removal errors   0    Removes received          0
Ring recovery actions 0

Line errors           0    Burst errors              0
ARI/FCI errors        0    Inputs dropped            0
Frame copy errors     0    Token errors              0
Lost frames           0

+network 0 3
TKR>dump 4

MAC address  State      Usage  RIF
400000033350 ON_RING   No     02F0

TKR>exit
+Ctrl+p
*
```

Figure 34. Token-Ring Monitoring via the ASCII Console

3.4 Configuring Serial Interfaces

This section describes how to configure the serial interfaces. It includes a short description of the interface type and the required configuration steps.

The following serial interfaces are currently supported:

- The X.25 interface
- The frame relay interface
- The point-to-point interface
- The SDLC-relay interface
- The SDLC interface
- The V.25bis network interface

3.4.1 The X.25 Interface

This section describes the X.25 interface implementation. It includes the configuration steps and references a configuration scenario.

3.4.2 X.25 Implementation

3.4.2.1 Addressing

You must assign a unique X.121 network address to each interface. This address is used during call establishment and also used by the remote DTE for mapping the destination protocol address to the X.121 call addresses. The mapping of the protocol to the X.121 call address is static and is configured on a per protocol and a per network interface basis. The exception is defense data network (DDN) addresses. The so-called IP HostTableFormat (IP HTF) addresses used in DDN can be dynamically translated into X.121 addresses.

You must map the destination protocol address to the destination DTE address.

The Call User Data (CUD) field is only used when you configure IPX as a routing protocol. The CUD field is used for IPX to X.25 address mapping and can either be standard or Proteon proprietary. Standard indicates that the usage is protocol multiplexing used in RFC 1356. Proteon proprietary indicates compatibility with other Proteon routers specifying this.

3.4.2.2 Virtual Circuits and Protocols

When configuring virtual circuits and protocols:

- Assign the used protocols on the router's X.25 interface together with the SVC parameters: window size, default packet size, maximum packet size, circuit idle time and the maximum number of SVCs that are open to a given destination for a protocol.
- For PVC, assign the corresponding protocol, window size and packet size.
- A router interface can support any combination of PVCs and SVCs (up to a maximum of 239).
- The range of defined PVCs must not overlap the defined range of SVCs.
- Virtual circuit numbers can be defined between 1 and 4095.
- Define the high and low SVC numbers required. Refer to Table 24 for a list of default SVC numbers.

Table 24. Default SVC Numbers		
SVC type	Low	High
Inbound	0	0
Two-way	1	64
Outbound	0	0

- Define the range of PVCs; defaults for low and high are 0.

3.4.2.3 National Personality

When you use an ASCII console, the setup uses sets of predefined parameter settings for typical X.25 network providers. Such a set defines 28 default parameters for each public data network defined by the Nways MRNS and is called a national personality.

3.4.2.4 X.25 Enhancements with MRNS Version 1.2

Maximum Transmit Unit (MTU) is now configurable in the range 576 to 4096 with the X.25 Config-Set MTU command. The MTU size defaults to 1500. T1/T2 timers have increased granularity. They were configurable in integral seconds and are now configurable in hundredths (T1=1.00 to 255.99, default 4.00 and T2=0.00 to 255.99, default 2.00). With this improvement, constant drop lines are avoided. In this version there is a set that describes the characteristic of GTE's Telenet and another set which describes the DDN network. If you want to change this or if your X.25 public data network is not one of the above, you need to review the 28 settings and specify them according to your needs. The settings can be changed using the commands:

```
X.25 config>national enable/disable...
```

```
X.25 config>national set...
```

Parameters that are not influenced by a national personality can be changed using the following commands:

```
X.25 config>Enable/Disable...
```

```
X.25 config>Set...
```

However, the 28 predefined default settings concerning the national personality of both GTE Telenet and DDN differ only on one parameter: Request reverse charging. The Nways MRS Configuration Program uses the defaults of the GTE Telenet national personality. Refer to 3.4.3, "Configuring X.25" for details.

3.4.2.5 X.25 Interface Support

The following applies to the IBM 2210 X.25 interface support:

- It is supported on RS-232, V.35, V.36 and X.21.
- It supports internal as well as external clocking. When using internal clocking, a DCE cable allows you to connect your IBM 2210 directly to another DTE.

3.4.3 Configuring X.25

To configure X.25 on the IBM 2210, you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRNS.

3.4.4 X.25 Configuration Commands

This section summarizes the X.25 configuration commands available within the CONFIG process of the Nways MRNS. To access the commands, issue the following command:

```
Config>network #
```

where # is the interface number for which you defined X.25. Table 25 on page 80 shows the commands available. *The Nways MRNS Software User's Guide* covers these commands in detail. This section also includes five additional tables that show an overview of the commands together with their

defaults and a reference to the subpanel name of the Device Interfaces panel for X.25 of the Nways MRS Configuration Program.

- For the Add command, refer to Table 26.
- For the Enable/Disable command, refer to Table 27.
- For the National Enable/Disable command, refer to Table 28 on page 81.
- For the National Set command, refer to Table 29 on page 81.
- For the Set command, refer to Table 30 on page 82.

Table 25. X.25 Configuration Commands

Command	Function
? (Help)	Lists the interface configuration commands, or lists the options associated with specific commands.
Add	Adds an address translation, a protocol encapsulation, or a PVC definition.
Change	Changes an address translation, a protocol encapsulation, or a PVC definition.
Delete	Deletes an address translation, a protocol encapsulation, or a PVC definition.
Disable	Disables interface-resets, incoming-calls-barred, outgoing-calls-barred, or dynamic DDN address translations.
Enable	Enables interface-resets, incoming-calls-barred, outgoing-calls-barred, or dynamic DDN address translations.
List	Displays the defined address translations, national personality parameters, protocol encapsulation, or PVC definitions.
National Disable	Disables the features defined by the national personality configuration.
National Enable	Enables the features defined by the national personality configuration.
National Restore	Restores the national personality configuration to its default values.
National Set	Sets parameters defined by the national personality configuration.
Set	Refer to Table 30 on page 82 for a list of all set commands.
Exit	Exits the X.25 configuration environment and returns to the CONFIG environment.

Table 26. Add... Defaults and Configuration Program Reference

Command	Default	Configuration Program Subpanel
Add Address	none	mappings
Add Htf-Address	N/A	<i>not implemented</i>
Add Protocol	none	X.25 per protocol configuration panel
Add PVC	none	performance

Table 27 (Page 1 of 2). Enable/Disable... Defaults and Configuration Program Reference

Command	Default	Configuration Program Subpanel
DDN-Address-Translations	disabled	performance
Interface-Resets	enabled	allow
Incomming-Calls-Barred	disabled	allow

<i>Table 27 (Page 2 of 2). Enable/Disable... Defaults and Configuration Program Reference</i>		
Command	Default	Configuration Program Subpanel
Outgoing-Calls-Barred	disabled	allow

<i>Table 28. National Enable/Disable... Defaults and Configuration Program Reference</i>		
Command	Default	Configuration Program Subpanel
Accept-reverse-charges	enabled 1	charges
CCitt	enabled	standard
Clear-w/diag	enabled	diagnostics
Flow-control negotiation	enabled	performance
Frame-ext-seq-mode	disabled	allow
Multi-link-addresses	disabled	allow
OSI-84	enabled	standard
OSI-88	disabled	standard
Packet-ext-seq-mode	disabled	allow
Packet-layer-restarts	enabled	allow
Request-reverse-charge	enabled 2	charges
Reset-w/diag	enabled	charges
Restart-w/diag	enabled	charges
Suppress-calling-addresses	enabled	allow
Suppress-idle-fram-rr	enabled	allow
Suppress-non-zero-cause	disabled	allow
Throughput-class-negotiation	enabled	performance

Notes:

1 Accept-reverse-charges is not applicable to DDN.

2 Request-reverse-charges is disabled by default for DDN.

<i>Table 29 (Page 1 of 2). National Set... Defaults and Configuration Program Reference</i>		
Command	Default	Configuration Program Subpanel
Call-req	20	timers
Clear-req	18	timers
Disconnect-procedure	passive	timers
Dp-timer	500	timers
Frame-window-size	7	packet size
Network-type	CCITT/DDN 1	standard
N2-timeouts	20	timers
Packet-size	128,256,7 2	packet size
Reset	18	timer

Table 29 (Page 2 of 2). National Set... Defaults and Configuration Program Reference		
Command	Default	Configuration Program Subpanel
Restart	18	timer
Standard-version	1984	standard
T1-timer	4 3	timers
T2-timers	2 3	timers

Notes:

- 1** For GTE Telenet, the default is CCITT and for DDN, the default is DDN.
- 2** The values represent default packet size, maximum packet size and packet window size.
- 3** The value of these timers are the defaults, but in Version 1 Release 2 it is possible to define other values.

Table 30. Set... Defaults and Configuration Program Reference		
Command	Default	Configuration Program subpanel
Address	none	node CONFIG
Cable		general
Calls-Out	4	node CONFIG
Clocking	external	general
Default-Window-Size	2	node CONFIG
Equipment Type	DTE	node CONFIG
HTF Addr	none	not implemented
Inter-Frame-Delay	0	general (transmit delay)
MTU	576 to 4096 1	size
National-Personality	GTE-Telenet	not implemented
PVC Low/High	0/0	not implemented
Speed	0	general (clock speed)
SVC Low/High	2	node CONFIG
Throughput-Class Inbound/Outbound	2400/2400	packet size
VC-Idle	30	node CONFIG

Notes:

- 1** Default size, but in Version 1 Release 2 it is possible to set up.
- 2** Refer to Table 24 on page 78 for a list of default SVC values.

3.4.5 X.25 Configuration Steps

For an example of how to configure X.25, refer to 9.6.1, “Scenario 12: Routing IPX over X.25” on page 418 or 4.4.8, “Scenario 8: IP Tunnel Bridge Implementation via X.25 Network” on page 247.

To configure X.25, use the following steps:

- Change the data link protocol for the corresponding serial interface to X.25. This can be done on the Device Interfaces panel of the Devices directory or by using the console command:

Config>**set data-link X25**

- Set equipment and cable type. Either use the Node CONFIG panel or the following console command:

X.25 config>**set equipment** or

X.25 config>**set cable**

- Set the local X.25 address. Either use the Node CONFIG subpanel or the console command:

X.25 config>**add address**

- Define the routed protocols. Either use the X.25 Per Protocol Configuration panel on the Device directory or the console command:

X.25 config>**add protocol**

- Define the SVC and PVC ranges. For SVCs use the Node CONFIG subpanel or the console command:

X.25 config>**set svc high/low...**

For PVCs you can only set the range using the console command:

X.25 config>**set pvc high/low**

- Add PVCs. Use either the PVC subpanel or the console command:

X.25 config>**add pvc**

Note

The PVC subpanel label is not visible until you click on the small arrow at the right bottom side of the label listing.

- Additionally, set your X.25 parameters according to your needs. Refer to 3.4.4, “X.25 Configuration Commands” on page 79 for details on defaults and Nways MRS Configuration Program equivalents.

3.4.6 Monitoring X.25

For an example of monitoring the X.25 interface, refer to 9.6.1, “Scenario 12: Routing IPX over X.25” on page 418.

There are two ways of looking at the X.25 interface. In both cases, access the GWCON console:

1. To get information about the physical interface such as modem leads and error counters use the command:

+interface #

Where # is the interface number for which you configured X.25.

2. To get information about the X.25 configuration use the command:

+network #

Where # is the interface number for which you configured X.25.

The commands listed in Table 31 are available. *The Nways MRNS Software User's Guide* covers these commands in detail.

Table 31. X.25 Monitoring Commands	
Command	Function
? (Help)	Displays all the X.25 monitoring commands or any options associated with a specific command.
List PVCs	Displays the configured permanent virtual circuits.
List SVCs	Displays the active switched virtual circuits.
Parameters	Displays the parameters for the packet, frame or physical levels of the X.25 configuration.
Statistics	Displays the statistics for the packet, frame or physical levels of the X.25 configuration.
Exit	Exits the X.25 console process and returns to the GWCON environment.

3.4.7 The Frame Relay Interface

This section describes how to configure frame relay on the IBM 2210. It includes a brief overview of frame relay terms and their implementation. It describes the configuration steps and includes a reference to a scenario.

3.4.7.1 Frame Relay Terminology and Implementation

Frame relay is a communications protocol similar to packet switching. Every frame, which may be of variable length, contains addressing information. The frames are forwarded to the frame relay network, which attempts to deliver them to the required destination. Frame relay is different from packet switching because it operates at layer 2 of the OSI reference model, whereas packet switching operates at layer 3.

Frame Relay implements all its required protocol functions within layer 2. Those required functions, also referred to as core functions, are:

- Examine the frame check sequence (FCS) of a frame and discard the frame if there have been errors.
- Route the frame to the appropriate link based on the Frame Address field.
- Check for congestion of the frame relay switch and either set congestion notification bits in the Address field of a frame or discard the frame.

The Addressing information in the Address field of a frame has only local significance; there is no network address. Current frame relay networks only support a permanent connection between two end users, and are referred to as a permanent virtual circuit (PVC). A PVC will be established when the network starts up and will be permanently available until the network itself shuts down. In the Address field the PVC number is identified by data link connection identifier (DLCI).

To manage the PVCs, a set of procedures and messages has been described. It is called the local management interface (LMI) and controls the connection between the user and the network. The LMI is responsible for:

- Ensuring the link between the user and the network is active
- Notifying the addition and deletion of PVCs
- Delivering status messages regarding the availability of the circuits

To be able to control the interface, a separate virtual circuit is used. The circuit number (management circuit number) is dependent on the LMI-type being used. The LMI-type being used is dependent on the frame relay network provider. Supported types are Rev1, ANSI (Annex D) and CCITT (Annex A).

If you enable orphan circuits for IBM 2210 (which is the default), the available PVCs on the interface are automatically added to your configuration. Otherwise, you need to add PVCs manually.

The IBM 2210 will try to find the protocol address of the other side using InARP. If the device or protocol at the other end does not support InARP on the frame relay interface you need to add protocol addresses to add static protocol and address mapping. This would be necessary, for example, if you want to route IPX over frame relay.

Committed Information Rate: For each DLCI, a committed information rate (CIR) may be assigned. This is the data rate that the user can expect to have into the network. A user can, however, exceed this rate if there is capacity available on the physical connection. The network, however, has the right to discard any frame in case of congestion due to this so-called burst traffic. To differentiate which frames will be discarded, it is possible to mark a frame discard eligible. It is vendor-dependent to decide which frames are being marked. For example, all frames that exceed the CIR could be marked, which may resolve the congestion problem experienced at that time. Public frame relay networks may give some kind of guarantee of data delivery when you stay within your CIR. The IBM 2210 implements the circuit monitoring feature that, when enabled, maintains the transmission rate at the CIR as it was defined.

Congestion Monitoring: Congestion monitoring is an optional feature, set per interface, that allows the 2210 to vary in response to network congestion. Congestion monitoring is enabled by default. It can be disabled with the `disable congestion-monitor` configuration command. When congestion occurs, the frame relay network is responsible for notifying the sender and receiver by sending out FECN or a BECN signal. BECN is set if messages sent by the router will encounter congestion condition, and FECN is set if messages received by the router encountered congestion along the way. When the router receives a frame containing BECN, it is the router's responsibility to throttle down the PVC's variable information rate if congestion monitoring is enabled.

3.4.8 Configuring Frame Relay

To configure frame relay on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRNS.

3.4.8.1 Frame Relay Configuration Commands

This section summarizes the frame relay configuration commands available within the CONFIG process of the Nways MRNS. To access the commands, issue:

Config>**network #**

where # is the interface number for which you defined frame relay. Table 32 shows the commands available. *The Nways MRNS Software User's Guide* covers these commands in detail.

Table 32. Frame Relay Configuration Commands

Command	Function
? (Help)	Lists the configuration commands, or lists any parameters associated with specific commands.
Add	Adds PVCs and destination protocol addresses to the frame relay interface.
Change	Modifies a previously defined PVC.
Disable	Disables any enabled frame relay feature.
Enable	Enables frame relay features such as circuit monitoring, management options, multicast, protocol broadcast and orphans.
List	Displays the current configuration of the LMI and PVCs.
Remove	Deletes any previously added PVCs or protocol addresses.
Set	Configures the properties associated with frame relay parameters (cir-adjustment, frame-size, line-speed, N1 parameter, N2 parameter, N3 parameter, P1 parameter and T1 parameter).
Exit	Exits the frame relay configuration environment and returns to the CONFIG environment.

3.4.9 Frame Relay Configuration Steps

To configure frame relay, use the following steps:

1. Change the data link protocol for the corresponding serial interface to frame relay. This can be done on the Device Interfaces panel of the Devices directory or by using the console command:

Config>**set data-link frame-relay**

2. Select the desired LMI-type; its default is enabled and set to LMI-Rev1. To change it using the configuration program, use the LMI subpanel of the Device Interfaces panel or use the following console commands:

FR config>**set lmi-type**

FR config>**enable/disable lmi**

3. Additionally, you may need to add one or more PVCs. This depends on whether you disabled LMI or disabled orphan circuits. To add PVCs use the PVC subpanel of the Device Interfaces panel or use the console command:

FR config>**add pvc**

When adding a PVC, you can set the CIR and optionally you can assign a name to each circuit.

4. Configure (depending on the protocol) the frame relay destination address(es). Use the Protocol subpanel on the Device Interfaces panel or use the console command:

FR config>**add protocol**

5. Additional features. The features can be enabled/disabled on the LMI subpanel of the Device Interfaces panel or by using console commands:

To set the CIR monitoring feature:

FR config>**enable/disable cir-monitor**

To set multicast emulation on each PVC:

FR config>**enable/disable multicast-emulation**

To set the usage of non-configured PVCs:

FR config>**enable/disable orphan-circuits**

To set the usage of protocol broadcasts on the interface:

FR config>**enable/disable protocol-broadcast**

For more information about frame relay and OSPF, refer to 8.1.4.1, “OSPF and Non-Broadcast Networks” on page 333.

3.4.10 Monitoring Frame Relay

There are two ways of looking at the frame relay interface. In both cases, access the GWCON console:

1. To get information about the physical interface such as modem leads and error counters use the command:

+interface #

2. To get information about the frame relay configuration, use the command:

+network #

where # is the interface number for which you configured frame relay.

The commands listed in Table 33 are available. *The Nways MRNS Software User's Guide* covers these commands in detail.

Table 33. Frame Relay Monitoring Commands	
Command	Function
? (Help)	Displays all the frame relay monitoring commands or any options associated with a specific command.
Clear	Clears statistical information on the frame relay interface.
List All	Displays circuit, management and PVC statistics on the frame relay interface.
List Circuit	Displays detailed PVC configuration and statistical information for a specific PVC.
List LMI	Displays statistics relevant to the logical management on the frame relay interface.
List Permanent-Virtual-Circuit	Displays general link layer statistics and configuration information for all configured PVCs on the frame relay interface.
Exit	Exits the frame relay console process and returns to the GWCON environment.

3.4.10.1 Frame Relay Interoperability with the IBM 6611 Network Processor

Besides LMI-types *REV1* and *ANSI*, the 6611 also supports an LMI type of *NONE*. This is effectively the same as defining all the PVCs available on the interface to the 2210.

3.4.11 The Point-to-Point Interface

This section describes how to configure a PPP interface and contains references to configuration scenarios. Its characteristics are:

- PPP is supported on RS-232, V.35, V.36, X.21 and V.25bis.
- The default encoding type is NRZ.
- It supports internal clocking as well as external clocking. When using internal clocking, a DCE cable allows you to connect your IBM 2210 directly to another DTE.

3.4.12 Configuring PPP

To configure PPP on the IBM 2210, you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRNS.

3.4.12.1 PPP Configuration Commands

This section summarizes the PPP configuration commands available within the CONFIG process of the Nways MRNS. To access the commands, issue the following:

Config>**network #**

where # is the interface number for which you defined PPP. Table 34 shows the commands available. *The Nways MRNS Software User's Guide* covers these commands in detail.

Table 34. Point-to-Point Configuration Commands	
Command	Function
? (Help)	Lists the point-to-point configuration commands, or lists any options associated with specific commands.
List	Lists all information related to the point-to-point interfaces protocols, parameters and options
Set	Set HDLC parameters, LCP options and parameters, IPCP options, BNCP options, and NCP parameters.
Exit	Exits the PPP configuration environment and returns to the CONFIG environment.

3.4.13 PPP Configuration Steps

To configure PPP, use the following steps:

1. Change the data link protocol for the corresponding serial interface to PPP. This can be done on the Device Interfaces panel of the Devices directory or by using the console command:

Config>**set data-link ppp**

2. Specify HDLC parameters such as cable, clocking and encoding. Either use the General subpanel of the Device Interface panel or use the command:

PPP config>**set hdlc...**

3. Optionally change the other PPP parameters such as BNCP, IPCP, LCP to your needs. Use one of the subpanels on the Device Interfaces panel or the console command:
PPP config>**set...**

3.4.14 Monitoring Point-to-Point

There are two ways of looking at the PPP interface. In both cases, access the GWCON console:

1. To get information about the physical interface such as modem leads and error counters use the command:

+interface #

where # is the interface number for which you defined PPP.

2. To get information about the PPP configuration, use the command:

+network #

where # is the interface number for which you defined PPP.

The commands listed in Table 35 are available. *The Nways MRS Software User's Guide* covers these commands in detail.

Table 35. Point-to-Point Monitoring Commands	
Command	Function
? (Help)	Displays all the point-to-point commands or lists subcommand options for a specific command.
Clear	Clears statistical information from point-to-point interfaces.
List	Displays information and counters related to the point-to-point interface and PPP parameters and options.
Exit	Exits the point-to-point console process and returns to the GWCON environment.

3.4.15 The SDLC Interface

This section describes the SDLC interface implementation. It contains the configuration steps and a reference to a configuration scenario.

3.4.15.1 SDLC Implementation

The SDLC traffic can only be forwarded using data link switching (DLSw) or advanced peer-to-peer networking (APPN). For more information, refer to Chapter 10, "Data Link Switching" on page 449. As for logical link control type 2 (LLC2), the SDLC data link (DLC) ends in the router. The router, therefore, implements an SDLC link station and acts as an SDLC endstation. Figure 35 on page 90 shows an SDLC session establishment and disconnection when using DLSw.

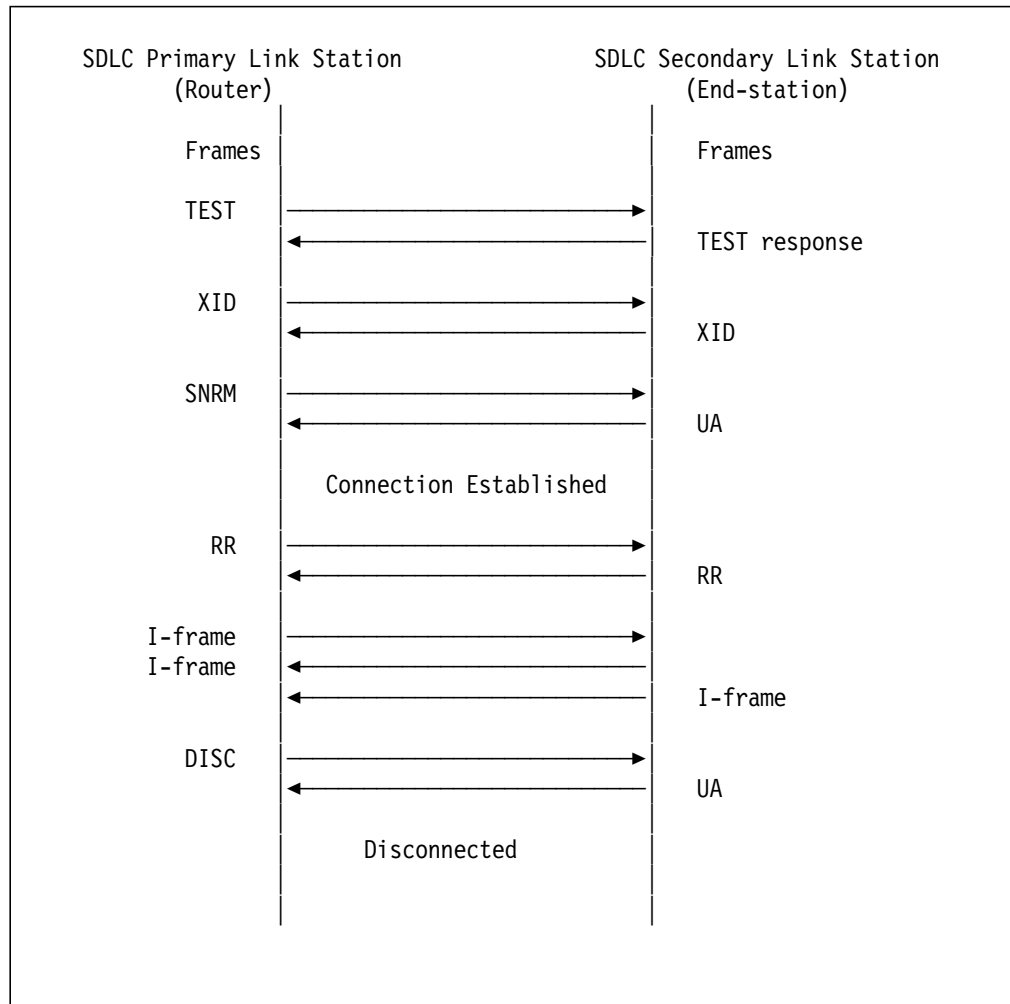


Figure 35. SDLC Session Establishment

A link between two nodes may require that one link station takes the role of *primary* link station and one link station takes the role of *secondary* link station. This role setting does not imply that the link stations maintain a *master slave*.

Link roles are coordinated at link activation time. The link station roles must either be predefined or negotiated during link activation. Predefinition of link station roles requires that the definitions at both ends match. If both nodes define the local link station as primary or both define the local link station as secondary, link activation will fail. Defining a link station as *negotiable* means that the link station role can be either primary or secondary and that the actual role will be determined during link activation. If both ends are defined as negotiable, the final roles are decided on the basis of node identification fields exchanged between the two link stations, during link activation.

Within SDLC, only the primary station can establish a connection. The router (primary) will send an SDLC TEST frame when it receives a CANUREACH frame from one of its DLSw session partners. The secondary station cannot transmit data unless polled by the primary. The SDLC link will be connected to DLSw after the UA is received. The router will then only transmit the I-frames across the (IP) network. This technique is called spoofing.

The SDLC link is seen from the host as a switched resource. Therefore, you must have a switched major node definition for every SDLC link station.

Nways MRNS V1R3 only supports the attachment of secondary SDLC stations because the 2210 could only assume a primary link station role. With Nways MRS V1R1, the 2210 can be either a primary or secondary SDLC link station, based on the configuration, or based on SNA XID negotiation. When you use an SDLC link, as said before, you may need DLSw. Within DLSw, you need to add the SDLC devices to the DLSw configuration.

PU Type Support: In the primary role, the IBM 2210 supports multiple SDLC devices of differing PU types on the same physical multipoint SDLC line. In that case, you need to set the link to multipoint. IBM 2210 supports PU types 2.0, 2.1, 4, and 4/5.

When adding a PU T2.0 device, IBM 2210 requests that you provide a source MAC address, an IDBLK and IDNUM and LLC Source SAP. The router will use this information to respond to XID frames coming from the host. When this device is allowed to initiate the connection request, you also need to specify the LLC destination SAP and the destination MAC address. In that case, the 2210 will send a CANUREACH to its DLSw partners for the specified destination MAC address.

The following values should match for PU Type 2.0:

- The source MAC address needs to match the DIALNO keyword on the PATH statement in the VTAM switched major node.
- The IDBLK needs to match the IDBLK keyword on the PU statement in the VTAM switched major node.
- The IDNUM needs to match the IDNUM keyword on the PU statement in the VTAM switched major node.
- The LLC source SAP identifies the PU link station to DLSw; it should match the DIALNO keyword on the PATH statement in the VTAM switched major node. You can, however, set it to auto-assign if you specified a multidrop SDLC line.
- Running in active mode, the destination MAC address needs to match the MAC address of your destination and the LLC destination SAP must be 04.

Running in passive mode, the LLC destination SAP must be 0.

When you add a PU T2.1, you need to set the *link role* to *secondary* or *negotiable* on the router. From this information, the router determines that the device type is a PU T2.1. Because the router always wants to be primary, you need to force the attached SDLC link station to *secondary*. In the case of PU T2.1, the values for IDNUM and IDBLK will be ignored and the XID3 frames will be forwarded to the SDLC link station to establish the SNA logical link with the partner node.

The new SDLC software supports the IBM 3174 group poll function for SDLC secondary station. It's configured by issuing the following:

```
SDLC 2>set station(name) group-inclusion yes
```

```
SDLC 2>set link group-poll (address in hex) (frame size)
```

You can test the SDLC connectivity from the router to the link station with the Test command. This can be useful, because the router does not respond to test

frames received from the local SDLC station until its destination is reachable by DLSw. This command allows you to send a specific amount of SDLC Test-frames with a specified length and waits for the response. This is a monitoring command and can only be issued for disabled lines.

SDLC 2>**disable station ...**

SDLC 2>**test station...**

After this command, you will be prompted for the *number of frames* and *frame length*.

3.4.16 Configuring SDLC

To configure SDLC on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRS.

The monitoring function allows you to dynamically change SDLC resources. The link for which you want to make the changes must be disabled.

3.4.16.1 SDLC Configuration Commands

This section summarizes the SDLC configuration commands available within the CONFIG process of the Nways MRS. To access the commands, issue the following command:

Config>**network #**

where # is the interface number for which you defined SDLC. Table 36 shows the commands available. The *Nways MRS Software User's Guide* covers these commands in detail.

Table 36. SDLC Configuration Commands	
Command	Function
? (Help)	Lists the SDLC configuration commands, or lists any parameters associated with specific commands.
Add	Adds an SDLC endstation.
Delete	Removes an SDLC end link station.
Disable	Prevents connections to one of the SDLC link stations.
Enable	Allows connections to one of the SDLC link stations.
List	Displays configured information for one of the SDLC link stations.
Set	Configures specific interface and link station information.
Exit	Exits the SDLC configuration environment and returns to the CONFIG environment.

3.4.17 SDLC Configuration Steps

To configure SDLC, use the following steps:

- Change the *data link protocol* for the corresponding serial interface to SDLC. This can be done on the Device Interfaces panel of the Devices directory or by using the following console command:

SDLC 2 Config>**set data-link sdlc**

- Set the *general link* requirements, such as link encoding, link cable type, and link clocking. Use the General subpanel or the console command:

Config>**set link...**

- Set the *detailed link* parameters such as link role, link type etc. Use the Detail subpanel or the the console command:

SDLC 2 Config>**set link...**

- Add one or more SDLC end link stations. For each link station you can define the station address, station name, maximum packet size and receive and transmit window sizes. Use either the Remote panel or the following console command:

SDLC 2 Config>**add remote-secondary**

Note: The router is by default the primary endstation, if you do not use this command and if you configured an SDLC station in DLSw or in APPN, the endstation is added for you.

- Especially in case of multipoint connections, it might be necessary to change the polling values of the link. To do this, use either the Polling panel or the following console command:

SDLC 2 Config>**set link poll...**

- Finally, you need to configure SDLC in the DLSw or APPN protocol. Only one protocol at a time, DLSw or APPN, may run over a given SDLC interface. The first protocol to become active will own the SDLC interface.

3.4.18 Monitoring SDLC

There are two ways of looking at the SDLC interface. In both cases, access the GWCON console:

1. To get information about the physical interface such as modem leads and error counters use the following command:

+interface #

where # is the number of the corresponding SDLC interface.

2. To get information about the SDLC configuration, and to dynamically change the SDLC link station configuration, use the following command:

+network #

where # is the number of the corresponding SDLC interface.

The commands listed in Table 37 are available from the console. The *Nways MRS Software User's Guide* covers these commands in detail.

Table 37 (Page 1 of 2). SDLC Monitoring Commands	
Command	Function
? (Help)	Displays all the SDLC monitoring commands or any options for a specific command.
Add	Adds an SDLC station.
Clear	Clears the counters on the SDLC interface.
Delete	Dynamically removes an SDLC link station.
Disable	Disables connections to one SDLC link station.
Enable	Enables connections to one SDLC link station.
List	Displays statistics on one or all SDLC link stations.
Set	Configures specific interface and link station information.

Table 37 (Page 2 of 2). SDLC Monitoring Commands

Command	Function
Test	Tests the link between the router and the SDLC link station.
Exit	Exits the SDLC monitoring process and returns to the GWCON environment.

3.4.19 The SDLC Relay Interface

This section describes the SDLC Relay interface implementation and the required configuration steps. There is no configuration scenario in this book on this item.

3.4.19.1 SDLC Relay Implementation

SDLC Relay uses the IP encapsulation technique to connect two disjointed SDLC links. It encapsulates all the SDLC frames into IP and transfers it through the IP network to a specified IP destination. This destination router removes the IP information and forwards the SDLC frame onto its attached SDLC link. The implementation implies that the receive ready (RR) frames will also cross the IP network and as such do not have the advantage of DLSw, which locally acknowledges these frames. This means that with relay implementation, session timeout situations may occur because of delays in your IP network. SDLC Data and control frames pass transparently through SDLC Relay, while DLSw needs to interpret and modify some of them. Along with the fact that DLSw terminates the SDLC connection (for example, multilink TGs between NCPs) the relay function is not supported over DLSw. That's one reason for implementing SDLC relay instead of SDLC.

3.4.20 Configuring SDLC Relay

SDLC Relay is implemented as a protocol. You need to configure the SDLC Relay interface separately.

Note

You cannot configure SDLC Relay using the Nways MRS Configuration Program.

3.4.20.1 SDLC Relay Configuration Commands

This section summarizes the SDLC Relay configuration commands available within the CONFIG process of the Nways MRS and consists of the following two parts:

- The interface configuration
- The protocol configuration

The SDLC Relay Link Configuration Commands: To access these commands, issue the following command:

```
Config>network #
```

where # is the interface number for which you defined SDLC Relay. Table 38 on page 95 shows the commands available. The *Nways MRS Software User's Guide* covers these commands in detail.

Table 38. SDLC Relay Link Configuration Commands	
Command	Function
? (Help)	Lists the SDLC Relay configuration commands for the link, or lists the options associated with that command.
List	Displays the link configuration.
Set	Sets the link parameters and remote station parameters.
Exit	Exits SDLC Relay link configuration environment and returns to the CONFIG environment.

SDLC Relay Protocol Configuration Commands: This section summarizes the SDLC Relay protocol configuration commands available within the CONFIG process of the Nways MRS. To access the commands, issue the following command:

Config>**Protocol sdlc**

which brings you to the following prompt:

SDLC Config>

Table 39 shows the commands available.

Table 39. SDLC Relay Protocol Configuration Commands	
Command	Function
? (Help)	Lists the SDLC Relay protocol configuration commands, or lists the options associated with that command.
Add	Adds groups, local ports, and remote ports.
Delete	Deletes groups, local ports, and remote ports.
Disable	Disables groups and ports.
Enable	Enables groups and ports.
List	Displays SDLC Relay group and port configuration.
Exit	Exits the SDLC Relay protocol configuration environment and returns to the CONFIG environment.

3.4.21 SDLC Relay Configuration Steps

This section describes the basic steps for configuring SDLC Relay. Note that to use SDLC Relay you should have defined an IP network.

- Define the SDLC Relay link. Change the *data link protocol* for the corresponding serial interface to SDLC Relay. Use the following console command:

Config>**set data-link srlly**

- Set the link parameters for the link station. These parameters include encoding, cable type, clocking, speed, frame size, etc. Use the following console command:

SRLY Config>**set...**

- Define the SDLC endpoints of your IP network. This is done from the SDLC Protocol configuration console. To access this, use the following command:

Config>**protocol sdlc**

To define the IP endpoints, you need to define a group, which is represented by a number and, subsequently, you add a local port and a remote port to this group. The local port must match your SLDC Relay interface number and the remote port must match the IP address of the destination router. Use the following console commands to accomplish this:

```
SRLY Config>add group
SRLY Config>add local-port
SRLY Config>add remote-port
```

3.4.22 Monitoring SDLC Relay

There are two ways of looking at the SDLC Relay configuration. In both cases access the GWCON console.

1. To get information about the SDLC Relay interface such as modem leads and error counters, use the following command:

+interface #

where # is the interface number of the V.25bis interface.

2. To get information about the SDLC Relay configuration and statistics use the following command:

+protocol sdlc

The commands listed in Table 40 are available. *The Nways MRS Software User's Guide* covers these commands in detail.

Table 40. SDLC Relay Monitoring Commands

Command	Function
? (Help)	Displays all the SDLC Relay monitoring commands or lists the options associated with a specific command.
Clear-port-statistics	Clears SDLC Relay statistics for a specified port.
Disable	Temporarily suppresses groups and ports.
Enable	Temporarily turns on groups and and ports.
List	Displays entire SDLC Relay and group-specific configurations.
Exit	Exits the SDLC Relay monitoring process and returns to the GWCON environment.

3.4.23 The V.25bis Network Interface

This section describes the V.25bis interface implementation. It includes the configuration steps and references to scenarios using the V.25bis interface (WAN Restoral and Dial on Demand).

3.4.23.1 V.25bis Implementation and Terminology

The V.25bis interface allows routers to establish serial connections over switched telephone lines using V.25bis modems. The V.25bis interface initiates and accepts switched circuit connections, either on demand, automatically from restart, or on command by the operator. This allows you to reduce communication costs because you only use resources required for specific needs. It also offers the flexibility of connecting to several destinations.

Each V.25bis interface consists of one serial line interface that is connected to a V.25bis modem and at the other end is connected to one or more dial circuits. The V.25bis interface operates as the data terminal equipment (DTE) and the modem operates as the data communications equipment (DCE).

Note

You can also use the V.25bis interface to connect a router to an integrated services digital network (ISDN) using a V.25bis-compliant ISDN Terminal Adapter. However, this is not tested in any of the scenarios in this book.

3.4.23.2 V.25bis Serial Line Interface

The V.25bis serial interface establishes connections with a peer router using the V.25bis modem. The serial line interface accepts or initiates connections on command from the dial circuit.

Routing protocols cannot communicate directly with a V.25bis serial line interface. These protocols should refer to the dial circuit and not to the V.25bis interface.

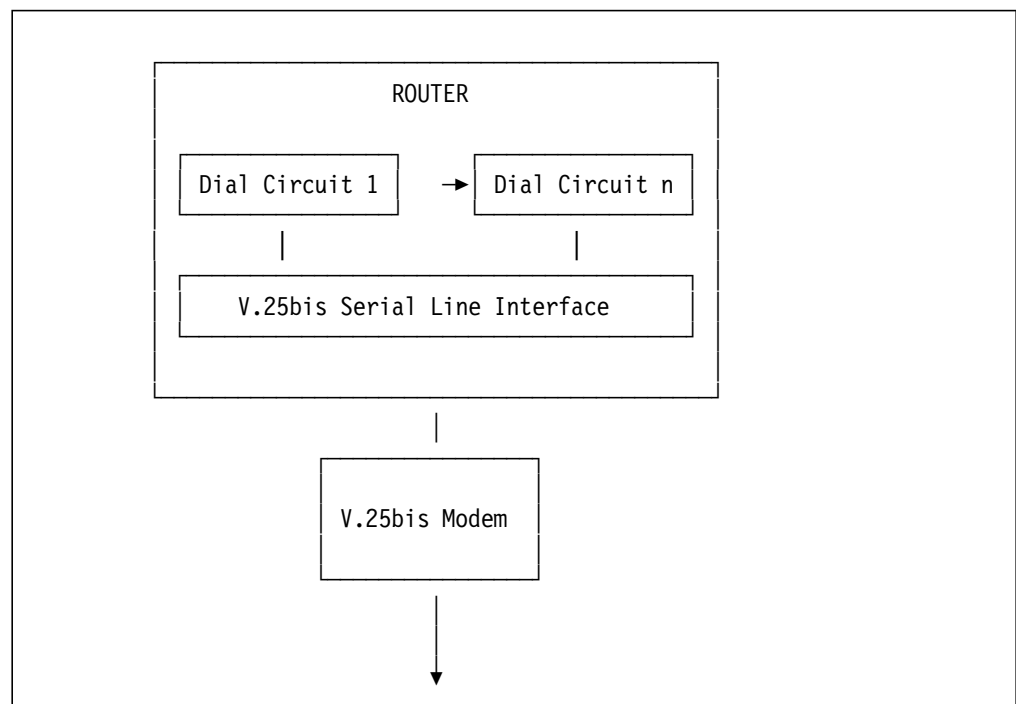


Figure 36. V.25bis Implementation

3.4.23.3 Dial Circuits

Dial circuits are a set of potential point-to-point network connections that are mapped to V.25bis serial line interfaces or ISDN Interfaces. For more information on ISDN interfaces see 3.5, “The ISDN Interface” on page 102. There are three types of dial circuits:

- Static circuits (or leased lines)
- Switched circuits that dial on demand and hang up after a specified idle time
- WAN Restoral circuits that are used only when a leased line fails

Figure 36 shows the relationship between a dial circuit and the serial line interface. You should add a dial circuit for each potential destination. You can map multiple dial circuits to one serial line interface. Each dial circuit appears as a normal serial line network running the PPP protocol. You can change the PPP settings for your dial circuit. This can only be done from the console with the following command:

Circuit config>**Encapsulator**

This gets you to the serial line configuration prompt:

SLC config>

Note

The Nways MRS Configuration Program does not provide the encapsulator function.

Be aware of the following when you make changes to the PPP parameters for a dial circuit:

- The V.25bis interface predefines clocking as external and encoding as NRZ. The DCE controls the clock speed. The V.25bis interface ignores those parameters in the PPP configuration.
- The V.25bis interface will not enforce transmit delay counters that you set in the PPP configuration.
- For WAN Restoral, the PPP parameters you define for this dial circuit must match the PPP parameters you defined for the interface that you want to back up (also known as primary interface).

On a dial circuit, you can set the *Idle timeout*. If there is no protocol traffic over the circuit for this period, the dial circuit hangs up. Setting this to zero specifies that there is no timeout period and that this is a dedicated circuit. For the WAN Restoral feature, you must set this to zero.

Additional features for a dial circuit are as follows:

- You can restrict a dial circuit to initiating *outbound calls* only, accepting *inbound calls* only, or both initiating and accepting calls.
- You can specify if you want an inbound call to match a *specific inbound destination name* or whether you accept *any inbound call*.

3.4.23.4 Addressing

To place a telephone call, specify the telephone number of the destination. To identify yourself to the destination, specify your own telephone number. For V.25bis, telephone numbers are called network *dial addresses* and, for convenience, they are given names called network *address names* that you can use to identify the telephone number.

When you set up a V.25bis serial line interface, you add addresses for each potential destination as well as for your own telephone number, which is called the *local network address*. When you configure a dial circuit, you set up the dial circuit with one of the destination addresses.

3.4.23.5 Circuit Contention

If one dial circuit is using the V.25bis circuit, other dial circuits will not be able to use it. The V.25bis device can only have one outstanding call at a time. Packets sent by protocols on dial circuits that cannot connect to the V.25bis interface will be dropped.

3.4.23.6 Call Verification

The V.25bis implementation uses a proprietary caller-ID protocol to match incoming calls to the specific dial circuits. The caller-ID protocol uses the inbound and outbound destination addresses in the dial circuit configuration to match the dial circuit that places the call to the dial circuit that receives the call. The caller-ID protocol is a brief identification protocol initiated by the caller and answered by the dial circuit that receives the call. If the caller does not provide the caller-ID message, the call may be rejected.

3.4.23.7 V.25bis Modem Requirements

You must have a V.25bis modem that supports the following circuits as outlined in the ITU/CCITT V.25bis 1988 specification:

- Circuit 106-Ready to Send (clear to send)
- Circuit 107-Data Set Ready
- Circuit 108/2-Data Terminal Ready
- Circuit 125-Calling (Ring) Indicator

Note

The V.25bis interface does not work with DCE (null modem) cables.

3.4.23.8 V.25bis Interface Restrictions

The following are some interface restrictions:

- You cannot boot the router over a V.25bis link.
- Bandwidth reservation is not supported on a V.25bis link.
- Because X.21 supports only two circuits, the V.25bis interface does not support X.21.
- This implementation of V.25bis supports addressed call mode (also known as circuit 108/2 mode) rather than direct call mode. Addressed call mode provides access to multiple remote destinations through one DCE.

3.4.23.9 V.25bis Interface Variables

The following variables are implemented:

- **Command Delay Timeout** After the router turns on data terminal ready (DTR), it waits this amount of time before it initiates or answers a call. If you set this parameter to 0, the router waits for the modem to respond to DTR with the clear to send (CSR) signal before it issues commands.
- **Connect Timeout** This is the number of seconds allowed for a call to be established. If you set this parameter to 0, the modem controls the connection timeout.
- **Disconnect Timeout** This specifies the amount of time the router waits after dropping DTR before it initiates further calls. If you set this parameter to 0,

the router waits for the modem to respond to the DTR drop by dropping CTS and data set ready (DSR) before it initiates the next call.

- **Retries-No-Answer** This specifies the maximum number of calls the router attempts to make to a non-responding address during the timeout period.
- **Timeout-No-Answer** After the router reaches the retries-no-answer value to a non-responding address, it stops further calls to that address until this time has expired.

3.4.23.10 Cost Control over Demand Circuits

Dial circuits always appear to be in the up state to the routing protocols. Most routing protocols send out periodic routing information that could cause the router to dial out each time the routing information is sent over *dial-on-demand* circuits. Therefore, you should configure IP to use only static routes and you should disable the routing protocols RIP and OSPF over the dial circuits. This prevents periodic routing updates. If you are using IPX, configure it for low-frequency updates and change update so that it sends broadcast messages only at specified times or when there is a problem.

3.4.24 Configuring V.25bis

When configuring V.25bis facilities or features, you need to configure:

- The telephone numbers and their associated names
- The physical V.25bis interface also known as serial line interface (SLI)
- The dial circuits

Refer to 11.10, “Dial-on-Demand” on page 683 for a description and scenario of configuring the dial-on-demand facility and refer to 11.5, “WAN Restoral (WRS)” on page 599 for a description and scenario of configuring dial-backup also known as the WAN Restoral feature. The following two sections show the configuration command overview for the V.25bis SLI and the dial circuit. The configuration steps are discussed in 3.4.25, “V.25bis Configuration Steps” on page 101.

3.4.24.1 V.25bis SLI Configuration Commands

This section summarizes the V.25bis configuration commands available within the CONFIG process of the Nways MRS. To access the commands, issue the following command:

Config>**network #**

where # is the interface number for which you defined V.25bis. Table 41 shows the commands available. *The Nways MRNS Software User's Guide* covers these commands in detail.

Table 41. V.25bis Configuration Commands	
Command	Function
? (Help)	Lists the V.25bis configuration commands, or lists the options associated with that command.
List	Displays the V.25bis configuration.
Set	Sets the local address, connect, disconnect, and no answer timeouts, number of retries after no answer, and command delay timeout.
Exit	Exits the V.25bis configuration environment and returns to the CONFIG environment.

3.4.24.2 V.25bis Dial Circuit Configuration Commands

This section summarizes the dial circuit configuration commands available within the CONFIG process of the Nways MRNS. To access the commands, issue the following command:

Config>**network #**

where # is the interface number for which you added a dial circuit. Table 42 shows the commands available. *The Nways MRNS Software User's Guide* covers these commands in detail.

Table 42. Dial Circuit Configuration Commands	
Command	Function
? (Help)	Lists the dial circuit configuration commands, or lists the options associated with that command.
Delete	Deletes the inbound call settings from the dial circuit configuration.
Encapsulator	Allows you to change the data-link protocol configuration.
List	Displays the dial circuit configuration parameters.
Set	Configures the dial circuit for inbound or outbound calls, maps the dial circuit to a serial line interface, and sets addresses, idle timeout and self-test delay.
Exit	Exits the dial circuit configuration environment and returns to the CONFIG environment.

3.4.25 V.25bis Configuration Steps

The following describes the basic steps for configuring the V.25bis-based features and facilities:

1. Define the Serial Line Interface. Change the *data-link protocol* for the corresponding serial interface to V.25bis. This can be done on the Device Interfaces panel of the Devices directory or by using the following console command:

Config>**set data-link v25bis**

2. Define address names and their corresponding telephone number for each local port (serial line interface) as well as for each destination port. Use either the V.25bis Addresses panel of the General directory, or the following console command:

Config>**add v25-bis-address**

3. Set the Serial Line Interface parameters such as the timer and retry values and the local address, using either the Device Interfaces panel of the Devices directory or the following console command:

V.25bis config>**set...**

4. Add the dial circuit(s). This can be done by using either the V.25bis Secondary Circuits panel of the General directory or the following console command:

config>**add device dial circuit**

5. Configure the dial circuit interface parameters. Use either the V.25bis Secondary Circuits panel of the General directory or one of the following console commands:

Circuit config>**set...**

Circuit config>encapsulator

3.4.26 Monitoring V.25bis and Dial Circuits

The following are the two ways of looking at the V.25bis interface. In both cases, access the GWCON console.

1. To get information about the V.25bis interface such as modem leads and error counters, use the following command:

+interface #

where # is the interface number of the V.25bis interface. You can use the same command to look at the dial circuit statistics; however, the # must match a dial circuit interface number.

2. To get information about the V.25bis and dial circuit configuration, use the following command:

+network #

where # is the interface number of the V.25bis interface.

The commands listed in Table 43 are available. The *Nways MRNS Software User's Guide* covers these commands in detail.

Table 43. V.25bis Monitoring Commands

Command	Function
? (Help)	Displays all the V.25bis monitoring commands or lists the options associated with a specific command.
Calls	Lists the number of completed and attempted connections made for each dial circuit mapped to this interface since the last time statistics were reset on the router.
Circuits	Shows the status of all data circuits configured on the V.25bis interface.
Parameters	Displays the current parameters for the V.25bis interface.
Statistics	Displays the current statistics for the V.25bis interface.
Exit	Exits the V.25bis Monitoring process and returns to the GWCON environment.

3.5 The ISDN Interface

Integrated Services Digital Network (ISDN) is now an internationally recognized standard. ISDN networks are now being deployed in the United States, Europe, and Asia.

This section describes how to configure the ISDN interface. It includes the following:

- Implementing the ISDN Interface
- ISDN Configuration Commands
- Configuration Steps
- Frame Relay over ISDN configuration

3.5.1 ISDN Driver Support

In Version 1 Release 1 of the IBM 2210 Nways MRS software program, ISDN is supported on the IBM 2210 Models 1Ux,1Sx,127,128 and x4x. The ISDN Basic Rate Interface (BRI) is supported on the Models 1Ux,1Sx,127 and 128. The ISDN Primary Rate Interface (PRI) is supported on the Models x4x.

The ISDN Basic Rate Interface (BRI) supports the following switches:

- AT&T 5ESS (United States)
- Northern Telecom DMS100 (United States)
- USNI1 (United States National ISDN1)
- USNI2 (United States National ISDN2)
- NET 3 (European ETSI)
- NTT INS64 (Japan)
- VN3 (France Telecom)
- AUS TS 013 (Australia)

The ISDN Primary Rate Interface (PRI) supports the following switches:

- AT&T 5ESS (United States)
- AT&T 4ESS (United States)
- Northern Telecom DMS250 (United States)
- USNI2 (United States National ISDN2)
- NET 5 (European ETSI)
- NTT INS1500 (Japan)
- AUS TS 014 (Australia)

3.5.2 ISDN Implementation

This section describes the characteristics of ISDN on the 2210.

3.5.2.1 Addressing

You must assign an ISDN address for each interface as well as for each destination. The ISDN address includes the following:

- Address Name

The address name is a description of the address. You can use any string of up to 23 printable ASCII characters.

- Network Dial Address

The dial address is the telephone number of the local or destination port. You can enter up to 15 numbers as well as 16 characters, including spaces and punctuation. The router uses only the numbers.

- Network Subdial Address (optional)

This is an additional part of a telephone number, such as an extension, that is interpreted once the interface connects to a PBX. You can enter up to 20 numbers, as well as additional spaces and punctuation. The router uses only the numbers.

3.5.2.2 Dial Circuits

Dial circuits are a set of potential point-to-point network connections that are mapped to ISDN interfaces or V.25bis serial interfaces. For more information on V.25bis, see 3.4.23, “The V.25bis Network Interface” on page 96.

The following are three types of dial circuits:

- Static circuits (or leased lines)
- Switched circuits that dial on demand and hang up after a specified idle time
- WAN Restoral circuits that are used only when a leased line fails

You should add a dial circuit for each potential destination. You can map multiple dial circuits to one serial line interface.

To add a dial circuit, enter the add device dial-circuit command at the Config> prompt. The software assigns an interface number to each circuit. You will use this number to configure each circuit. For example:

```
Config>add device dial-circuit
```

adding device as interface 4.

Beware of the following when you configure PPP for ISDN:

- The ISDN interface will not enforce transmit delay counters that you set in the PPP configurations.
- Do not enable psuedo-serial Ethernet on the dial circuit.

3.5.2.3 Dial Circuit Configuration Commands (ISDN)

This section summarizes and explains the dial circuit configuration command.

Table 44 summarizes the dial circuit configuration commands. Enter the dial circuit configuration commands at the Circuit Config> prompt. You must restart the router for configuration changes to take effect. The *Nways MRS Software User's Guide* covers these commands in detail.

To access the Circuit Config> prompt, enter the network command followed by the interface number of the dial circuit.

Note: The dial circuit was assigned when you entered the add device dial-circuit command. You can enter the list devices command at the Config> prompt to display a list of the dial circuits that you added.

Table 44. Dial Circuit Configuration Commands (ISDN)	
Command	Function
? (Help)	Lists the dial circuit configuration commands, or lists the options associated with that command.
Delete	Deletes the inbound call settings from the dial circuit configuration.
Encapsulator	Allows you to change the data-link protocol configuration.
List	Displays the dial circuit configuration parameters.
Set	Configures the dial circuit for inbound or outbound calls, maps the dial circuit to a serial line interface, and sets addresses, idle timeout and self-test delay.
Exit	Exits the dial circuit configuration environment and returns to the Config> prompt.

3.5.3 ISDN Configuration Commands

This section summarizes the ISDN configuration commands available within the CONFIG Process of the Nways MRS. To access the commands, you need to issue the following commands:

```
Config>network #
```

where # is the interface number of the ISDN interface. You can use the list devices command at the Config> prompt to display a list of interfaces configured on the router.

Table 45 summarizes the ISDN configuration commands. The *Nways MRS Software User's Guide* documentation covers these commands in detail.

Table 45. ISDN Configuration Commands	
Command	Function
? (Help)	Lists the configuration commands or lists the options associated with that command.
Add	Adds accounting entries to the ISDN configuration.
Disable	Valid only for BRI. Disables Power Source 1 detection.
Enable	Valid only for BRI. Enables Power Source 1 detection.
List	Displays the ISDN Configuration.
Remove	Removes accounting entries from the ISDN configuration.
Set	Sets the framesize, interface, local-address-name, multipoint-selection, retries-call-address, service-profile-id, timeout-call-address, type of ISDN switch, directory numbers(dn0, dn1), and TEI. Multipoint-selection, service-profile-id, timeout-call-address and TEI are only for BRI. Dn1 is only for PRI.
Cause_Code MGMT	Stops further processing attempts to establish a connection through an interface.
Exit	Exits the ISDN configuration process and returns to the Config> prompt.

3.5.4 ISDN Configuration Steps

To configure ISDN, use the following steps:

1. Configure the ISDN Interface (PRI Only) using the following commands

- To configure the T1/J1 PRI interface:

For example:

```
Config> set int lbo a
```

```
Config> set int code b8zs
```

```
Config> set int zbtsi disabled
```

```
Config> set int esf-data_link ansi-ti.403
```

- To configure the E1 PRI interface:

For example:

```
Config> set int code HDB3
```

```
Config> set int crc4 enabled
```

Note: For configuring the ISDN Interface (PRI), you should specify some parameters. The *Nways MRS Software User's Guide* documentation covers those parameters in detail.

2. Add an ISDN address for each interface and destination using the following command:
Config> **add isdn-address**
3. Access the ISDN Config> prompt with the following command:
Config> **network #**
where # is the ISDN interface number.
4. Set the switch type to be connected to this ISDN interface with the following command:
ISDN Config> **set switch**
5. Set the network address name of the local port with the following command:
ISDN
Config> **set local-address-name**
Note: You must use one of the address names you defined using the add isdn-address command.
6. If you set the switch-variant to NET3, VN3, DMS250 or AUS, set the directory number of the local port. Set the network dial address (telephone number) of the local port with the following command:
ISDN Config> **set dn0**
Note: You can only configure DN0 for a PRI.
7. Set the TEI (Terminal Endpoint Identifier) to match the TEI signal of your ISDN switch with the following command:
ISDN Config> **set tei**
If you are connected to a 5ESS or USNI1 switch, you must set the TEI for each B-channel. The set tei command prompts you for a B-channel number.
Note: TEI is not Configurable for PRI because TEI for PRI is always 0.
8. Set the ISDN interface to either point-to-point (pp) or multipoint (mp).
Point-to-point is one ISDN device on an ISDN line. Multipoint is two or more ISDN devices sharing an ISDN line. With some switch variants, you must configure the line as multipoint regardless of how many devices are on it. Check with your ISDN service provider.
ISDN Config> **set multi-point-selection**
Multipoint Selection [MP]? **pp**
Note: You can only configure point-to-point for a PRI.
9. If you are connected to a U.S. switch variant, your service provider may require a Service Profile ID (SPID).
The SPID is a number up to 20 digits long that uniquely identifies the ISDN device. Your ISDN service provider assigns SPIDs as follows:
Config> **set spid**
Enter BChannel Number [1]? **1**
Enter Service Profile ID (SPID) []? **123**
10. Set the frame size so that it is greater than or equal to the frame size of the data-link protocol (PPP) running on the link with the following command:
Config> **set framesize**
11. Add a dial circuit or multiple dial circuits at the Config> prompt with the following command:

Config> **add device dial-circuit**

12. Change the dial circuit protocol to PPP with the following command:

Config> **set data-link ppp**

13. Enter the circuit configuration with the following command:

Config> **network #**

where # is the interface number of the dial circuit.

14. Map the dial circuit to and ISDN interface with the following command:

Circuit Config> **set net**

15. Specify the address name of the remote (destination) router to which the dial circuit will connect with the following command:

Circuit Config> **set destination**

16. Configure the dial circuit calling status (initiate calls, accept calls, or both) with the following command:

Circuit Config> **set calls**

To avoid a conflict if both ends of the link attempt to establish a call at the same time, configure one end to accept inbound calls only and the other end of the link to initiate outbound calls only.

Note: For WAN Restoral operations or another dial-on-demand application, you should set up the circuit for both inbound and outbound calls.

17. Specify the timeout period for the circuit with the following command:

Circuit Config> **set idle**

Note: If there is no traffic over the circuit for the specified time period, the circuit hangs up. To configure the circuit as a dedicated link you must set the timer to zero. To configure the circuit to dial on demand, you must set it to a value other than zero. The range is 0 to 65535 and the default is 60 seconds.

3.5.4.1 Optional Configuration Steps

The following describes optional ISDN and dial circuit configuration parameters:

- If your ISDN telephone service provides accounting information, you can use the add accounting entry command to track telephone charges.
- if your ISDN switch supplies Power Source 1 (PS1), you should enable PS1 on the interface. This allows the interface to detect when the switch shuts down and to clear all information about the last call before it re-establishes the connection. To do this, use the enable ps1 command. This command is valid for only BRI.
- If your ISDN switch does not supply PS1, you should disable PS1 on the interface. To do this, use the disable ps1 command. This command is valid for only BRI.
- For all ISDN switches except INS64, you can limit the number of calls to an address that does not respond or that rejects those calls. Use the set retries-call-address command to set the number of calls to a non-responding destination. Use the set timeout-call-address command to set the time period to wait before trying the call again.

- Optionally, you can enter the configuration process for the data-link layer protocol that is running on the dial circuit (PPP) using the encapsulator command.

When you have finished configuring the ISDN interface, you can use the list command to display your configuration.

3.5.5 Frame Relay over ISDN Configuration

You can connect to a frame relay network through an ISDN network. Dial circuits default to point-to-point (PPP) protocol. To change the protocol to frame relay, enter the set data-link fr command at the Config> prompt. A connection will only be usable if the data link on both ends matches.

If you configure the frame relay over ISDN interface, you can back up the primary frame relay interface using WAN Restoral (WRS) or WAN Reroute.

3.5.6 Monitoring ISDN and Dial Circuits

You can monitor both the ISDN interface and the dial circuit interface in the following two ways. From the GWCON console:

- Use the interface command, as follows, to display statistics for ISDN interfaces and dial circuits. This command will give you information about the physical interface, such as transmit and receive or status of the interface.
+interface #
- To get information about the ISDN or dial circuit (PPP) configuration, use the network command as follows:
+network #

Table 46 on page 109 summarizes the ISDN console commands. The *Nways MRS Software User's Guide* documentation covers these commands in detail.

<i>Table 46. ISDN Console Command Summary</i>	
Console Command	Function
? (Help)	Lists the ISDN console commands or lists the options associated with specific commands.
Accounting	Displays the telephone charges that have accrued for each network address configured by the add accounting entries ISDN configuration command.
Calls	Lists the number of completed and attempted connections made for each dial circuit mapped to this interface since the last time statistics were reset on the router.
Channels	Lists the statistics for a channel on the ISDN Primary Rate interface.
Circuits	Shows the status of all data circuits configured on the ISDN interface.
Parameters	Displays the current parameters for the ISDN interface.
Statistics	Displays the current statistics for the ISDN interface.
Conf_test_cmds	Do not use these commands. These commands are for use in the IBM development environment only. Using these commands can disable the ISDN BRI interface, requiring a router reset.
Exit	Exits the ISDN console process and returns to the GWCON (+) process.

Table 47 summarizes the dial circuit (PPP) console commands. The *Nways MRS Software User's Guide* documentation covers these commands in detail.

<i>Table 47. Dial Circuit Console Command Summary</i>	
Console Command	Function
? (Help)	Displays all the point-to-point commands or lists subcommand options for specific commands (if available).
Clear	Clears all statistics from point-to-point interfaces.
List	Displays information and counters related to the point-to-point interface and PPP parameters and options.
LLC	Displays the LLC console monitoring prompt.
Exit	Exits the point-to-point console process and returns to the GWCON (+) prompt.

Note: The options available for these commands depend on what protocols are available in the router software.

Chapter 4. Bridging

This chapter describes different bridging methods. It lists the bridging functionality provided by the IBM 2210 and the interoperability supported with an IBM 6611 Network Processor. It explains the commands available to customize the IBM 2210 as a bridge. Then it provides you with bridging configuration scenarios between two IBM 2210s and between the IBM 2210 and IBM 6611 Network Processor.

4.1 Introduction to Bridging

Bridges act as data link layer relays between LANs. A bridge participates as a device on the networks to which it is attached, exchanges information with devices on those networks, and selectively forwards information between the networks.

Figure 37 shows that a bridge implements the physical and data link layers of the OSI reference model.

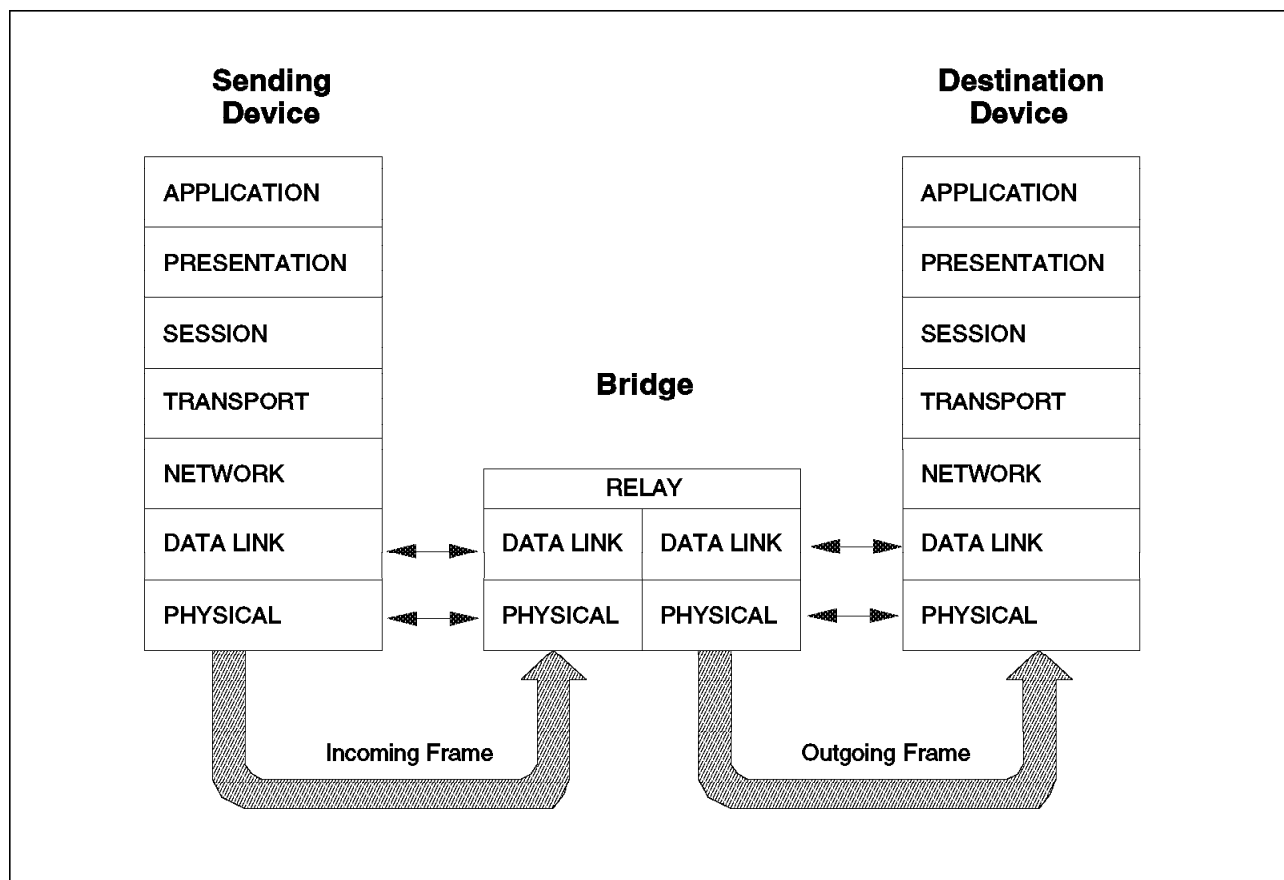


Figure 37. Bridge Implementation

The following list describes specific disadvantages to bridging:

- Bridges offer no protection against large volumes of broadcast packets. In forwarding broadcast packets, bridges are only carrying out their normal function, but in doing so can impact internetwork performance and function.

This can be a particular problem with remote bridges where broadcasts have to traverse inter-bridge serial links.

- Bridges have to drop packets that are too large for their attached networks. Bridges do not have the capability to fragment packets to accommodate networks with smaller maximum packet size.
- Bridges have no capability to provide congestion feedback to other bridges or to end nodes. This can lead to the need to discard packets with consequent impact on end system performance.

Equally, there are specific advantages to bridging:

- Bridges are *plug and play* and require little expertise to install.
- Bridges require little administrative overhead. Once installed they generally function with minimum attention.
- Bridges are truly multiprotocol. They forward all packets and protocols irrespective of whether the protocols are routable or not.
- Bridges are generally transparent to end systems. Generally, no specific customization is required at the end system.

To summarize, bridges are best used to provide convenient local connection within single site networks, possibly where there is limited technical and administrative support for the products. They are particularly suitable for environments where it is undesirable or impractical to configure end systems for operation with routers, or where the protocols in use are mainly non-routable.

4.2 Bridging Methods

There are two primary methods of bridging:

- Transparent bridging (mainly used with Ethernet LANs) also called spanning tree bridging (STB)
- Source route bridging (SRB) (used in 802.5 LANs)

Then, from these two primary methods of bridging, there are other methods listed below:

- Source route transparent bridging (SRT)
- Source route - translational bridging (SR-TB)
- Tunnel bridge (IP encapsulation)

All of these bridging methods are supported by the IBM 2210. For more details about the bridging methods supported by the IBM 2210, refer to 4.2.6, "Bridging Methods Supported by the IBM 2210" on page 119.

In the following sections, we provide a summary description of these bridging methods. For more information about the bridging methods, refer to *Nways MRS Protocol Configuration and Monitoring Reference*, SC30-3680-00.

4.2.1 Transparent Bridging (STB)

A transparent bridge is also called a spanning tree bridge (STB).

Transparent bridging is normally used to connect Ethernet LAN segments. It is specified in the ISO 8802-1 standard.

This form of bridging could also be used for the connection of token-ring LAN segments, although this is not common.

Transparent bridging is based on the principle that a sending device can transmit a frame to a receiving device on a LAN network without having any knowledge of the location of, or the path to, that receiving device.

Transparent bridges within a network are responsible for forwarding the frame to the correct destination and making the determination of whether a frame should be forwarded based on MAC sublayer destination address.

Transparent bridges achieve this by building and maintaining a *filtering database* that acts as a *forwarding table* for received frames. They build their database by copying all frames from the LANs to which they are attached, and learning the location of devices by inspecting the MAC sublayer *source address* in each received frame.

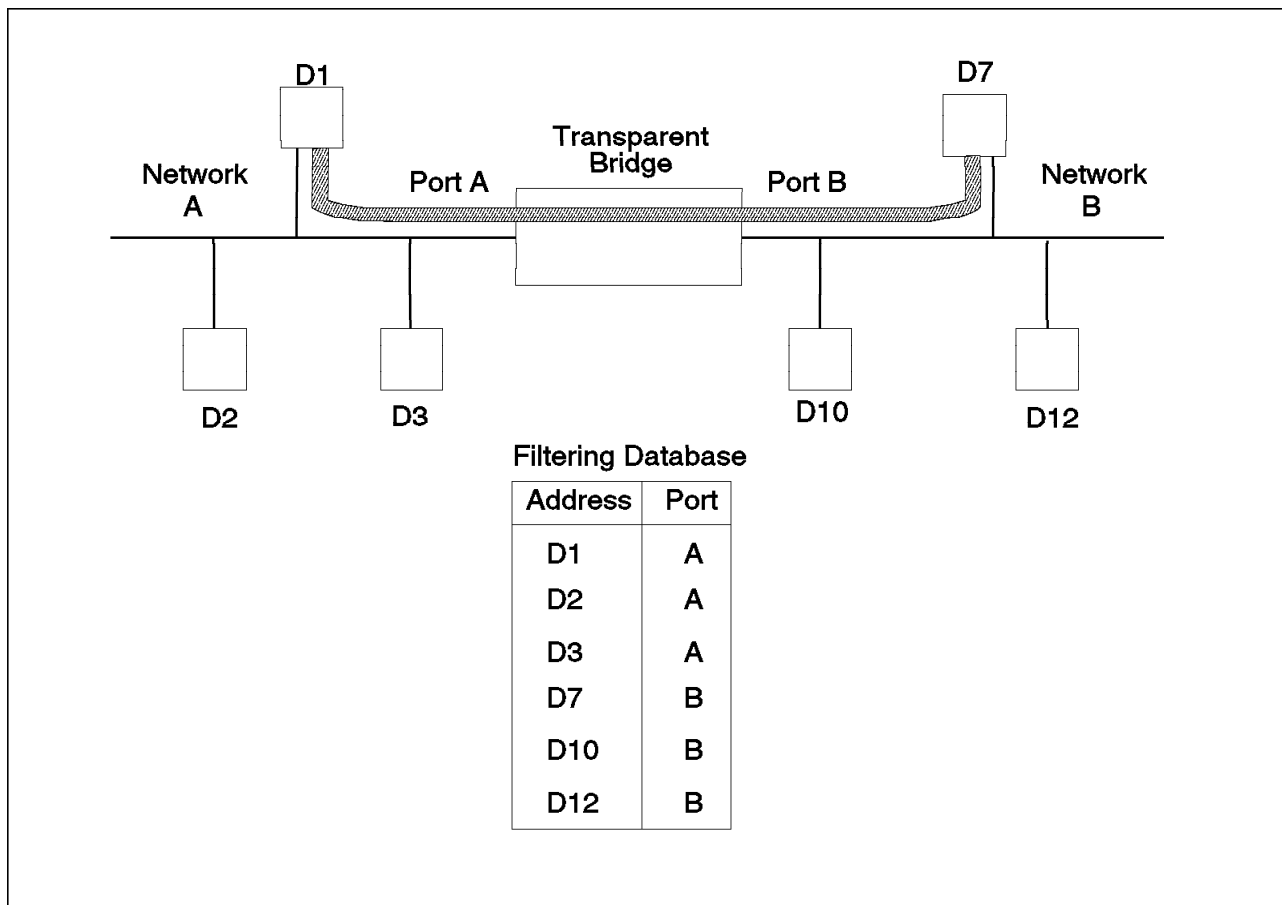


Figure 38. Transparent Bridging

Figure 38 illustrates how a transparent bridge will build up its filtering database. When the bridge receives a frame from device D1 on port A it learns that D1 can

be reached via the LAN on port A. Similarly, if a frame arrives from device D7 on port B, it learns that D7 can be reached via the LAN on port B.

For each new source address the bridge sees on the LANs, it adds an additional entry in its database. In time, a full picture is built up of all devices on the two LANs and the ports they can reach.

The bridge uses its filtering database to determine if an incoming frame should be forwarded or discarded. This is done by examining the MAC sublayer *destination address* of each frame and comparing it to the list of addresses in the filtering database:

- If the destination address is not in the database, the frame is forwarded on all forwarding ports except the receiving port.
- If the destination address is in the database and the frame was received on a port associated with the address, the frame is discarded.
- If the destination address is in the database and the frame was received on a port not associated with the address, the frame is forwarded to the associated port for this destination address in the database.

Transparent bridges require that there be only a *single* active path between any two LANs in an internetwork. This requirement is to ensure that frames do not loop such that they are seen on both ports of a bridge. If this happens the bridge will be unable to forward the frames correctly to their destination.

Transparent bridges support or use spanning tree protocol, which ensures a loop-free topology between all the transparent bridges within the network.

4.2.2 Source Route Bridging (SRB)

Source route bridging is implemented by IBM and compatible bridge products for use over token-ring LAN segments.

Source routing requires a sending device to specify the path that should be taken by a frame across an internetwork, rather than allowing the decision to be made by individual bridges. To do this, a sending device must determine the best path to a destination and include it in all frames to that destination. The best path to a destination is found using a discovery process, one implementation of which is described below.

A *sending* device sends a discovery frame to the intended destination device, marked single-route broadcast. Bridges in a token-ring internetwork should be configured using the token-ring spanning tree algorithm to permit only one path for single-route broadcast frames between devices. The destination device should therefore receive only a single copy of the discovery frame.

The destination device responds to the discovery frame with a discovery response frame, marked all-routes broadcast. This will contain the most significant bit (the route information indicator, also called RII) set in the source MAC address field, and an entry in the routing information field (RIF). This will initially contain zero in the bridge number field, and the number of the networks to which the destination device is attached in the segment number field.

The discovery response frame, because it is marked all-routes broadcast, will pass through all bridges on its way back to the original sending device. Each bridge that the frame passes through must insert its bridge number and LAN

segment, and hence the frames that return to the original sending device contain the routes they have taken through the bridged internetwork.

The routing information field can currently only hold data about seven (or thirteen) bridges and eight (or fourteen) LAN segments. If a frame is received by a bridge with this field full, it will be discarded. This limits the number of bridge *hops* in the network to seven (or thirteen), and consequently the maximum size of source route bridged internetworks.

The original sending device therefore receives one or more discovery response frames. These frames contain routing control, and bridge and LAN segment numbers in their routing information fields. The routing control field indicates the number of bridge/LAN segment in the routing information field, and also the maximum frame size that can be supported by the route.

The sending device can now select the best route to use through the internetwork to reach the destination device. Current implementations select the route in the *first* received discovery response frame (the fastest path at the time of the discovery process), although the architecture allows route selection based on other criteria, for example, maximum frame size supported by the route.

Figure 39 shows how the routing information field is used to define a route through an internetwork between end nodes D1 and D7.

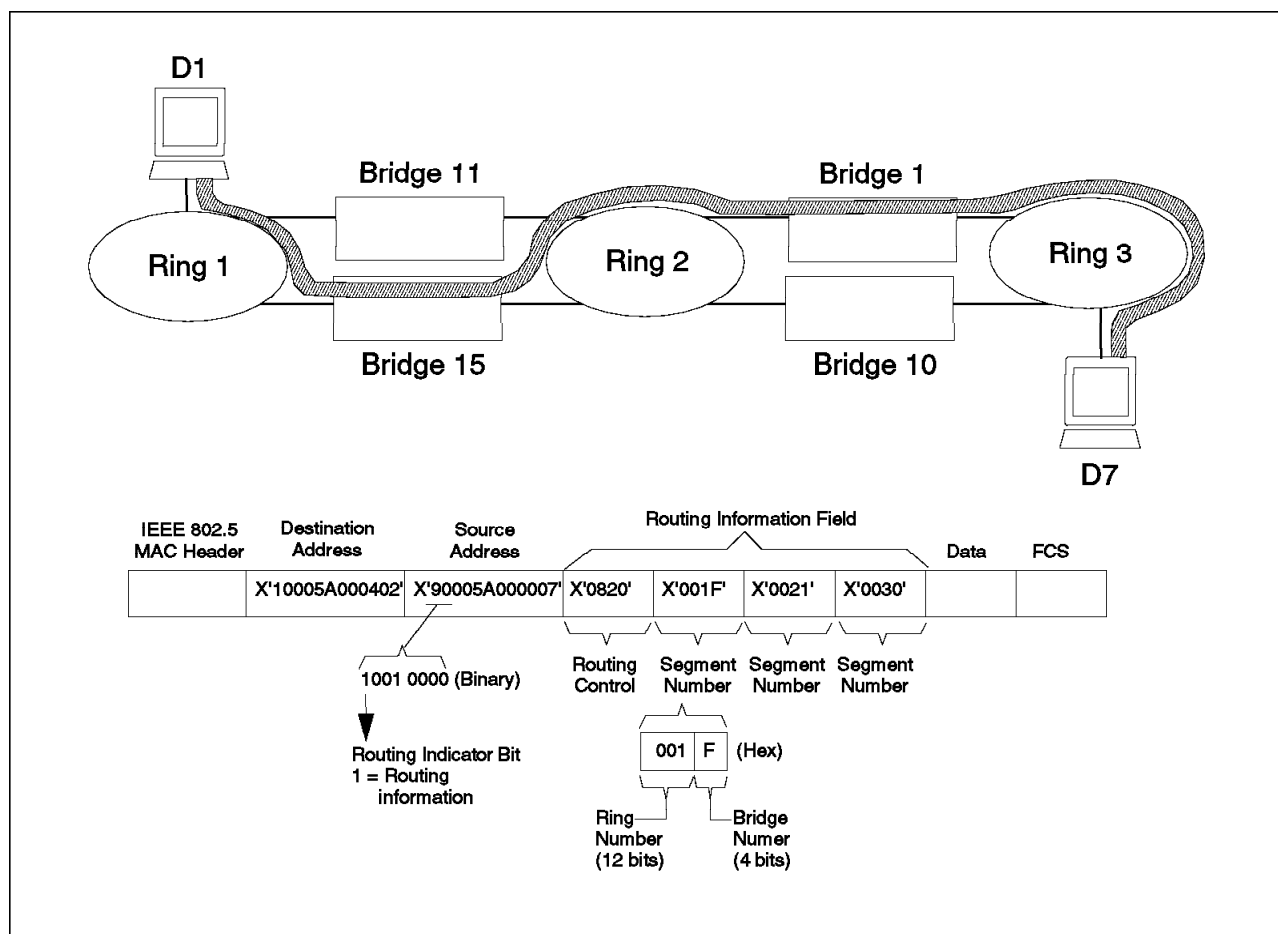


Figure 39. Source Route Bridging

4.2.3 Source Route Transparent Bridging (SRT)

The IEEE 802.1 committee identified the need for source route bridges to interoperate with transparent bridges in the same internetwork. A *source route transparent bridge (SRT)* standard has been defined to achieve this goal.

The principle behind SRT bridges is very simple. An SRT bridge inspects all received frames and looks for the presence of the routing information indicator (RII) and the routing information field (RIF). If these fields are present, the SRT bridge uses them and acts as a source route bridge. If not, the SRT bridge operates in transparent bridge mode and forwards frames based on their MAC sublayer destination address and its associated entry in the filtering database.

The source route transparent bridge does not allow source route bridge devices to communicate with transparent bridge devices. SRT bridge is the capability for its interfaces to understand both source route bridging and transparent bridging devices. But an SRT bridge will never translate source route bridge frames into transparent bridge frames, and vice versa.

Figure 40 shows you frames with RII=1 are forwarded with RII=1 and frames with RII=0 are forwarded with RII=0.

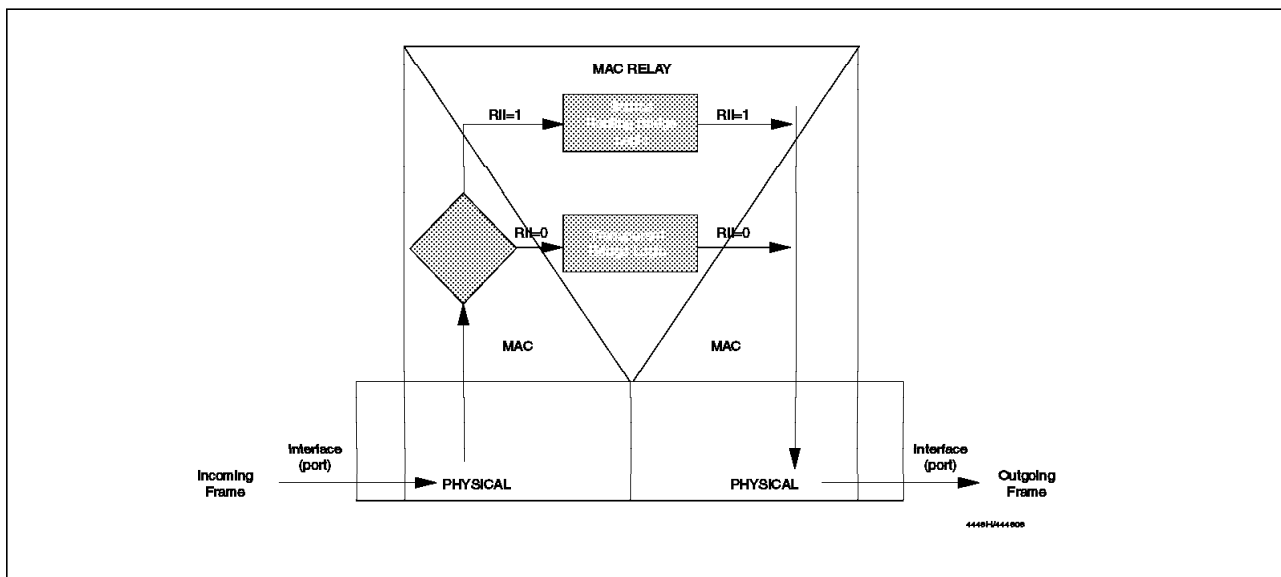


Figure 40. Source Route Transparent Bridge

4.2.4 Source Route-Translational Bridge (SR-TB)

Source route-translational bridge (SR-TB) is not an ISO standard definition. However, more and more bridges are implementing the SR-TB because of the need to interconnect a source route bridge domain with a transparent bridge domain.

The goal of the source route-translational bridge is to translate a source route bridge frame into a transparent bridge frame and vice versa.

The SR-TB bridges have to change the MAC layer protocol from (or to) Ethernet protocol to (or from) token-ring protocol. Actually, regarding the ISO bridge definition, this translation does not belong to a bridge. But it is implemented in

a lot of bridges, in order to be able to interconnect source route bridge domain and transparent bridge domain regardless of the protocol of the upper layer.

Figure 41 shows you that the SR-TB allows a SRB device with RII=1 to communicate with a STB device (RII=0).

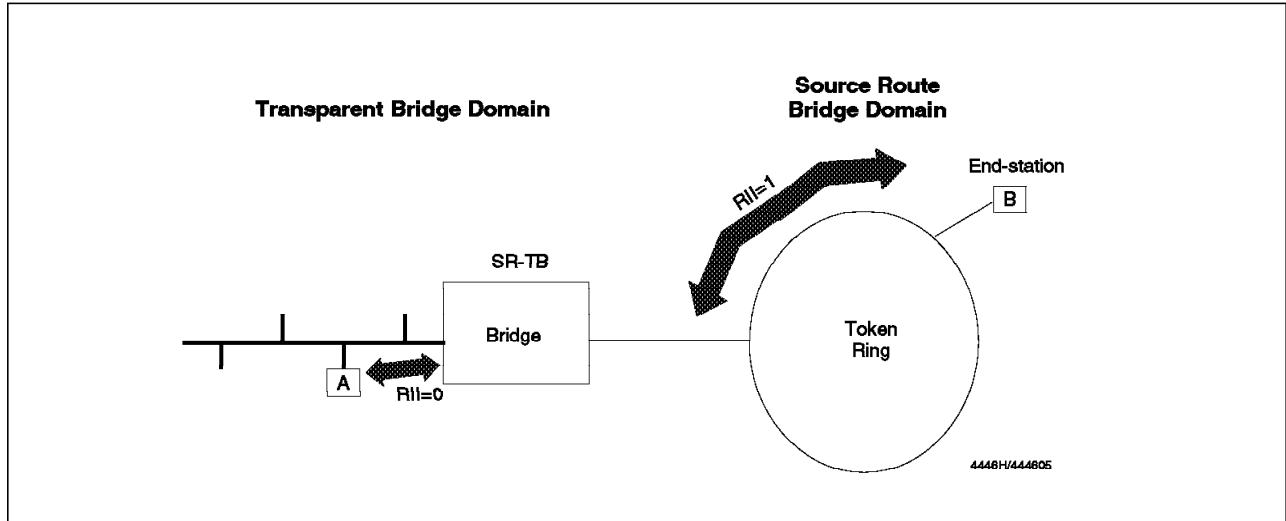


Figure 41. Source Route-Translational Bridging

4.2.5 Tunnel Bridge

The tunnel bridge allows source route bridge domains or transparent bridge domains to communicate across an IP network. For more information about IP protocol, see Chapter 7, "IP Routing Protocols" on page 295.

The tunnel bridge receives bridged frames from its source route bridge or transparent bridge domain. The frames are encapsulated into IP datagrams, which are sent to the destination IP address. These IP datagrams are routed in the IP network as any other IP datagrams, with the IP rules.

The destination IP address is actually another bridge implementing the tunnel bridge feature. This target bridge removes the IP envelope from these IP datagrams, making them source route bridge or transparent bridge frames. Then the target bridge sends these frames to its source route bridge domain or transparent bridge domain as any other bridged frames.

Figure 42 on page 118 shows you an example of the tunnel bridge implementation.

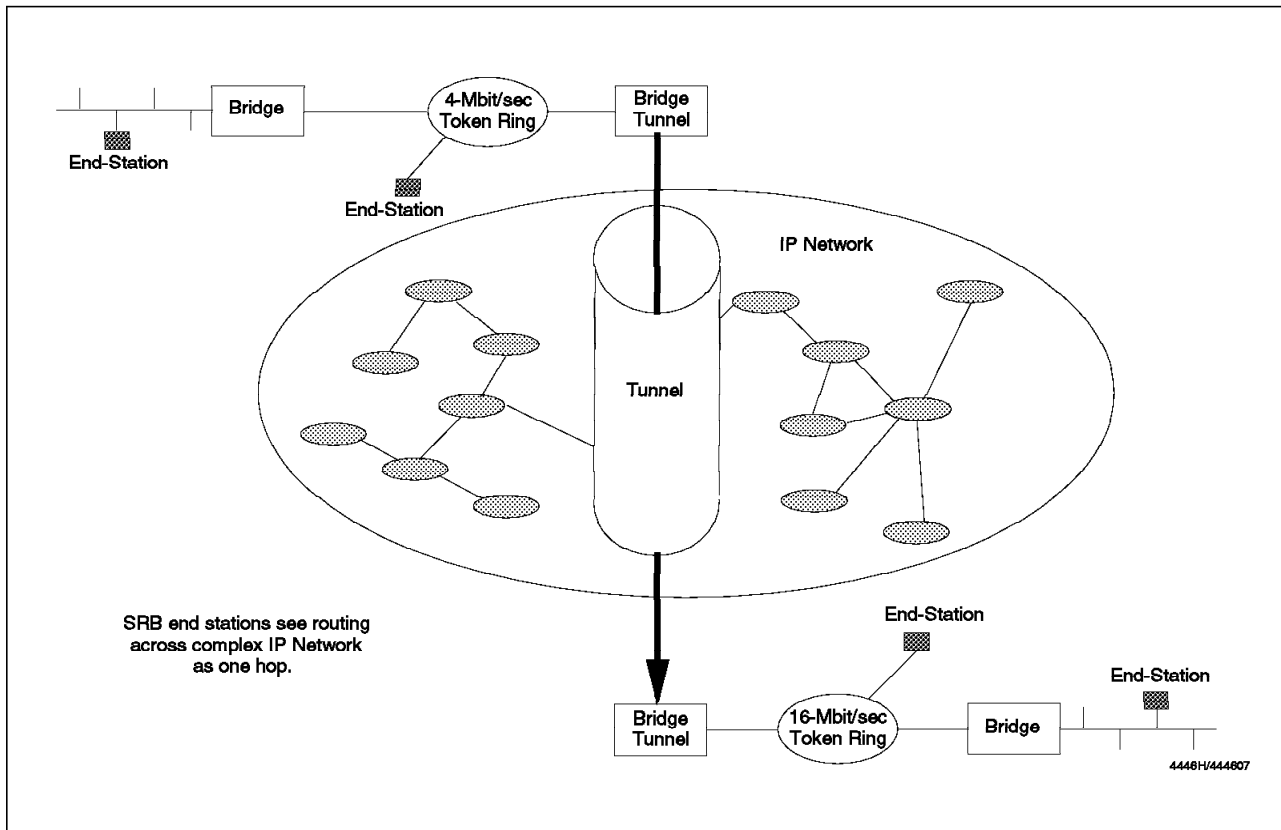


Figure 42. Tunnel Bridging

With tunnel bridging, as far as the source route bridge is concerned, the IP network is seen as a single LAN segment, regardless of the complexity of the IP network. Then it adds only one hop to cross this IP network.

The number of hops from the source device to the source IP tunnel bridge, plus one hop to cross the IP network, plus the number of hops from the destination IP tunnel bridge to the destination device, must not exceed the seven hops count limitation of the source route bridge implementation.

4.2.6 Bridging Methods Supported by the IBM 2210

The supported functionality listed in this section is for the Nways MRS Program Version 1 Release 1 for the IBM 2210.

The IBM 2210 is an adaptive source routing transparent (ASRT) bridge. It is a software collection of the following four bridging options:

- Spanning tree bridge or transparent bridge (STB)
- Source route bridge (SRB)
- Source route transparent bridge (SRT)
- Source route-translational bridge (SR-TB)

The dial backup or WAN Restoral (WRS) feature over a PPP primary link supports any bridging method.

The Dial on Demand feature does not support any bridging methods on serial or on ISDN links.

IBM 2210 supports bridging over PPP and frame relay serial links only. It cannot perform bridging over X.25 or SDLC links. If you are planning to transport bridged traffic over frame relay or X.25, you must use the tunnel bridge function provided by IBM 2210. Note that the tunnel bridge is supported over any serial link that supports IP. This includes PPP, frame relay and X.25 serial links.

SRB, STB and SRT bridging methods have to be enabled on the interfaces, while SR-TB and tunnel bridge are enabled at the bridge level.

Table 48 shows the bridging methods supported by each IBM 2210 interface.

<i>Table 48. Supported Bridging Methods for the IBM 2210</i>								
Bridging Methods	PPP	FR	X.25	SDLC	Dial on Demand	Dial Backup	Token-Ring	Ethernet
STB	yes	yes	<i>no</i>	<i>no</i>	<i>no</i>	yes	<i>yes</i>	yes
SRB	yes	yes	<i>no</i>	<i>no</i>	<i>no</i>	yes	yes	<i>no</i>
SRT	yes	yes	<i>no</i>	<i>no</i>	<i>no</i>	yes	yes	<i>no</i>
SR-TB	yes	yes	<i>no</i>	<i>no</i>	<i>no</i>	yes	yes	yes
Tunnel (IP)	yes	yes	yes	<i>no</i>	yes	yes	yes	yes

With the ASRT bridge, the collection of configuration parameters for the bridge and all its interfaces produces a *bridge personality*. The bridge personality is also called bridge behavior.

Figure 43 on page 120 shows you how to list the bridge personality via the ASCII console attached to the IBM 2210.

```

*
*talk 6

Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:  ENABLED                      Bridge Behaviour: ADAPTIVE SRT
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  6      No. of Source routing segments: 3
SRB: Max ARE Hop cnt:  14             Max STE Hop cnt: 14
SR-TB Conversion: ENABLED  TB-Virtual Segment:0x21  MTU for TB-Domain: 1470
1:N Source Routing:  ACTIVE              Internal-Virtual Segment:0x24
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d and IBM-8209
DLS for the bridge:  DISABLED
Number of ports added: 3
Port Number:  1      Interface Number:  0 Port Behaviour: STB & SRB
Port Number:  2      Interface Number:  1 Port Behaviour: SRB Only
Port Number:  3      Interface Number:  2 Port Behaviour: SRB Only

ASRT config>exit
Config>Ctrl+p
*

```

Figure 43. List the Bridge Personality via an ASCII Console

The bridge personality may have the following values:

- SRB (pure source routing bridge)
- STB (pure transparent bridge)
- SRT (source route transparent bridge)
- SR-TB (source route-translational bridge)
- ASRT (either SRB, STB, SRT or SR-TB, depending on the source and the destination devices)
- Unknown (when the bridge customization results in no valid bridging)

Table 49 provides a guide to the configuration settings needed for interfaces to produce the desired bridge personality. In this table, ports A, B and C could be an Ethernet, token-ring or serial link on the IBM 2210.

Note that the only bridging methods supported by the Ethernet interface is STB. The token-ring interface supports STB, SRB, or both STB and SRB. The serial link supports STB, SRB, or both SRB and STB bridging methods.

Table 49 (Page 1 of 2). Bridge Personality Regarding Bridge Configuration

Port A	Port B	Port C	SR <-> TB Conversion	Bridge personality
STB	STB	No bridging	Disable	STB
STB	SRB	No bridging	Enable	SR-TB

<i>Table 49 (Page 2 of 2). Bridge Personality Regarding Bridge Configuration</i>				
Port A	Port B	Port C	SR <-> TB Conversion	Bridge personality
STB	STB & SRB	No bridging	Enable	ASRT
SRB	SRB	No bridging	Disable	SRB
SRB	STB & SRB	No bridging	Enable	ASRT
STB & SRB	STB & SRB	No bridging	Disable	SRT
STB & SRB	STB & SRB	No bridging	Enable	ASRT
STB	STB	STB	Disable	STB
STB	STB	SRB	Enable	SR-TB
STB	STB	STB & SRB	Enable	ASRT
STB	SRB	SRB	Enable	SR-TB
STB	SRB	STB & SRB	Disable	SRT
STB	SRB	STB & SRB	Enable	ASRT
STB	STB & SRB	STB & SRB	Disable	SRT
STB	STB & SRB	STB & SRB	Enable	ASRT
SRB	SRB	SRB	Disable	SRB
SRB	SRB	STB & SRB	Enable	ASRT
SRB	STB & SRB	STB & SRB	Disable	SRT
SRB	STB & SRB	STB & SRB	Enable	ASRT
STB & SRB	STB & SRB	STB & SRB	Disable	SRT
STB & SRB	STB & SRB	STB & SRB	Enable	ASRT

4.2.7 Bridging Methods Supported between the 2210 and the 6611

The supported functionality listed in this section corresponds to the Nways MRS Program Version 1 Release 1 for the IBM 2210 and to IBM 6611 MPNP Program Version 1 Release 3 for the IBM 6611 Network Processor.

A 2210 bridge may communicate with a 6611 bridge either over token-ring, Ethernet or a PPP serial link.

Note that tunnel bridge is not supported between the 2210 and the 6611.

Table 50 shows the bridging methods supported over each interface of either the 2210 or the 6611.

<i>Table 50. Supported Bridging Methods between the 2210 and the 6611</i>					
Bridging Methods	Ethernet	Token-Ring	PPP	FR	X.25
STB	yes	no	yes	yes	no
SRB	no	yes	yes	yes	no
SR-TB	yes	yes	yes	yes	no

Note

When you want to perform source route-translational bridging between the IBM 2210 and the IBM 6611 Network Processor:

1. You may configure either the IBM 2210 or the IBM 6611 Network Processor to perform the translational function if the source routing (token-ring) side is attached to the IBM 6611 Network Processor.
2. You must configure the IBM 6611 Network Processor to perform the translational bridging if the transparent (Ethernet) side is attached to the IBM 6611 Network Processor. In this case, if you cannot configure the IBM 2210 to perform the translational bridging.

4.3 Bridging Configuration Commands

The following sections summarize the bridging configuration commands and the tunnel bridge configuration commands available via the CONFIG process of the Nways MRS and the Nways MRS Configuration Program.

Table 51 on page 123 shows you the main ASRT commands available. The *Nways MRS Protocol Configuration and Monitoring Reference*, SC30-3680-01, covers these commands in detail.

<i>Table 51. ASRT Configuration Commands</i>	
Command	Function
? (Help)	Lists all the ASRT configuration commands, or lists the options associated with specific commands.
Add	Adds station address entries to the permanent database, specific address mapping, LAN/WAN ports, protocol filters, and a tunnel between endstations across an IP internetwork.
Change	Allows the user to change bridge and segment number.
Delete	Deletes station address entries, specific address mapping, LAN/WAN ports, protocol filters, and a tunnel between endstations across an IP internetwork.
Disable	Disables bridging functionality, duplicate frames, mapping between group and functional addresses, propagation of spanning tree explorer frames, source routing on a given port, reception of spanning tree explorer frames over a tunnel, conversion of source routed frame to transparent frame, transparent (spanning tree) bridging functionality on a given port, and a tunnel between bridges.
Enable	Enables bridging functionality, duplicate frames, mapping between group and functional addresses, propagation of spanning tree explorer frames, source routing on a given port, reception of spanning tree explorer frames over a tunnel, conversion of source routed frame to transparent frame, transparent (spanning tree) bridging functionality on a given port, and a tunnel between bridges.
List	Displays information about the complete bridge configuration or about selected configuration parameters.
Name caching	Accesses NetBIOS name caching configuration prompt.
NetBIOS-filtering	Allows access to the NetBIOS filtering configuration prompt so that NetBIOS filtering configuration command can be entered.
Set	Sets aging time for dynamic address entries, bridge address, maximum frame size for tunneling, largest frame (LF) bit encoding, maximum frame size, spanning tree protocol bridge and port parameters, Route Descriptor (RD) values, and filtering database size.
Tunnel	Allows access to the tunnel configuration prompt so that tunnel configuration commands can be entered. See Table 52 on page 133 about the tunnel bridge commands.
Exit	Exits the ASRT configuration process and returns to the CONFIG environment.

Nways MRS Configuration Program provides the following panels for configuring the bridging functions of the IBM 2210:

- Bridging-General panel - This panel is accessed by selecting **Bridging-General** of the Bridging directory.
- Spanning Tree Protocol General panel - This panel is accessed by selecting the **General** panel of the Spanning Tree Protocol subdirectory of the Bridging directory.
- Spanning Tree Protocol Interfaces panel - This panel is accessed by selecting the **Interfaces** panel of the Spanning Tree Protocol subdirectory of the Bridging directory.
- Address Filtering panel - This panel is accessed by selecting the **Address Filtering** panel of the Filtering subdirectory of the Bridging directory.
- Ethernet Filtering panel, DSAP Filtering panel and SNAP Filtering panel - These panels are accessed by selecting the corresponding panel (Ethernet, DSAP or SNAP) of the Protocol Filtering subdirectory of the Filtering subdirectory of the Bridging directory.

- Ethernet Mapping panel, DSAP Address Mapping panel and SNAP Address Mapping panel - These panels are accessed by selecting the corresponding panel (Ethernet, DSAP or SNAP) of the Protocol Mapping subdirectory of the Bridging directory.
- Bridging Interfaces panel - This panel is accessed by selecting the **Interfaces** panel of the Interfaces subdirectory of the Bridging directory.
- TCP/IP Host Services panel - This panel is accessed by selecting the **TCP/IP Host Service** panel of the TCP/IP Host Services subdirectory of the Bridging directory.
- NetBIOS Name Caching panel - This panel is accessed by selecting the **Name Caching** panel of the NetBIOS subdirectory of the Bridging directory.
- NetBIOS Filtering panel - This panel is accessed by selecting the **Enable** panel of the Filtering subdirectory of the NetBIOS subdirectory of the Bridging directory.
- NetBIOS Filter Name Lists panel - This panel is accessed by selecting the **Name Lists** panel of the Filtering subdirectory of the NetBIOS subdirectory of the Bridging directory.
- NetBIOS Interfaces panel - This panel is accessed by selecting the **Interfaces** panel of the Filtering subdirectory of the NetBIOS subdirectory of the Bridging directory.

Note

See 11.11, "NetBIOS Facilities" on page 713 for NetBIOS Name Caching and NetBIOS Filtering configuration commands.

4.3.1 Basic Bridging Configuration Commands

The following are the commands used for every bridging configuration:

- To access the Bridging Protocol, enter the following command from the CONFIG process:

```
Config>protocol asrt
```

The prompt becomes:

```
ASRT Config>
```

For Nways MRS Configuration Program, all the panels used to configure Bridging are within the Bridging directory.

- You may enable bridging at the box level using the following command:

```
ASRT Config>enable bridge
```

Note that bridging is disabled by default.

For Nways MRS Configuration Program, you must select **Enable Bridging** in the Bridging General panel.

- You may list the current bridging configuration using the following command:

```
ASRT Config>list bridge
```

This command allows you to determine if the bridging is enabled.

- If you are planning to configure the IBM 2210 to perform Data Link Switching function, you must enable DLSw using the following command:

```
ASRT Config>enable dls
```

By default, dls is disabled.

For Nways MRS Configuration Program, you must select **Enable DLSw** in the Bridging General panel.

- By default, the ASRT protocol has just one bridging port (port 1). This port is associated with interface 0 (the LAN interface). You must add the other ports on which you wish to perform bridging. For example, to add port number 2 for interface 1, issue the following command:

```
ASRT Config>add port 1 2
```

By default, a new added port bridges packet using STB.

You can display bridge ports and their corresponding interfaces using the following command:

```
ASRT Config>list port
```

You cannot add or delete ports via Nways MRS Configuration Program.

- You can delete bridging ports using the following command:

```
ASRT Config>delete port
```

For example, to delete port number 2 issue the following command:

```
ASRT Config>delete port 2
```

- You may change the bridging method configured for each port by disabling the current bridging method and enabling the desired bridging method. For example, as the added ports are configured for STB by default, to change the bridging method for port 1 to SRB with LAN segment number of DEF and the bridge number A, issue the following commands:

```
ASRT Config>disable transparent 1
```

```
ASRT Config>enable source-routing 1 DEF A
```

Note that the bridge number must be entered only in the first Enable Source-Routing command issued for the IBM 2210, whereas the LAN segment number must be entered for each Enable Source-Routing command. If you enter the bridge number in the subsequent Enable Source-Routing commands, it will be ignored.

You can change the bridge number using the following command:

```
ASRT Config>change bridge B
```

where B is the new bridge number.

For Nways MRS Configuration Program, the bridge number is set in the Bridging General panel, while the LAN segment number is set at the corresponding interface configuration of the Bridging Interfaces panel.

If you have more than one port customized in the IBM 2210, you will be prompted for the internal virtual segment number. This is used to simulate a virtual segment in the IBM 2210 and will add a hop in the routing information field (RIF).

For Nways MRS Configuration Program, the internal virtual segment must be set in the Bridging General panel.

- You may want to prevent a port from participating in the spanning tree protocol. To do so, you must disable the port. For example, to disable port 1, issue the following command:

```
ASRT config>set port disable 1
```

For Nways MRS Configuration Program, enable each interface you want to participate in bridging by using the Bridging Interfaces panel. By default, the ports are disabled by Nways MRS Configuration Program.

Note

After disabling a port, there is no command to enable it again. The only way to enable the port is to delete it and add the port again.

4.3.2 Configuration Commands for SRB Bridging

To configure your IBM 2210 for source route bridging (SRB), you may perform the following:

- You may change the bridge number using the following command, which changes the bridge number to B:

ASRT Config>**change bridge B**

- You may change the segment number using the following example that changes the segment number from DEF to 123:

ASRT Config>**change segment DEF 123**

For Nways MRS Configuration Program, you can change the bridge number using the Bridging General panel, or change the LAN segment number for an interface using the Bridging Interfaces panel.

- You may want to allow propagation of spanning tree explorer frames on a port when source route bridging is enabled. For example, to allow port 2 to propagate spanning tree explorer frames, issue the following command:

ASRT Config>**enable spanning-tree-explorer 2**

For Nways MRS Configuration Program, you can enable the propagation of spanning tree explorer frames using the Interfaces panel of the Interfaces subdirectory of the Bridging directory.

- You may set the number of bits in the Routing Control field of the routing information field (RIF) that determines the largest frame size that can be sent via bridge. See the RIF layout on Figure 28 on page 60 for more details. For example, to use 6 bits for the largest frame size, issue the following command:

ASRT config>**set lf-bit-interpretation extended**

To use 3 bits for the largest frame size, issue the following command:

ASRT config>**set lf-bit-interpretation basic**

The default for lf-bit-interpretation is 6 bits (extended).

You can display the current lf-bit-interpretation setting using the List Bridge command.

For Nways MRS Configuration Program, use the Bridging General panel for setting this parameter.

- You may want to set the largest MAC service data unit (MSDU) for a specific port. For example, to set the MSDU to 3812 on port 1, issue the following command:

ASRT config>**set maximum-packet-size 1 3812**

You can display the current maximum-packet-size value for a port using the List Port command.

For Nways MRS Configuration Program, use the Bridging Interfaces panel to set this parameter.

- You may set the maximum number of the route descriptor (also called route designator) in the routing information field (RIF) for the all route explorer frames (ARE) or spanning tree explorer frames (STE). For example, to set up 10 route descriptors for the all route explorer frames, issue the following command:

```
ASRT config>set route-descriptor-limit are 10
```

To set up 10 route descriptors for the spanning tree explorer Frames, issue the following command:

```
ASRT config>set route-descriptor-limit ste 10
```

The default for both ARE and STE is 14 route descriptors.

You can display the current limits for the route descriptors using the List Bridge command.

For Nways MRS Configuration Program, you can set the route-descriptor-limit using the Bridging General panel.

4.3.3 Configuration Commands for Spanning Tree Protocol

The following commands are used to configure the spanning tree protocol on the IBM 2210:

- To enable the spanning tree protocol, you must issue the following command:

```
ASRT Config>enable stp
```

With SR-TB conversion disabled, the spanning tree protocol used is the IEEE 802.1d protocol if there is at least one port with transparent bridging methods. If all ports have only source route bridging methods enabled, the spanning tree protocol will be the IBM-SRB proprietary protocol.

You can display which spanning tree protocol is enabled by using the List Bridge command.

For Nways MRS Configuration Program, use the Spanning Tree Protocol General panel.

- To use the spanning tree protocol, each bridge must have a unique address assigned to it. You may assign a bridge address to the IBM 2210 using the following command:

```
ASRT config>set bridge 4000002210A1
```

You can display the bridge address used by your IBM 2210 using either List Bridge or the List Protocol command.

In Nways MRS Configuration Program, the bridge address is set by using the Spanning Tree Protocol General panel.

- You may want to allow the IBM 2210 to participate in spanning tree protocols with IBM 8209 bridges. This could be done only when SR-TB conversion is enabled. To do so, issue the following command:

```
ASRT Config>enable IBM8209_spanning_tree
```

With SR-TB conversion enabled, the spanning tree protocols used are IEEE 802.1d protocol on the TB ports and IBM8209 protocol on the SR ports.

You can display which spanning tree protocol is enabled using the List Bridge command.

With Nways MRS Configuration Program, you can enable SR-TB conversion using the Bridging General panel.

- You may want to set a port status to blocked status as a starting point. The actual state of the port will later be determined by the spanning tree protocol as it determines the network topology.

For example, to set the status of port 2 to blocked, issue the following command:

```
ASRT config>set port blocked 2
```

In Nways MRS Configuration Program, each interface can be selectively enabled or disabled for the spanning tree protocol using the Spanning Tree Protocol Interfaces panel.

- You may want to tune the following spanning tree protocol parameters at the bridge level:
 - Bridge Maximum Age (20)
 - Bridge Hello Time (2)
 - Bridge Forward Delay (15)
 - Bridge Priority (32768)

Note that the defaults are shown in parentheses.

To change the above parameters, you must enter the following command, which will then prompt you for each of the parameters:

```
ASRT config>set protocol bridge
```

You can display the setting of these parameters using the List Protocol command.

In Nways MRS Configuration Program, these four parameters can be set using the Spanning Tree Protocol General panel.

- You may want to tune the following spanning tree protocol parameters at a specific port level:
 - Port Path-Cost (0)
 - Port Priority (128)

The defaults for these parameters are shown in parentheses.

For example, to change the above parameters for port 1, enter the following command:

```
ASRT config>set protocol port 1
```

You will then be prompted to enter each of the parameters.

You can display the current setting for these parameters using the List Port command.

In Nways MRS Configuration Program, both parameters can be set using the Spanning Tree Protocol Interfaces panel.

4.3.4 Configuration Commands for the Filtering Database

The following commands may be used to customize the filtering database (also called forwarding table) of the IBM 2210:

- You may add permanent MAC address entries in the IBM 2210 Filtering Database. These entries are copied into the filtering database as permanent entries when the bridge is started. When entering permanent entries, you are given the option to specify the outgoing forwarding map for each incoming port. For example, the following commands add the MAC address 02005A123456 to the filtering database and specify that the frames destined to this MAC address that are received on port 1 are to be bridged to port 2:

```
ASRT config>add address 02005A123456
Exclude destination address from all ports?(Yes or [No]): No
Use same output port mapping for all input Ports?(Yes or [No]): No
Output port mapping:
  Input Port Number [1]? 1
  Bridge to all ports?(Yes or [No]): No
  Bridge to port 1 - Yes or [No]: No
  Bridge to port 2 - Yes or [No]: Yes
  Bridge to port 3 - Yes or [No]: No
  Bridge to port 4 - Yes or [No]: No
  continue to another input port? (Yes or [No]): No
Source Address Filtering Applies? (Yes or [No]): No
```

You can display the entries in the filtering database using the List Range command.

In Nways MRS Configuration Program, add permanent MAC addresses in the filtering database using the Address Filtering panel.

- You may set the aging time for the dynamic entries in the filtering database. You can also specify the frequency of the checking of the aging time for these entries. The frequency of checking the filtering database is called resolution time.

For example, to set an aging time of 600 seconds with a resolution time of 10 seconds, you must issue the following command:

```
ASRT config>set age 600 10
```

By default, the aging time is 300 seconds and the resolution time is 5 seconds.

You can display the current aging time and resolution time using the List Filtering command.

Note: The aging time is also used for aging RIF entries in the RIF table in the case of SR-TB bridge personality.

In Nways MRS Configuration Program, you can set these parameters using the Bridging General window.

- You may specify the maximum number of MAC addresses allowed in the filtering database. For example, to set a maximum of 500 entries for the filtering database, you must issue the following command:

```
ASRT config>set filtering 500
```

The default filtering database size is 1024 entries multiplied by the number of ports.

You can display the maximum number of entries allowed in the filtering database using the List Filtering command.

In Nways MRS Configuration Program, you can set the filtering database size using the Bridging General panel.

4.3.5 Configuration Commands for the SR-TB Bridging

You may use the following commands to customize the source route-translational bridging method on the IBM 2210:

- To enable the source route-translational bridging (SR-TB) at the box level, with the TB domain seen as a virtual segment number FFF from the SRB domain, issue the following command:

```
ASRT Config>enable sr-tb-conversion fff
```

You can display the settings of SR-TB conversion and also the TB-domain segment number using the List Bridge command.

In the Nways MRS Configuration Program, the SR-TB conversion and the virtual segment number for TB domain are set using the Bridging General panel.

- If you have enabled both source route bridging (SRB) and transparent bridging (STB) on a serial port and the IBM 2210 receives either a spanning tree explorer (STE) frame or a transparent spanning frame (TSF) from its LAN port, by default, the IBM 2210 sends two copies of this frame on the serial port. These two frames will be one spanning tree explorer (STE) frame with RIF information (RIL bit = 1) for the source route bridge domain, and one transparent spanning frame (TSF) without RIF information (RIL bit = 0) for the transparent bridge domain.

This is because the IBM 2210 does not yet know whether the destination is in the source route bridge domain or in the transparent bridge domain.

If you want the explorer frames received on the LAN port (port 1) to be sent only as a transparent spanning frame (TSF) without RIF (RIL = 0), issue the following commands:

```
ASRT config>enable duplicate tsf  
Port Number [1]? 1  
ASRT config>disable duplicate ste  
Port Number [1]? 1
```

If you want the explorer frames received on the LAN port (port 1) to be sent only as a spanning tree explorer frame (STE) with RIF (RIL = 1), you must issue the following commands:

```
ASRT config>enable duplicate ste  
Port Number [1]? 1  
ASRT config>disable duplicate tsf  
Port Number [1]? 1
```

You can see if duplicate STEs and duplicate TSFs are enabled using the List Port command.

In Nways MRS Configuration Program, you can set the above parameters using the Bridging Interfaces panel.

- In a source route-translational bridge environment, some protocols use *group* addresses for Ethernet that do not correspond to the equivalent *functional* addresses used in token-ring. Therefore, the IBM 2210 allows you to create specific mappings between Ethernet group addresses and token-ring functional addresses.

For every mapped Ethertype on Ethernet interface, the corresponding SNAP or SAP value on token-ring must be added. For example, to have the IBM 2210 to do source route-translational bridging (SR-TB) for DEC LAT, the address mapping shown in Figure 44 on page 131 must be defined.

Token-Ring Address In Non-Canonical	Ethernet Address In Canonical	Description
-----	-----	-----
C00000100000	CF0000000000	Loopback
C00000200000	09002B040000	LAST (group 0)
C00000400000	09002B020107	LAT Xwin Service Solicit
C00001000000	09002B020104	LAT solicit
C00002000000	09002B00000F	LAT Advertisement
C00020000000	AB0000020000	MOP Console
C00040000000	AB0000010000	MOP Dump/Load

Figure 44. Address Mapping for DEC LAT Source Route - Translational Bridge

The following are the commands that must be used to define the first line in Figure 44 in both directions:

```
ASRT config>add mapping ether 6004
Group-Address (in 12-digit hex) []? CF0000000000
Functional-Address (in non-canonical 12-digit hex) []? C00000100000
ASRT config>add mapping snap 0000006004
Group-Address (in 12-digit hex) []? CF0000000000
Functional-Address (in non-canonical 12-digit hex) []? C00000100000
```

Note

0000006004 is the SNAP value for DEC LAT.

You may display the mapping addresses using the List Mapping command. For example to display the mapping addresses of Ether protocol with protocol type value of 6004, issue the following command:

```
ASRT config>list mapping ether 6004
```

In Nways MRS Configuration Program, use the corresponding protocol Address Mapping panel for each protocol. There is the Ethernet Address Mapping panel for Ethernet protocol, the DSAP Address Mapping panel for DSAP protocol and the SNAP Address Mapping panel for SNAP protocol.

- You may globally enable or disable the mapping between the functional addresses and the group addresses in both directions. For example, to enable the mapping, issue the following command:

```
ASRT config>enable fa-ga-mapping
```

Note that fa-ga-mapping is enabled by default.

You can display the fa-ga-mapping setting using the List Bridge command.

For Nways MRS Configuration Program, use the the Bridging General panel to enable or disable fa-ga-mapping.

4.3.6 Configuration Commands for the Protocol Filtering

You may configure the IBM 2210 to discard received packets based on their protocol type. This can be done for a specific port or all the ports. The protocol filter allows you to filter the packets based on:

- SNAP
- Ether type
- DSAP

For example, to discard NetBIOS packets (SAP=F0) on port 1, you must issue the following command:

```
ASRT config>add prot-filter dsap f0
Filter packets arriving on all ports?(Yes or [No]): No
Filter packets arriving on port 1 - Yes or [No]: Yes
Filter packets arriving on port 2 - Yes or [No]: No
Filter packets arriving on port 3 - Yes or [No]: No
```

You can display the protocol filter for a specific port using the List Prot-Filter command.

In Nways MRS Configuration Program, the protocol filters can be configured using the Ethernet Filtering, DASP Filtering and SNAP Filtering panels available under the Protocol Filtering panel.

You may also configure the IBM 2210 to perform filtering based on the source and destination MAC address of the received packets. This can be done using the MAC filtering feature (MCF), which is described in 11.4, “MAC Filtering (MCF)” on page 566.

4.3.7 Configuration Commands for the Tunnel Bridging

Table 52 on page 133 shows the list of the commands that you may use to configure tunnel bridging for the IBM 2210. The *Nways MRS Protocol Configuration and Monitoring Reference*, SC30-3680-01, covers these commands in detail.

Note

Tunnel bridge configuration via Nways MRS Configuration Program is not supported. You must use Nways MRS via an ASCII console to customize the IBM 2210 for tunnel bridging.

<i>Table 52. Tunnel Configuration Commands</i>	
Command	Function
? (Help)	Lists all the tunnel configuration commands, or lists the options associated with specific commands.
Add	Adds the unicast IP address of destination bridges participating in an IP unicast addressing configuration for bridging over IP.
Delete	Deletes the unicast IP address of destination bridges participating in an IP unicast addressing configuration for bridging over IP.
Join	Allows the 2210 to join a peer-group, a client-group or a server-group to participate in an IP multicast addressing configuration for bridging over IP.
Leave	Allows the 2210 to leave a peer-group, a client-group or a server-group to participate in an IP multicast addressing configuration for bridging over IP.
List	Displays the IP addresses of endstations participating in an IP multicast and unicast addressing configuration for bridging over IP. Also displays the size (in number of bytes) of bridging packets being routed through an IP tunnel and whether or not multicast addressing is enabled or disabled.
Set	Sets a new multicast IP address used for the IP multicast addressing configuration for bridging over IP.
Exit	Exits the tunnel configuration process and returns to the ASRT configuration process.

To customize tunnel bridging for your IBM 2210, you may use the following commands:

- You must add the ports that are to perform tunnel bridging. For example, to configure port 3 to perform tunnel bridging, you must issue the following command:

```
ASRT config>add tunnel 3
```

Note

The IBM 2210 supports only one port for tunnel bridging.

Note that if you enable source routing on the tunnel port, you must also enter the segment number. You must also ensure that the IBM 2210 at the other end has enabled source routing on its tunnel port with the same segment number.

You may display the settings of the tunnel port using the List Bridge command.

- To access the tunnel bridge configuration, you must issue the following command:

```
ASRT config>tunnel
```

Then the new prompt becomes:

```
TNL config>
```

For a tunnel port, you must use the Add command to add the IP address of the bridge at the other end. The IP address at the other end may be a unicast remote IP address or a multicast IP address.

For unicast IP addressing, the tunneling configuration requires you to specify the IP address of the destination bridge. This address will be used by the IBM 2210 to convert the segment number in the routing information field (RIF)

in a source routed frame to the corresponding IP address of the destination bridge. For transparent bridging frames, the IP address identifies the other endpoint of the tunnel.

For multicast IP addressing, the tunneling configuration requires only the IP multicast address reserved for tunneling. Three groups of multicast addresses are used. The first group is for All Route Explorer (ARE) frames, the second group is for sending Spanning Tree Explorer (STE) frames, and the third group is for Specifically Routed Frames (SRF). Both unicast and multicast IP addresses could coexist for a port configured for tunnel bridging.

- For example, to add a unicast IP address of 9.67.46.131, where 9.67.46.131 is the IP address of the other end of the tunnel, issue the following command:

```
TNL config>add address 9.67.46.131
```

Both ends of a tunnel must issue the Add Address command to point to the opposite end of the tunnel.

Note: You can add more than one unicast IP address on your tunnel.

- To display the current tunnel configuration, you must issue the following command:

```
TNL config>list all
```

Note

When you have at least one unicast IP address customized, the IBM 2210 no longer shows you the multicast IP address.

- You may use the multicast IP address rather than unicast IP address(es). Or, you may use both unicast and multicast addressing at the same time. To use the multicast IP address, OSPF routing protocol is required. For more information about OSPF routing protocol see 7.4, “Open Shortest Path First (OSPF)” on page 305.

IBM 2210 supports only one multicast address per bridge. 224.186.0.0 multicast is defined by default. If you want to modify the multicast IP address, you may use the following example:

```
TNL config>set base-multicast-address 224.187.0.0
```

- Using multicast address, you must join one or more multicast group for bridging over IP.

The IBM 2210 supports use of the group membership function to allow it to dynamically discover the other end of the IP tunnel, instead of having to manually configure the remote IP addresses. This feature utilizes the Multicast OSPF (MOSPF) function, which is described in 8.1.5, “MOSPF” on page 335.

The group membership defines two types of group:

- Client/Server Group
- Peer-to-Peer Group

Client/server groups have members who are designated as either a client or a server. Server bridges only form tunnel connections with client routers. Each client server group has a group number assigned so you can use several client server groups with the same multicast IP address, either on the same or on different 2210s.

Peer-to-peer groups have members who are all designated peers. All members of a peer-to-peer group will form tunnel connections with all other members of the group. Each peer-to-peer group has a group number assigned so you can use several peer-to-peer groups with the same multicast IP address, either on the same or on different 2210s.

Group membership will only work between routers that support it, so a combination of group memberships and pre-configured defined remote IP addresses definitions may be required in your network.

If you use an X.25 or a frame relay serial link on one end of the multicast IP tunnel, care must be taken to configure the *internal IP address* with an IP address that does not belong to any other interface of the 2210. This is already required for all OSPF configurations because the X.25 and frame relay IP interface does not support Internet Group Management Protocol (IGMP) used for multicast OSPF (MOSPF).

To join peer-group 1, you must issue this command:

```
TNL config>join peer-group 1
```

The peer-group number must be in the decimal range 0-64. The other ends of the tunnel must join the same peer group 1 with the same multicast IP address. More than one peer group can be joined on the same IBM 2210.

To join client-group 2, you must issue this command:

```
TNL config>join client-group 2
```

The client-group number must be in the decimal range 0-64. The other ends of the tunnel must join the corresponding server-group 2, using the same multicast IP address, with this command:

```
TNL config>join server-group 2
```

The server-group number must be in the decimal range 0-64. More than one client or server group can be joined on the same IBM 2210. With the same multicast IP address in all your IBM 2210s, several IBM 2210s can join the same client group in order to reach one or more IBM 2210s that have joined the same server group.

- To exit the tunnel configuration, issue this command:

```
TNL config>exit
```

You will then come back to the ASRT configuration with this prompt:

```
ASRT config>
```

- To exit the ASRT configuration, issue this command:

```
ASRT config>exit
```

You will then come back to the CONFIG process with this prompt:

```
Config>
```

4.3.8 Configuration Commands for the TCP/IP Host Services

For Nways MRS via an ASCII Console, TCP/IP Host Services cannot be configured under ASRT (Bridging) protocol. For the IBM 2210, TCP/IP Host Services, which is known as protocol *hst*, can be accessed from the CONFIG process.

The TCP/IP Host Services allow you to assign an IP address to the IBM 2210 when it is configured as a bridge. This IP address can be used for management and maintenance purposes. For example, it will allow you to do the following:

- Manage the IBM 2210 using an SNMP manager
- Use TELNET to/from IBM 2210
- Download and upload IBM 2210 configuration using TFTP protocol
- Perform the TFTP neighbor boot function
- Use IP commands such as Ping and Traceroute to perform diagnosis

Table 53 shows you the TCP/IP Host Services commands. For more details about these commands, please refer to *Nways MRS Protocol Configuration and Monitoring Reference*, SC30-3680-01.

Table 53. TCP/IP Host Services Configuration Commands	
Command	Function
? (Help)	Lists all of the TCP/IP host configuration commands, or lists the options associated with specific commands.
Add	Adds a default gateway.
Delete	Deletes a default gateway.
Disable	Disables TCP/IP Host Services, router-discovery process, or RIP listening.
Enable	Enables TCP/IP Host Services, router-discovery process, or RIP listening.
List	Lists the TCP/IP Host Services configuration.
Set	Sets the IBM 2210's IP address.
Exit	Exits the TCP/IP Host Services configuration and returns to the CONFIG process.

- To access the TCP/IP Host Services, you must issue the following command:

Config>**protocol hst**

The following prompt will be displayed:

TCP/IP-Host config>

In Nways MRS Configuration Program, the TCP/IP Host Services parameters are in the TCP/IP Host Services panel.

- To enable the TCP/IP Host Services on your IBM 2210, you must issue the following command:

TCP/IP-Host config>**enable services**

Note that TCP/IP Host Services is enabled by default.

- To set the IP address of 9.67.46.131 with subnetmask 255.255.255.240, for your IBM 2210, issue the following command:

TCP/IP-Host config>**set address 9.67.46.131 255.255.255.240**

Note that the IBM 2210 can have only one IP address.

- To enable the learning of the default gateway through the reception of the ICMP router discovery messages, issue the following command:

TCP/IP-Host config>**enable router-discovery**

Router-discovery is enabled by default.

- To enable the building of the route table entries by listening to RIP messages, you must issue the following command:

TCP/IP-Host config>**enable rip-listening**

Enabling this will allow the IBM 2210 to build a routing table based on RIP messages broadcast by the routers in your network. But, the IBM 2210 will never send any RIP messages, as it is not an IP router in this case.

RIP-listening is disabled by default.

- To specify the router with the IP address of 9.67.46.132 to be used by the IBM 2210 as the default gateway, you must issue the following command:

TCP/IP-Host config>**add default-gateway 9.67.46.132**

- You can display the TCP/IP Host Services that are configured for your IBM 2210 using the List All command.
- To exit the TCP/IP Host Services and come back to the CONFIG process, you must issue this command:

TCP/IP-Host config>**exit**

The prompt becomes:

Config>

4.4 Bridging Scenarios and Configurations

This section provides some scenarios and configurations of the bridging methods explained above. These scenarios will test various bridging methods between two IBM 2210s and between an IBM 2210 and an IBM 6611 Network Processor.

All scenarios in this section, except the last one, have been performed with Nways MRS Program Version 1 Release 1 for the IBM 2210 and with IBM 6611 MPNP Program Version 1 Release 3 for the IBM 6611 Network Processor.

For every scenario, the Nways MRS customization information is provided for both the ASCII console commands and via Nways MRS Configuration program.

In these scenarios, we have assigned an IP address to each IBM 2210. This IP address corresponds to the TCP/IP host protocol. It allows the IBM 2210 to be managed via SNMP and maintained via the TFTP protocol. Setting this IP address does not allow the IBM 2210 to route the IP protocol.

Note

To configure TCP/IP Host Services, you must not have any IP address configured on the 2210 interfaces. That is, the IBM 2210 must not be configured as an IP router. The TCP/IP Host Services is only configured when the IBM 2210 is performing bridging functions only.

Note

When you use Nways MRS Configuration Program to configure your IBM 2210 and the IBM 2210 is configured as a bridge only (no IP routing), then you must either specify a valid IP address in the TCP/IP Host Services or disable TCP/IP Host Services (which is enabled by default). Otherwise, the IBM 2210 will not run your configuration and will enter a loop of reloading the IBM 2210.

When you use Nways MRS to customize your IBM 2210 for SRB, the internal segment is activated by default. This internal segment that is assigned the segment number 001 by default will add one extra hop to your network.

In the IBM 6611 Network Processor, a number of inbound source SAP filters are enabled by default on the token-ring interface. These filters discard the inbound All-Route Broadcast or Single Route Broadcast frames for the following SAPs:

- AA (SNAP format for any protocol)
- BC (Banyan)
- E0 (Novell IPX)

Because TCP/IP uses the SNAP format on token-ring LANs, in our scenarios we have removed the SAP AA (which is the SAP value for the SNAP format) from these filters in order to be able to bridge TCP/IP traffic.

Note

The following scenarios were in fact implemented using the Nways MRNS. There should be no difference in how to configure bridging using Nways MRS.

4.4.1 Scenario 1: STB Implementation

In this scenario, we have two 2210 Model 12Es, each with one Ethernet LAN interface and two serial interfaces. These 2210s are referred to as 2210A and 2210B.

Both 2210s are configured as pure transparent bridges. That is, STB is configured on both the Ethernet and serial 1 interfaces for both 2210s. We have assigned the IP address of 9.67.46.146 (subnet mask 255.255.255.240) to 2210A and 9.67.46.145 (subnet mask 255.255.255.240) to 2210B. The Serial 2 interface is not used in either 2210.

The serial link between the two 2210s is a PPP link connected to RS-232 modems.

Figure 45 shows the configuration of the network for this scenario. The customization parameters we used to test this scenario are shown in:

- Figure 46 on page 140 (2210A configuration via an ASCII console)
- Figure 47 on page 145 (2210A configuration via Nways MRS)

Configuration of the 2210B is not shown, as it is identical (except for the IP address) to the configuration of the 2210A.

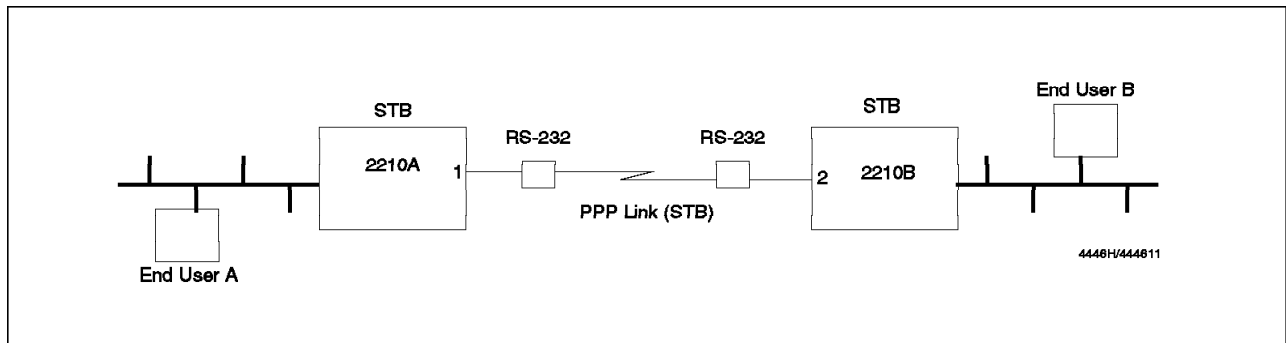


Figure 45. Scenario 1: STB Configuration with IBM 2210s

```

*
*talk 6 1

Config>network 0 2
Ethernet interface configuration
ETH config>list 3
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 1 4
Point-to-Point user configuration
PPP Config>list all 5

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>set hdlc cable rs-232 dte 6

:

```

Figure 46 (Part 1 of 5). Scenario 1: 2210A Customization via an ASCII Console

```

:
PPP Config>list all

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Config>disable interface 2      7
Config>list devices            8
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
      (Disabled)
Config>protocol asrt           9
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge      10

:

```

Figure 46 (Part 2 of 5). Scenario 1: 2210A Customization via an ASCII Console

```

:
ASRT config>list bridge 11

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  0       No. of Source routing segments: 0
SRB: Max ARE Hop cnt:  0           Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 1
Port Number:  1    Interface Number:  0 Port Behaviour: STB Only

ASRT config>add port 1 2 12
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: STB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  0       No. of Source routing segments: 0
SRB: Max ARE Hop cnt:  0           Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number:  1    Interface Number:  0 Port Behaviour: STB Only
Port Number:  2    Interface Number:  1 Port Behaviour: STB Only

ASRT config>exit
Config>protocol hst 13
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address 14
IP-Host address [0.0.0.0]? 9.67.46.146
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

:

```

Figure 46 (Part 3 of 5). Scenario 1: 2210A Customization via an ASCII Console

```

:
TCP/IP-Host config>list all      15

IP-Host IP address : 9.67.46.146
Address Mask       : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

TCP/IP-Host config>exit
Config>Ctrl+p
*restart      16
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
*talk 5      17

CGW Operator Console

+protocol asrt      18
ASRT>list bridge    19
Bridge ID (prio/add): 32768/00-00-93-80-80-D0
Bridge state:        Enabled
Bridge type:         STB
Bridge capability:   ASRT
Number of ports:     2
STP Participation:   IEEE802.1d

Port  Interface  State  MAC Address          Modes  Maximum
      1  Eth/0       Up    00-00-93-80-80-D0    T      MSDU   Segment
      2  PPP/0       Up    00-00-00-00-00-00    T      1514   1504

SR bridge number:    0
SR virtual segment:  000
Adaptive segment:    000

:

```

Figure 46 (Part 4 of 5). Scenario 1: 2210A Customization via an ASCII Console

```
:  
ASRT>exit  
+Ctrl+p  
*
```

Figure 46 (Part 5 of 5). Scenario 1: 2210A Customization via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Customization of the network number 0. This is the Ethernet LAN interface.
- 3** List the configuration of the Ethernet interface.
- 4** Customization of network 1. This is the serial 1 interface.
- 5** List the configuration of the serial 1 interface.
- 6** Specify that an RS-232 DTE cable is used.
- 7** Interface 2 is not used in this scenario.
- 8** List the configuration of devices (interfaces).
- 9** Access the bridging configuration.
- 10** Enable bridging at the box level.
- 11** List the configuration of the bridging function.
- 12** Add a port for serial 1 (interface 1) and assign port number 2 to it. This port is configured for STB by default.
- 13** Access the TCP/IP host configuration.
- 14** Assign an IP address to the 2210.
- 15** List the TCP/IP host configuration.
- 16** Restart the 2210 to get the configuration running.
- 17** The configuration is now running on the 2210. We access the CGW operator console to monitor the running configuration.
- 18** Access the bridge monitoring function.
- 19** List the status of the bridge. Note that both bridged interfaces are active.

```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 12E 2
  Select CONFIGURATION of Ethernet line
  ENABLE INTERFACE
  Select CONNECTOR TYPE
  Select AUTO-CONFIG 3
  Select IP ENCAPSULATION
  Select ETHERNET

Select the data-link protocol of Serial 1 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 1
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZ
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select RS-232 DTE 4
  Select subpanel LCP 5
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP 5
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP 5
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

```

⋮

Figure 47 (Part 1 of 3). Scenario 1: 2210A Customization via the Nways MRS Configuration Program

```

:
  Select CONFIGURATION of Serial 2
    On GENERAL subpanel :
      DISABLE INTERFACE 6

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 7
DISABLE DLSw

  In SOURCE ROUTING BRIDGE box
    BRIDGE NUMBER = 1
    MAXIMUM ARE HOP COUNT = 14
    MAXIMUM STE HOP COUNT = 14
    INTERNAL VIRTUAL SEGMENT = 1
    Select LF BIT INTERPRETATION
      Select EXTENDED
    ENABLE FA-GA

  In SOURCE ROUTING TRANSPARENT BRIDGE box
    DISABLE SR <--> TB CONVERSION

  In TRANSPARENT BRIDGE box
    FILT. DBASE SIZE = 2048
    AGING TIME = 300
    RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE ETHERNET 8
  Select CONFIGURE of Ethernet
    Select INTERFACE SUPPORTS
      Select STB 9
    Select DUPLICATE FRAMES
      Select STE&TSF
    SEGMENT NUMBER = 1

ENABLE SERIAL 1 10
  Select CONFIGURE of Serial 1
    Select INTERFACE SUPPORTS
      Select STB 11
    Select DUPLICATE FRAMES
      Select STE&TSF
    SEGMENT NUMBER = 1
    MTU UNIT = 4399
    ENABLE STE

:

```

Figure 47 (Part 2 of 3). Scenario 1: 2210A Customization via the Nways MRS Configuration Program


```

:
DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
ENABLE IP-HOST SERVICES
ENABLE ROUTER DISCOVERY
DISABLE RIP-LISTENING
IP-HOST ADDRESS = 9.67.46.146      12
IP-HOST MASK = 255.255.255.240
In DEFAULT GATEWAY IP ADDRESS
Nothing Customized

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION      13

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter STBBI      14
Select OK

```

Figure 47 (Part 3 of 3). Scenario 1: 2210A Customization via the Nways MRS Configuration Program

Notes:

- 1 Start the customization from an empty configuration.
- 2 This is a 2210 Model 12E with an Ethernet LAN interface, 4 MB of Flash, and 8 MB of RAM.
- 3 Allow the IBM 2210 to automatically determine which Ethernet connector is used.
- 4 Specify that an RS-232 DTE cable is used on serial 1.
- 5 This subpanel has not been changed. Default settings are used for all the parameters.
- 6 Interface 2 (serial 2) is not used in this scenario.
- 7 Enable bridging function at the box level.
- 8 Enable the Ethernet interface for bridging.
- 9 Enable transparent bridging on the Ethernet interface.
- 10 Enable the serial 1 interface for bridging.
- 11 Enable transparent bridging on the serial 1 interface.
- 12 Set an IP address for the IBM 2210

13 Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.

15 The name of the configuration file stored in your workstation.

4.4.2 Scenario 2: STB Interoperability with the 6611

In this scenario, we have a 2210 Model 12E with an Ethernet LAN, and a 6611 Model 170 with another Ethernet LAN.

The 2210 and the 6611 are connected to each other over a PPP link via a pair of V.35 modems. Both the 6611 and the 2210 are configured for STB (transparent bridging) over their respective Ethernet LANs and the PPP link.

For the 2210, serial 2 interface is not used.

Figure 48 shows the configuration of the network used in this scenario.

The customization parameters we used to test this scenario are shown in:

- Figure 49 on page 150 (2210 configuration via an ASCII console)
- Figure 50 on page 155 (2210 configuration via Nways MRS)
- Figure 51 on page 159 (6611 configuration via IBM 6611 MPNP)

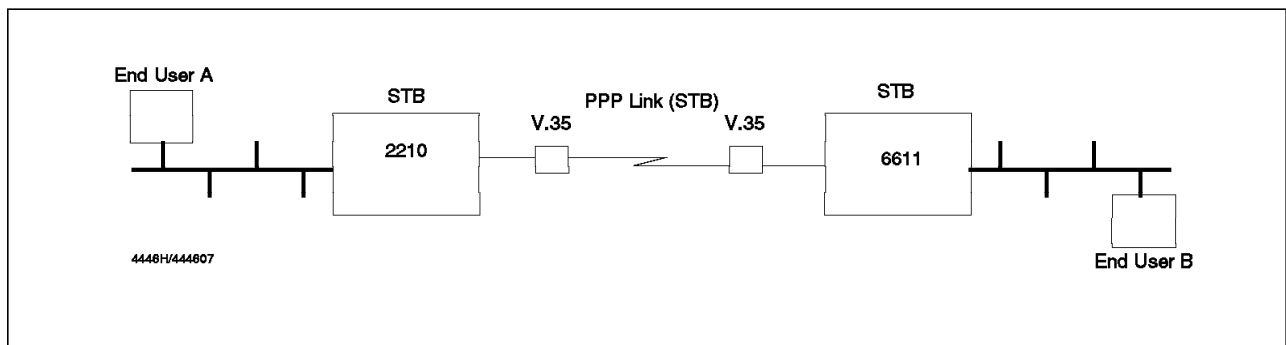


Figure 48. Scenario 2: STB Configuration between the IBM 2210 and the IBM 6611 Network Processor

```

*
*talk 6 1

Config>network 0 2
Ethernet interface configuration
ETH config>list 3
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 1 4
Point-to-Point user configuration
PPP Config>list all 5

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>set hdlc encoding nrzi 6
PPP Config>set hdlc cable v35 dte 7

:

```

Figure 49 (Part 1 of 5). Scenario 2: 2210 Customization via an ASCII Console

```

:
PPP Config>list all

Maximum frame size in bytes = 2048
Encoding: NRZI
Idle State: Flag
Clocking: External
Cable type: V.35 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Config>disable interface 2      8
Config>list devices            9
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
      (Disabled)
Config>protocol asrt           10
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge      11

:

```

Figure 49 (Part 2 of 5). Scenario 2: 2210 Customization via an ASCII Console

```

:
ASRT config>list bridge 12

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  0      No. of Source routing segments: 0
SRB: Max ARE Hop cnt:  0          Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE      Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 1
Port Number:  1    Interface Number:  0 Port Behaviour: STB Only

ASRT config>add port 1 2 13
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: STB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  0      No. of Source routing segments: 0
SRB: Max ARE Hop cnt:  0          Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE      Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number:  1    Interface Number:  0 Port Behaviour: STB Only
Port Number:  2    Interface Number:  1 Port Behaviour: STB Only

ASRT config>exit
Config>protocol hst 14
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address 15
IP-Host address [0.0.0.0]? 9.67.46.145
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

```

Figure 49 (Part 3 of 5). Scenario 2: 2210 Customization via an ASCII Console

```

:
TCP/IP-Host config>list all      16

IP-Host IP address : 9.67.46.145
Address Mask       : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

TCP/IP-Host config>exit
Config>Ctrl+p
*restart      17
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
*talk 5      18

CGW Operator Console

+protocol asrt      19
ASRT>list bridge    20
Bridge ID (prio/add): 32768/00-00-93-80-80-D0
Bridge state:      Enabled
Bridge type:      STB
Bridge capability: ASRT
Number of ports:   2
STP Participation: IEEE802.1d

Port  Interface  State  MAC Address          Modes  Maximum
      1  Eth/0       Up    00-00-93-80-80-D0    T      MSDU   Segment
      2  PPP/0       Up    00-00-00-00-00-00    T      1514   1504

SR bridge number:    0
SR virtual segment:  000
Adaptive segment:    000

:

```

Figure 49 (Part 4 of 5). Scenario 2: 2210 Customization via an ASCII Console

```
⋮  
ASRT>exit  
+Ctrl+p  
*
```

Figure 49 (Part 5 of 5). Scenario 2: 2210 Customization via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Customization of an Ethernet LAN interface (interface 0).
- 3** List the configuration for the Ethernet interface.
- 4** Customization of serial 1 link (interface 1).
- 5** List the configuration of serial 1.
- 6** This is required, because the default encoding on IBM 6611 Network Processor is NRZI.
- 7** Specify that a V.35 DTE cable is used.
- 8** This interface is not used in our scenario.
- 9** List the configuration of devices (interfaces).
- 10** Access the bridging configuration.
- 11** Enable bridging at the box level.
- 12** List the bridging configuration.
- 13** Add a port for the serial 1 interface (interface 1). Port number 2 is assigned to this port. By default, this port is enabled for STB.
- 14** Access the TCP/IP host configuration.
- 15** Set an IP address at box level for the 2210.
- 16** List the TCP/IP host configuration.
- 17** Restart the 2210 to get the configuration running.
- 18** The configuration is now running on the 2210. We access the CGW operator console to monitor the running configuration.
- 19** Access the bridge monitoring function.
- 20** List the bridge configuration. Note that both bridge interfaces are active.


```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 12E 2
  Select CONFIGURATION of Ethernet line
  ENABLE INTERFACE
  Select CONNECTOR TYPE
  Select AUTO-CONFIG 3
  Select IP ENCAPSULATION
  Select ETHERNET

Select the data-link protocol of Serial 1 (PPP by default)
Select PPP

Select CONFIGURATION of Serial 1
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZI 4
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select V35 DTE 5
  Select subpanel LCP 6
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP 6
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP 6
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

```

⋮

Figure 50 (Part 1 of 3). Scenario 2: 2210 Customization via the Nways MRS Configuration Program

```

:
  Select CONFIGURATION of Serial 2
    On GENERAL subpanel :
      DISABLE INTERFACE 7

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 8
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 1
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 1
  Select LF BIT INTERPRETATION
    Select EXTENDED
  ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
  DISABLE SR <-> TB CONVERSION

In TRANSPARENT BRIDGE box
  FILT. DBASE SIZE = 2048
  AGING TIME = 300
  RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE ETHERNET 9
  Select CONFIGURE of Ethernet
    Select INTERFACE SUPPORTS
      Select STB 10
    Select DUPLICATE FRAMES
      Select STE&TSF
    SEGMENT NUMBER = 1

ENABLE SERIAL 1 11
  Select CONFIGURE of Serial 2
    Select INTERFACE SUPPORTS
      Select STB 12
    Select DUPLICATE FRAMES
      Select STE&TSF
    SEGMENT NUMBER = 1
    MTU UNIT = 4399
    ENABLE STE

:

```

Figure 50 (Part 2 of 3). Scenario 2: 2210 Customization via the Nways MRS Configuration Program

```

:
DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
ENABLE IP-HOST SERVICES
ENABLE ROUTER DISCOVERY
DISABLE RIP-LISTENING
IP-HOST ADDRESS = 9.67.46.145      13
IP-HOST MASK = 255.255.255.240
In DEFAULT GATEWAY IP ADDRESS
Nothing Customized

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION      14

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter STBBI      15
Select OK

```

Figure 50 (Part 3 of 3). Scenario 2: 2210 Customization via the Nways MRS Configuration Program

Notes:

- 1 Start the customization from an empty configuration.
- 2 This is a 2210 Model 12E with an Ethernet LAN interface, 4 MB of Flash, and 8 MB of RAM.
- 3 This allows the 2210 to automatically determine the connector used on the Ethernet interface.
- 4 Default encoding of the 6611 for the serial link is NRZI.
- 5 Specify the type of cable used on the serial 1 interface.
- 6 This subpanel has not been changed. Default values are used for all the parameters.
- 7 This interface 2 is not used in this scenario.
- 8 Enable bridging function at the box level.
- 9 Enable the Ethernet interface for bridging.
- 10 Enable transparent bridging on the Ethernet interface.
- 11 Enable the serial 1 interface for bridging.
- 12 Enable transparent bridging on the serial 1 interface.

- 13** Set an IP address at box level.
- 14** Create the configuration file that will be loaded into the 2210 via TFTP.
- 15** This is the name of the configuration file stored on the workstation.

```

Select ETHERNET ADAPTER CONFIGURATION
  Enable PHYSICAL INTERFACE 1

  Select PHYSICAL INTERFACE CONFIGURATION
    Select UNIVERSALLY ADMINISTERED ADDRESS 2

  Enable TRANSPARENT BRIDGE 3

  Select TRANSPARENT BRIDGE
    SPANNING TREE MODE = AUTOMATIC

Select SERIAL ADAPTER CONFIGURATION

  Select PPP
    Enable PHYSICAL INTERFACE 4

    Select PHYSICAL INTERFACE CONFIGURATION
      INTERFACE CABLE = V35, V36, or EIA232 5
      TRANSMIT CLOCK SOURCE = DCE
      DATA ENCODING = NRZI 6

    Enable PPP CONFIGURATION 7

    Enable TRANSPARENT BRIDGE 8

    Select TRANSPARENT BRIDGE
      SPANNING TREE MODE = AUTOMATIC

Select NODE CONFIGURATION
  Enable TRANSPARENT BRIDGING 9

```

Figure 51. Scenario 2: 6611 Customization via the IBM 6611 MPNP Configuration Program

Notes:

- 1 Enable the Ethernet interface.
- 2 Select UAA MAC address for the Ethernet card.
- 3 Enable transparent bridging on the Ethernet interface.
- 4 Enable the serial interface.
- 5 Specify the type of cable used on this interface.
- 6 NRZI encoding is the default.
- 7 Enable the PPP configuration for the serial interface.
- 8 Enable transparent bridging for the serial interface.
- 9 Enable transparent bridging at the box level.

4.4.3 Scenario 3: SRB Implementation

In this scenario, we have two 2210 Model 12Ts, each with one token-ring LAN interface and two serial interfaces. These 2210s are referred to as 2210A and 2210B.

Both 2210s are configured as pure source route bridges. That is, SRB is configured on both the token-ring and serial 1 interfaces for both 2210s. We have assigned the IP address of 9.67.46.146 (subnet mask 255.255.255.240) to 2210A and 9.67.46.145 (subnet mask 255.255.255.240) to 2210B. The Serial 2 interface is not used in either 2210.

The serial link between the two 2210s is a PPP link connected to RS-232 modems and has the segment number FF1.

The 2210A token-ring interface has the segment number FF0. The bridge number of 2210A is 1. The locally administered address of the 2210A token-ring interface is 40002210A001.

The 2210B token-ring interface has the segment number FF2. The bridge number of 2210B is 2. The locally administered address of the 2210B token-ring interface is 40002210B002.

Figure 52 shows the configuration of the network for this scenario. The customization parameters that we used to test this scenario are shown in:

- Figure 53 on page 161 (2210A configuration via an ASCII console)
- Figure 55 on page 172 (2210A configuration via Nways MRS)
- Figure 54 on page 167 (2210B configuration via an ASCII console)
- Figure 56 on page 176 (2210B configuration via Nways MRS)

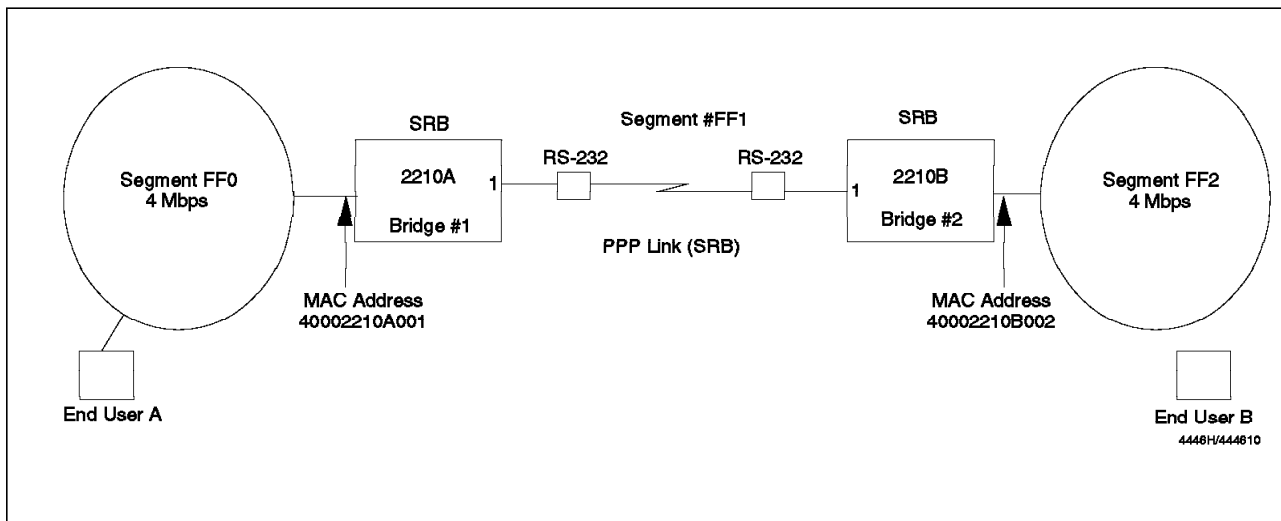


Figure 52. Scenario 3: SRB Configuration between IBM 2210s

```

*
*talk 6 1

Config>list devices 2
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>network 0 3
Token-Ring interface configuration
TKR config>list 4
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Shielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 000000000000
IPX interface configuration record missing
This message is normal in the system.
TKR config>media unshielded 5
TKR config>set physical-address 40:00:22:10:A0:01 6
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Unshielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 7
Point-to-Point user configuration
PPP Config>list hdlc 8

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>set hdlc cable rs-232 dte 9

:

```

Figure 53 (Part 1 of 5). Scenario 3: 2210A Customization via an ASCII Console

```

:
PPP Config>list all 10

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:           20   CONFIG Nak Tries:           10
Terminate Tries:               10   Retry Timer:               3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:           20   CONFIG Nak Tries:           10
Terminate Tries:               10   Retry Timer:               3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Config>disable interface 2 11
Config>list devices
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
               (Disabled)
Config>protocol asrt 12
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 13

:

```

Figure 53 (Part 2 of 5). Scenario 3: 2210A Customization via an ASCII Console


```

:
ASRT config>list bridge 14

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: DISABLED
Number of ports added: 1
Port Number: 1    Interface Number: 0 Port Behaviour: STB Only

ASRT config>disable transparent 15
Port Number [1]? 1
ASRT config>enable source-routing 16
Port Number [1]? 1
Segment Number for the port in hex(1 - FFF) [1]? FF0
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>add port 17
Interface Number [0]? 1
Port Number [2]? 2
ASRT config>disable transparent 18
Port Number [1]? 2
ASRT config>enable source-routing 19
Port Number [1]? 2
Segment Number for the port in hex(1 - FFF) [1]? FF1
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: SRB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 1        No. of Source routing segments: 2
SRB: Max ARE Hop cnt: 14                Max STE Hop cnt: 14
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IBM-SRB proprietary
DLS for the bridge: DISABLED
Number of ports added: 2
Port Number: 1    Interface Number: 0 Port Behaviour: SRB Only
Port Number: 2    Interface Number: 1 Port Behaviour: SRB Only

ASRT config>exit

:

```

Figure 53 (Part 3 of 5). Scenario 3: 2210A Customization via an ASCII Console

```

:
Config>protocol hst 20
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address 21
IP-Host address [0.0.0.0]? 9.67.46.146
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

TCP/IP-Host config>list all 22

IP-Host IP address : 9.67.46.146
Address Mask      : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

TCP/IP-Host config>exit
Config>Ctrl+p
*restart 23
Are you sure you want to restart the gateway? (Yes or [No]): Yes


Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 24

CGW Operator Console

:

```

Figure 53 (Part 4 of 5). Scenario 3: 2210A Customization via an ASCII Console

```

:
+protocol asrt 25
ASRT>list bridge 26
Bridge ID (prio/add): 32768/02-00-44-08-05-80
Bridge state: Enabled
Bridge type: SRB
Bridge capability: ASRT
Number of ports: 2
STP Participation: IBM-SRB proprietary

Port Interface State MAC Address Modes Maximum MSDU Segment
  1 TKR/0 Up 02-00-44-08-05-80 SR 2096 FF0
  2 PPP/0 Up 00-00-00-00-00-00 SR 1504 FF1

SR bridge number: 1
SR virtual segment: 000
Adaptive segment: 000
ASRT>exit
+Ctrl+p
*
```

Figure 53 (Part 5 of 5). Scenario 3: 2210A Customization via an ASCII Console

Notes:

- 1 Talk to the CONFIG process.
- 2 List the configuration of devices (interfaces).
- 3 Customization of the network number 0. This is the token-ring LAN interface.
- 4 List the configuration of the token-ring interface.
- 5 The 2210 is connected to the token-ring LAN via a UTP cable. Default is STP.
- 6 This is the locally administered address of the token-ring interface.
- 7 Customization of network 1. This is the serial 1 interface.
- 8 List the configuration of HDLC parameters for serial 1 interface.
- 9 Specify that an RS-232 DTE cable is used.
- 10 List the configuration of serial 1.
- 11 Interface 2 is not used in this scenario.
- 12 Access the bridging configuration.
- 13 Enable the bridging function at the box level.
- 14 List the bridging configuration.
- 15 Disable transparent bridging (STB) on the token-ring interface.

- 16** Enable source route bridging (SRB) on the token-ring interface. Assign the segment number FF0 to the token-ring segment, and assign the bridge number 1 to the 2210.
- 17** Add a bridging port for the serial 1 interface (interface 1). The port number is 2.
- 18** Disable transparent bridging (STB) on the serial 1 interface.
- 19** Enable source route bridging (SRB) on the serial 1 interface. Assign the segment number FF1 to the serial interface. This is the same segment number assigned to the serial interface on the 2210B.
- 20** Access the TCP/IP host configuration.
- 21** Set an IP address at the box level.
- 22** List the TCP/IP host configuration.
- 23** Restart the 2210 to get the configuration running.
- 24** The configuration is now running on the 2210. We access the CGW operator console to monitor the running configuration.
- 25** Access the bridge monitoring function.
- 26** List the bridge configuration. Note that both interfaces are active.

```

*
*talk 6 1

Config>list devices 2
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>network 0 3
Token-Ring interface configuration
TKR config>list 4
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Shielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 000000000000
IPX interface configuration record missing

TKR config>media unshielded 5
TKR config>set physical-address 40:00:22:10:B0:02 6
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Unshielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 40002210B002
IPX interface configuration record missing

TKR config>exit
Config>network 1 7
Point-to-Point user configuration
PPP Config>list hdlc 8

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>set hdlc cable rs-232 dte 9

:

```

Figure 54 (Part 1 of 4). Scenario 3: 2210B Customization via an ASCII Console

```

:
PPP Config>list all 10

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:           20   CONFIG Nak Tries:           10
Terminate Tries:                10   Retry Timer:                3000

LCP Options
-----
Max Receive Unit:               2048   Magic Number:               Yes

NCP Parameters
-----
CONFIG Request Tries:           20   CONFIG Nak Tries:           10
Terminate Tries:                10   Retry Timer:                3000

IPCP Options
-----
IPCP Compression:               None
IP Address:                     Don't Send or Request
PPP Config>exit
Config>disable interface 2 11
Config>list devices
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
               (Disabled)
Config>protocol asrt 12
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 13
:

```

Figure 54 (Part 2 of 4). Scenario 3: 2210B Customization via an ASCII Console

```

:
ASRT config>list bridge 14

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  0      No. of Source routing segments: 0
SRB: Max ARE Hop cnt:  0          Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 1
Port Number:  1    Interface Number:  0 Port Behaviour: STB Only

ASRT config>disable transparent 15
Port Number [1]? 1
ASRT config>enable source-routing 16
Port Number [1]? 1
Segment Number for the port in hex(1 - FFF) [1]? FF2
Bridge number in hex (1 - 9, A - F) [1]? 2
ASRT config>add port 17
Interface Number [0]? 1
Port Number [2]? 2
ASRT config>disable transparent 18
Port Number [1]? 2
ASRT config>enable source-routing 19
Port Number [1]? 2
Segment Number for the port in hex(1 - FFF) [1]? FF1
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: SRB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  1      No. of Source routing segments: 2
SRB: Max ARE Hop cnt:  14          Max STE Hop cnt: 14
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IBM-SRB proprietary
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number:  1    Interface Number:  0 Port Behaviour: SRB Only
Port Number:  2    Interface Number:  1 Port Behaviour: SRB Only

ASRT config>exit

:

```

Figure 54 (Part 3 of 4). Scenario 3: 2210B Customization via an ASCII Console

```

:
Config>protocol hst 20
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address 21
IP-Host address [0.0.0.0]? 9.67.46.145
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

TCP/IP-Host config>list all 22

IP-Host IP address : 9.67.46.145
Address Mask      : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

TCP/IP-Host config>exit
Config>Ctrl+p
*restart 23
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*

```

Figure 54 (Part 4 of 4). Scenario 3: 2210B Customization via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** List the configuration of devices (interfaces).
- 3** Customization of the network number 0. This is the token-ring LAN interface.
- 4** List the configuration for the token-ring interface.
- 5** The 2210 is connected to the token-ring LAN via a UTP cable. The default is STP.
- 6** This is the locally administered address of the token-ring interface.
- 7** Customization of network 1. This is the serial 1 interface.

- 8** List the configuration of HDLC parameters for the serial 1 interface.
- 9** Specify that an RS-232 DTE cable is used.
- 10** List the configuration of serial 1.
- 11** Interface 2 is not used in this scenario.
- 12** Access the bridging configuration.
- 13** Enable bridging functionality at the box level.
- 14** List the bridging configuration.
- 15** Disable transparent bridging (STB) on the token-ring interface.
- 16** Enable source route bridging (SRB) on the token-ring interface. Assign the segment number FF2 to the token-ring segment, and assign the bridge number 2 to the 2210.
- 17** Add a bridging port for the serial 1 interface (interface 1). The port number is 2.
- 18** Disable transparent bridging (STB) on the serial 1 interface.
- 19** Enable source route bridging (SRB) on the serial 1 interface. Assign the segment number FF1 to the serial interface. This is the same segment number assigned to the serial interface on the 2210A.
- 20** Access the TCP/IP host configuration.
- 21** Set an IP address at box level.
- 22** List the TCP/IP host configuration.
- 23** Restart the 2210 to get the configuration running.

```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 12T 2
  Select CONFIGURATION of Token-Ring line
  ENABLE INTERFACE
  MAC ADDRESS = 40002210A001 3
  Select SPEED
  Select 4
  Select PACKET SIZE
  Select 2052
  Select CABLE TYPE
  Select UTP 4
  RIF TIMER = 120
  DISABLE END NODE SOURCE ROUTING

Select the data-link protocol of Serial 1 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 1
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZ
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select RS-232 DTE 5
  Select subpanel LCP 6
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP 6
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP 6
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

  :

```

Figure 55 (Part 1 of 3). Scenario 3: 2210A Customization via the Nways MRS Configuration Program

```

:
  Select CONFIGURATION of Serial 2
    On GENERAL subpanel :
      DISABLE INTERFACE 7

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 8
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 1 9
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 1
  Select LF BIT INTERPRETATION
    Select EXTENDED
  ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
  DISABLE SR <--> TB CONVERSION

In TRANSPARENT BRIDGE box
  FILT. DBASE SIZE = 2048
  AGING TIME = 300
  RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE Token-Ring 10
Select CONFIGURE of Token-Ring
  Select INTERFACE SUPPORTS
    Select SRB 11
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = FF0 12
  MTU UNIT = 4399
  ENABLE STE

ENABLE SERIAL 1 13
Select CONFIGURE of Serial 2
  Select INTERFACE SUPPORTS
    Select SRB 14
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = FF1 15
  MTU UNIT = 4399
  ENABLE STE

:

```

Figure 55 (Part 2 of 3). Scenario 3: 2210A Customization via the Nways MRS Configuration Program

```

:
DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
ENABLE IP-HOST SERVICES
ENABLE ROUTER DISCOVERY
DISABLE RIP-LISTENING
IP-HOST ADDRESS = 9.67.46.146      16
IP-HOST MASK = 255.255.255.240
In DEFAULT GATEWAY IP ADDRESS
Nothing Customized

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION      17

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter SRBA2      18
Select OK

```

Figure 55 (Part 3 of 3). Scenario 3: 2210A Customization via the Nways MRS Configuration Program

Notes:

- 1 Start the customization from an empty configuration.
- 2 This is a 2210 Model 12T with a token-ring interface, 4 MB of Flash, and 8 MB of RAM.
- 3 This is the locally administered address of the token-ring interface.
- 4 The 2210 is connected to the token-ring LAN using the UTP connector. The default is STP.
- 5 Specify that an RS-232 DTE cable is used for serial 1.
- 6 This subpanel has not been changed. Default settings are used for all the parameters.
- 7 Interface 2 is not used in this scenario.
- 8 Enable bridging function at the box level.
- 9 The bridge number of 2210 is 1.
- 10 Enable the token-ring interface for bridging.
- 11 Enable source route bridging on the token-ring interface.
- 12 This is the segment number of the token-ring LAN interface.

- 13** Enable the serial 1 interface for bridging.
- 14** Enable source route bridging on the serial 1 interface.
- 15** This is the segment number of the serial link interface.
- 16** Set an IP address at box level.
- 17** Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.
- 18** This is the name of the configuration file stored in your workstation.

```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 2
  Select CONFIGURATION of Token-Ring line
  ENABLE INTERFACE
  MAC ADDRESS = 40002210B002 3
  Select SPEED
  Select 4
  Select PACKET SIZE
  Select 2052
  Select CABLE TYPE
  Select UTP 4
  RIF TIMER = 120
  DISABLE END NODE SOURCE ROUTING

Select the data-link protocol of Serial 1 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 1
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZ
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select RS-232 DTE 5
  Select subpanel LCP 6
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP 6
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP 6
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

  :

```

Figure 56 (Part 1 of 3). Scenario 3: 2210B Customization via the Nways MRS Configuration Program

```

:
  Select CONFIGURATION of Serial 2
    On GENERAL subpanel :
      DISABLE INTERFACE 7

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 8
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 2 9
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 2 10
  Select LF BIT INTERPRETATION
    Select EXTENDED
  ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
  DISABLE SR <=> TB CONVERSION

In TRANSPARENT BRIDGE box
  FILT. DBASE SIZE = 2048
  AGING TIME = 300
  RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE Token-Ring 11
Select CONFIGURE of Token-Ring
  Select INTERFACE SUPPORTS
    Select SRB 12
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = FF2 13
  MTU UNIT = 4399
  ENABLE STE

ENABLE SERIAL 1 14
Select CONFIGURE of Serial 2
  Select INTERFACE SUPPORTS
    Select SRB 15
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = FF1 16
  MTU UNIT = 4399
  ENABLE STE
:

```

Figure 56 (Part 2 of 3). Scenario 3: 2210B Customization via the Nways MRS Configuration Program

```

:
DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
ENABLE IP-HOST SERVICES
ENABLE ROUTER DISCOVERY
DISABLE RIP-LISTENING
IP-HOST ADDRESS = 9.67.46.145      17
IP-HOST MASK = 255.255.255.240
In DEFAULT GATEWAY IP ADDRESS
Nothing Customized

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION      18

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter SRBB2      19
Select OK

```

Figure 56 (Part 3 of 3). Scenario 3: 2210B Customization via the Nways MRS Configuration Program

Notes:

- 1 Start the customization from an empty configuration.
- 2 This is a 2210 Model 12T with a token-ring interface, 4 MB of Flash, and 8 MB of RAM.
- 3 This is the locally administered address of the token-ring interface.
- 4 The 2210 is connected to the token-ring LAN using the UTP connector. The default is STP.
- 5 Specify that an RS-232 DTE cable is used for serial 1.
- 6 This subpanel has not been changed. Default settings are used for all the parameters.
- 7 Interface 2 is not used in this scenario.
- 8 Enable bridging function at the box level.
- 9 The bridge number of 2210 is 2.
- 10 With the Nways MRS Configuration program, using SRB will automatically enable the internal virtual segment. As the default internal segment 1 is already used by 2210A, we specified an unused segment number (2) for the internal segment.
- 11 Enable the token-ring interface for bridging.

- 12** Enable source route bridging on the token-ring interface.
- 13** This is the segment number of the token-ring LAN interface.
- 14** Enable the serial 1 interface for bridging.
- 15** Enable source route bridging on the serial 1 interface.
- 16** This is the segment number of the serial link interface.
- 17** Set an IP address at box level.
- 18** Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.
- 19** This is the name of the configuration file stored in your workstation.

4.4.4 Scenario 4: SRB Interoperability with the IBM 6611 Network Processor

In this scenario, we have a 2210 Model 12T with a token-ring LAN, and a 6611 Model 170 with another token-ring LAN.

The 2210 and the 6611 are connected to each other over a PPP link via a pair of V.35 modems. Both the 6611 and the 2210 are configured for SRB (Source Route Bridging) over their respective token-ring LANs and the PPP link.

For the 2210, the Serial 2 interface is not used.

Figure 57 shows the configuration of the network used in this scenario.

The customization parameters we used to test this scenario are shown in:

- Figure 58 on page 181 (2210 configuration via an ASCII console)
- Figure 59 on page 190 (2210 configuration via Nways MRS)
- Figure 60 on page 194 (6611 configuration via IBM 6611 MPNP)

The 2210 token-ring LAN interface is attached to the segment number FF0 and the bridge number of 2210 is 1. The locally administered address of the 2210 token-ring interface is 40002210A001. We have assigned the IP address of 9.67.46.146 (subnet mask is 255.255.255.240).

The 6611 token-ring LAN interface is attached to the segment number FF2 and the bridge number of 6611 is 2. The locally administered address of the 6611 token-ring interface is 40006611B001.

The segment number for the PPP link is FF1.

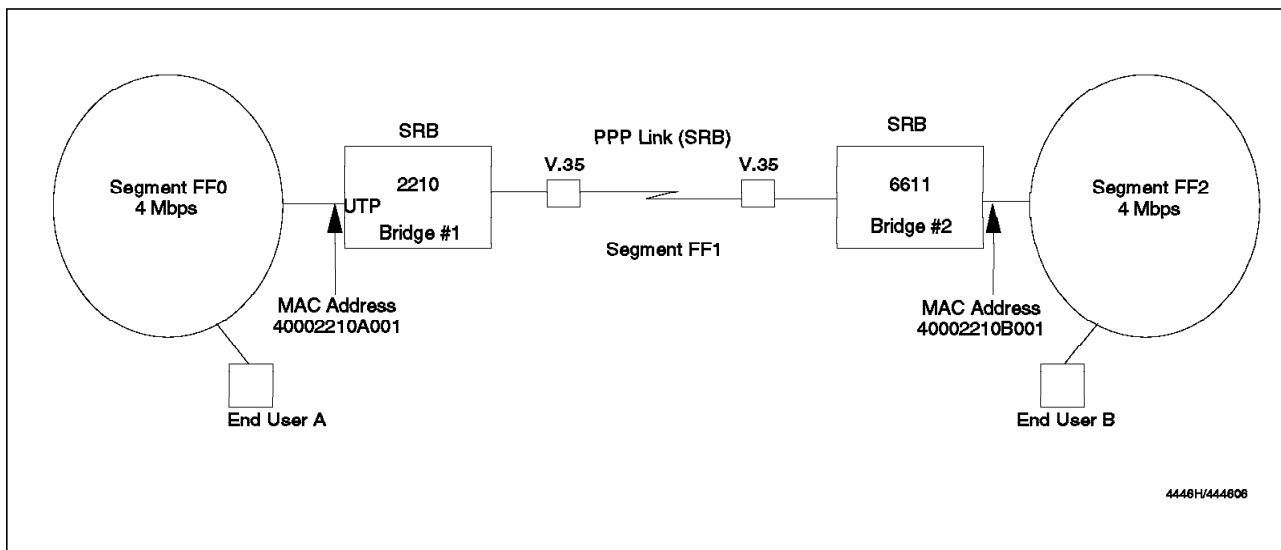


Figure 57. Scenario 4: SRB Configuration between the IBM 2210 and the IBM 6611 Network Processor

```

*
*talk 6 1

Config>list devices 2
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>network 0 3
Token-Ring interface configuration
TKR config>list 4
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Shielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 000000000000
IPX interface configuration record missing

TKR config>media unshielded 5
TKR config>set physical-address 40:00:22:10:A0:01 6
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Unshielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 7
Point-to-Point user configuration
PPP Config>list hdlc 8

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>set hdlc encoding nrzi 9
PPP Config>set hdlc cable V35 dte 10

:

```

Figure 58 (Part 1 of 8). Scenario 4: 2210 Customization via an ASCII Console

```

:
PPP Config>list all 11

Maximum frame size in bytes = 2048
Encoding: NRZI
Idle State: Flag
Clocking: External
Cable type: V.35 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:           20   CONFIG Nak Tries:           10
Terminate Tries:               10   Retry Timer:               3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:           20   CONFIG Nak Tries:           10
Terminate Tries:               10   Retry Timer:               3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Config>disable interface 2 12
Config>list devices
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
               (Disabled)
Config>protocol asrt 13
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 14

:

```

Figure 58 (Part 2 of 8). Scenario 4: 2210 Customization via an ASCII Console

```

:
ASRT config>list bridge 15

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  0      No. of Source routing segments: 0
SRB: Max ARE Hop cnt:  0          Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 1
Port Number:  1    Interface Number:  0 Port Behaviour: STB Only

ASRT config>disable transparent 16
Port Number [1]? 1
ASRT config>enable source-routing 17
Port Number [1]? 1
Segment Number for the port in hex(1 - FFF) [1]? FF0
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>add port 18
Interface Number [0]? 1
Port Number [2]? 2
ASRT config>disable transparent 19
Port Number [1]? 2
ASRT config>enable source-routing 20
Port Number [1]? 2
Segment Number for the port in hex(1 - FFF) [1]? FF1
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: SRB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  1      No. of Source routing segments: 2
SRB: Max ARE Hop cnt:  14          Max STE Hop cnt: 14
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IBM-SRB proprietary
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number:  1    Interface Number:  0 Port Behaviour: SRB Only
Port Number:  2    Interface Number:  1 Port Behaviour: SRB Only

ASRT config>exit

:

```

Figure 58 (Part 3 of 8). Scenario 4: 2210 Customization via an ASCII Console

```

:
Config>protocol hst 21
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address 22
IP-Host address [0.0.0.0]? 9.67.46.146
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

TCP/IP-Host config>list all 23

IP-Host IP address : 9.67.46.146
Address Mask      : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

TCP/IP-Host config>exit
Config>Ctrl+p
*restart 24
Are you sure you want to restart the gateway? (Yes or [No]): Yes


Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 25

CGW Operator Console

:

```

Figure 58 (Part 4 of 8). Scenario 4: 2210 Customization via an ASCII Console

```

:
+protocol asrt 26
ASRT>list bridge 27
Bridge ID (prio/add): 32768/02-00-44-08-05-80
Bridge state: Enabled
Bridge type: SRB
Bridge capability: ASRT
Number of ports: 2
STP Participation: IBM-SRB proprietary

Port Interface State MAC Address Modes Maximum MSDU Segment
1 TKR/0 Up 02-00-44-08-05-80 SR 2096 FF0
2 PPP/0 Up 00-00-00-00-00-00 SR 1504 FF1

SR bridge number: 1
SR virtual segment: 000
Adaptive segment: 000
ASRT>exit
+network 1 28
Point-to-Point Console
PPP>list all 29

Version: 1
LCP State: Open
Previous State: Ack Rcvd
Time Since Change: 59 minutes and 1 second

LCP Option Local Remote
-----
Max Receive Unit: 1500 1500
Async Char Mask: FFFFFFFF FFFFFFFF
Authentication: None None
Magic Number: 24373E5 None
Protocol Compr: No No
Addr/Cntl Compr: No No
32-Bit Checksum: No No

IPCP State: Listen
Previous State: Closed
Time Since Change: 59 minutes and 10 seconds

IPCP Option Local Remote
-----
IP Address 0.0.0.0 None
Compression Slots None None

:

```

Figure 58 (Part 5 of 8). Scenario 4: 2210 Customization via an ASCII Console

:

DNCP State: Closed
Previous State: Closed
Time Since Change: 59 minutes and 11 seconds

No IPX control protocol information available

BNCP State: Open
Previous State: Ack Rcvd
Time Since Change: 59 minutes and 9 seconds

BNCP Option	Local	Remote
-----	-----	-----
Tinygram Compression	DISABLED	DISABLED

Source-route Info:	Local Bridge#	Remote Bridge#	Line ID
	1	2	FF1

ATCP State: Listen
Previous State: Req Sent
Time Since Change: 58 minutes and 10 seconds

AppleTalk Address Info:
Common network number = 0
Local node ID = 0
Remote node ID = 0
No OSI control protocol information available

LCP Statistic	In	Out
-----	--	---
Packets:	6	6
Octets:	196	196
Cfg Req:	0	0
Cfg Ack:	0	0
Cfg Nak:	0	0
Cfg Rej:	0	0
Term Req:	0	0
Term Ack:	0	0
Echo Req:	2	4
Echo Resp:	4	2
Disc Req:	0	0
Code Rej:	0	0

:

Figure 58 (Part 6 of 8). Scenario 4: 2210 Customization via an ASCII Console


```

:
IPCP Statistic      In      Out
-----
Packets:           0      0
Octets:            0      0
Prot Rejects:      0      -

IP Statistic        In      Out
-----
Packets:           0      0
Octets:            0      0
Prot Rejects:      0      -

DNCP Statistic      In      Out
-----
Packets:           0      0
Octets:            0      0
Prot Rejects:      0      -

DN Statistic        In      Out
-----
Packets:           0      0
Octets:            0      0
Prot Rejects:      0      -

No IPX control protocol statistics available
No IPX statistics available

BNCP Statistic      In      Out
-----
Packets:           0      0
Octets:            0      0
Prot Rejects:      0      -

ATCP Statistic      In      Out
-----
Packets:           0      0
Octets:            0      0
Prot Rejects:      0      -

AP2 Statistic       In      Out
-----
Packets:           0      0
Octets:            0      0
Prot Rejects:      0      -

:

```

Figure 58 (Part 7 of 8). Scenario 4: 2210 Customization via an ASCII Console

```

:
No OSI control protocol statistics available
No OSI statistics available

Error Type                Count                Last One
-----
Bad Address:              0                0
Bad Control:              0                0
Unknown Protocol:         0                0
Invalid Protocol:         0                0
CONFIG Timeouts:          0                -
Terminate Timeouts:       0                -

PPP>exit
+Ctrl+p
*
```

Figure 58 (Part 8 of 8). Scenario 4: 2210 Customization via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** List the configuration of devices (interfaces).
- 3** Customization of the network number 0. This is the token-ring LAN interface.
- 4** List the configuration of the token-ring interface.
- 5** The 2210 is connected to the token-ring LAN via a UTP cable. The default is STP.
- 6** This is the locally administrated address of the token-ring interface.
- 7** Customization of network 1. This is the serial 1 interface.
- 8** List the configuration of HDLC parameters for the serial 1 interface.
- 9** The default encoding for serial link on the IBM 6611 Network Processor is NRZI.
- 10** Specify that a V.35 DTE cable is used.
- 11** List the configuration of serial 1.
- 12** Interface 2 is not used in this scenario.
- 13** Access the bridging configuration.
- 14** Enable the bridging function at the box level.
- 15** List the bridging configuration.
- 16** Disable transparent bridging (STB) on the token-ring interface.

17 Enable source route bridging (SRB) on the token-ring interface.

Assign the segment number FF0 to the token-ring segment, and assign the bridge number 1 to the 2210.

18 Add a bridging port for the serial 1 interface (interface 1). The port number is 2.

19 Disable transparent bridging (STB) on the serial 1 interface.

20 Enable source route bridging (SRB) on the serial 1 interface. Assign the segment number FF1 to the serial interface. This is the same segment number assigned to the serial interface on the 6611.

21 Access the TCP/IP host configuration.

22 Set an IP address at the box level.

23 List the TCP/IP host configuration.

24 Restart the 2210 to get the configuration running.

25 The configuration is now running on the 2210. We access the CGW operator console to monitor the running configuration.

26 Access the bridging monitoring function.

27 List the bridge configuration. Note that both interfaces are active.

28 Access the serial 1 monitoring function.

29 List the serial 1 configuration. Note the local and remote statistics.

```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 12T 2
  Select CONFIGURATION of Token-Ring line
  ENABLE INTERFACE
  MAC ADDRESS = 40002210A001 3
  Select SPEED
  Select 4
  Select PACKET SIZE
  Select 2052
  Select CABLE TYPE
  Select UTP 4
  RIF TIMER = 120
  DISABLE END NODE SOURCE ROUTING

Select the data-link protocol of Serial 1 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 1
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZI 5
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select V35 DTE 6
  Select subpanel LCP 7
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP 7
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP 7
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

  :

```

Figure 59 (Part 1 of 3). Scenario 4: 2210 Customization via the Nways MRS Configuration Program

```

:
  Select CONFIGURATION of Serial 2
    On GENERAL subpanel :
      DISABLE INTERFACE 8

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 9
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 1 10
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 1
  Select LF BIT INTERPRETATION
    Select EXTENDED
  ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
  DISABLE SR <-> TB CONVERSION

In TRANSPARENT BRIDGE box
  FILT. DBASE SIZE = 2048
  AGING TIME = 300
  RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE TOKEN-RING 11
Select CONFIGURE of Token-Ring
  Select INTERFACE SUPPORTS
    Select SRB 12
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = FF0 13
  MTU UNIT = 4399
  ENABLE STE

ENABLE SERIAL 1 14
Select CONFIGURE of Serial 1
  Select INTERFACE SUPPORTS
    Select SRB 15
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = FF1 16
  MTU UNIT = 4399
  ENABLE STE

:

```

Figure 59 (Part 2 of 3). Scenario 4: 2210 Customization via the Nways MRS Configuration Program

```

:
DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
ENABLE IP-HOST SERVICES
ENABLE ROUTER DISCOVERY
DISABLE RIP-LISTENING
IP-HOST ADDRESS = 9.67.46.146      17
IP-HOST MASK = 255.255.255.240
In DEFAULT GATEWAY IP ADDRESS
Nothing Customized

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION      18

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter SRBBI      19
Select OK

```

Figure 59 (Part 3 of 3). Scenario 4: 2210 Customization via the Nways MRS Configuration Program

Notes:

- 1 Start the customization from an empty configuration.
- 2 This is a 2210 Model 12T with a token-ring interface, 4MB of Flash, and 8MB RAM.
- 3 This is the locally administered address of the token-ring interface.
- 4 The 2210 is connected to the token-ring LAN using the UTP connector. The default is STP.
- 5 The default encoding for the serial link on the IBM 6611 Network Processor is NRZI.
- 6 Specify that an RS-232 DTE cable is used for serial 1.
- 7 This subpanel has not been changed. Default settings are used for all the parameters.
- 8 This interface 2, corresponding to WAN 2 (Serial 2) is unused.
- 9 Interface 2 is not used in this scenario.
- 10 The bridge number of 2210 is 1.
- 11 Enable the token-ring interface for bridging.
- 12 Enable source route bridging on the token-ring interface.

- 13** This is the segment number for the token-ring LAN interface.
- 14** Enable the serial 1 interface for bridging.
- 15** Enable source route bridging on the serial 1 interface.
- 16** This is the segment number for the serial link interface.
- 17** Set an IP address at the box level.
- 18** Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.
- 19** This is the name of the configuration file stored in your workstation.

```

Select TOKEN-RING ADAPTER CONFIGURATION
  Enable PHYSICAL INTERFACE 1

  Select PHYSICAL INTERFACE CONFIGURATION
    LOCALLY ADMINISTERED ADDRESS = 40006611B001 2
    MAC ADDRESS FORMAT = NONCANONICAL
    TOKEN-RING DATA RATE = 4 Mbps 3
    BROADCAST-TYPE = NON LOCAL

  Enable SR BRIDGE 4

  Select SR BRIDGE
    SPANNING TREE MODE = AUTOMATIC
    RING NUMBER = FF2 5
    MAXIMUM TRANSMISSION UNIT = 2052

  Select SR BRIDGE FILTERS
    Select SOURCE SAP INBOUND FILTER
      Delete the SAP = AA from the LIST OF INBOUND SOURCE SAP FILTER 6

Select SERIAL ADAPTER CONFIGURATION

  Select PPP
    Enable PHYSICAL INTERFACE 7

    Select PHYSICAL INTERFACE CONFIGURATION
      INTERFACE CABLE = V35, V36, or EIA232 8
      TRANSMIT CLOCK SOURCE = DCE
      DATA ENCODING = NRZI 9

    Enable PPP CONFIGURATION 10

    Enable SOURCE ROUTE BRIDGE 11

    Select SOURCE ROUTE BRIDGE
      SPANNING TREE MODE = AUTOMATIC
      RING NUMBER = FF1 12
      MAXIMUM TRANSMISSION UNIT = 2052

Select NODE CONFIGURATION
  Enable SOURCE ROUTE BRIDGING 13

  Select SOURCE ROUTE BRIDGING
    BRIDGE NUMBER = 2 14
    Disable LAN BRIDGING PROTOCOL

```

Figure 60. Scenario 4 and 5: 6611 Customization via the IBM 6611 MPNP Configuration Program

Notes:

- 1** Enable the token-ring interface.
- 2** This is the locally administered address of the token-ring interface.
- 3** This is the token-ring speed.
- 4** Enable source route bridging on token-ring interface.

- 5** This is the segment number of the token-ring to which the 6611 is attached.
- 6** To be able to bridge IP protocol, we have to remove this SAP filter.
- 7** Enable the serial interface.
- 8** Specify the type of cable used on this interface.
- 9** NRZI is the default encoding on the 6611.
- 10** Enable the PPP configuration for the serial interface.
- 11** Enable source route bridging for the serial interface.
- 12** This is the segment number of the serial link interface.
- 13** Enable source route bridging at the box level.
- 14** This is the bridge number of the 6611.

4.4.5 Scenario 5: SRT Bridge Implementation and Interoperability

In this scenario, we have a 2210A Model 12T with a token-ring LAN, a 2210B Model 12E with an Ethernet LAN and a 6611 Model 170 with a token-ring LAN.

The 2210A is a source route-transparent bridge, with SRB and STB on its token-ring interface, STB on its serial 1 interface and SRB on its Serial 2 interface. The segment number of the 2210A token-ring is FF0. The locally administered address (MAC address) of the token-ring interface is 40002210A001. The 2210A bridge number is 1. We have assigned the IP address of 9.67.46.146 (subnet mask 255.255.255.240) for the 2210A bridge.

The serial link between 2210A and 2210B is a PPP link connected via RS-232 modems. It belongs to the transparent bridge domain. The serial link between the 2210A and 6611 is a PPP link connected via V.35 modems. It belongs to the source route bridge domain, and its segment number is FF1.

The 2210B with Ethernet LAN is a pure transparent bridge with STB on both Ethernet and Serial 2 interfaces. We have assigned the IP address of 9.67.46.145 (subnet mask 255.255.255.240) to the 2210B bridge. For 2210B, the serial 1 interface is unused.

The 6611 is a pure source route bridge, with SRB on its token-ring, and serial interface. The segment number of the 6611 token-ring is FF2. The locally administered address of the token-ring interface is 40006611B001. The 6611 bridge number is 2.

Figure 61 on page 197 shows the configuration of the network used in this scenario.

The customization parameters we used to test this scenario are shown in:

- Figure 62 on page 198 (2210A configuration via an ASCII console)
- Figure 66 on page 220 (2210B configuration via an ASCII console)
- Figure 63 on page 204 (2210A configuration via Nways MRS)
- Figure 68 on page 230 (2210B configuration via Nways MRS)
- Figure 60 on page 194 (6611 configuration via IBM 6611 MPNP)

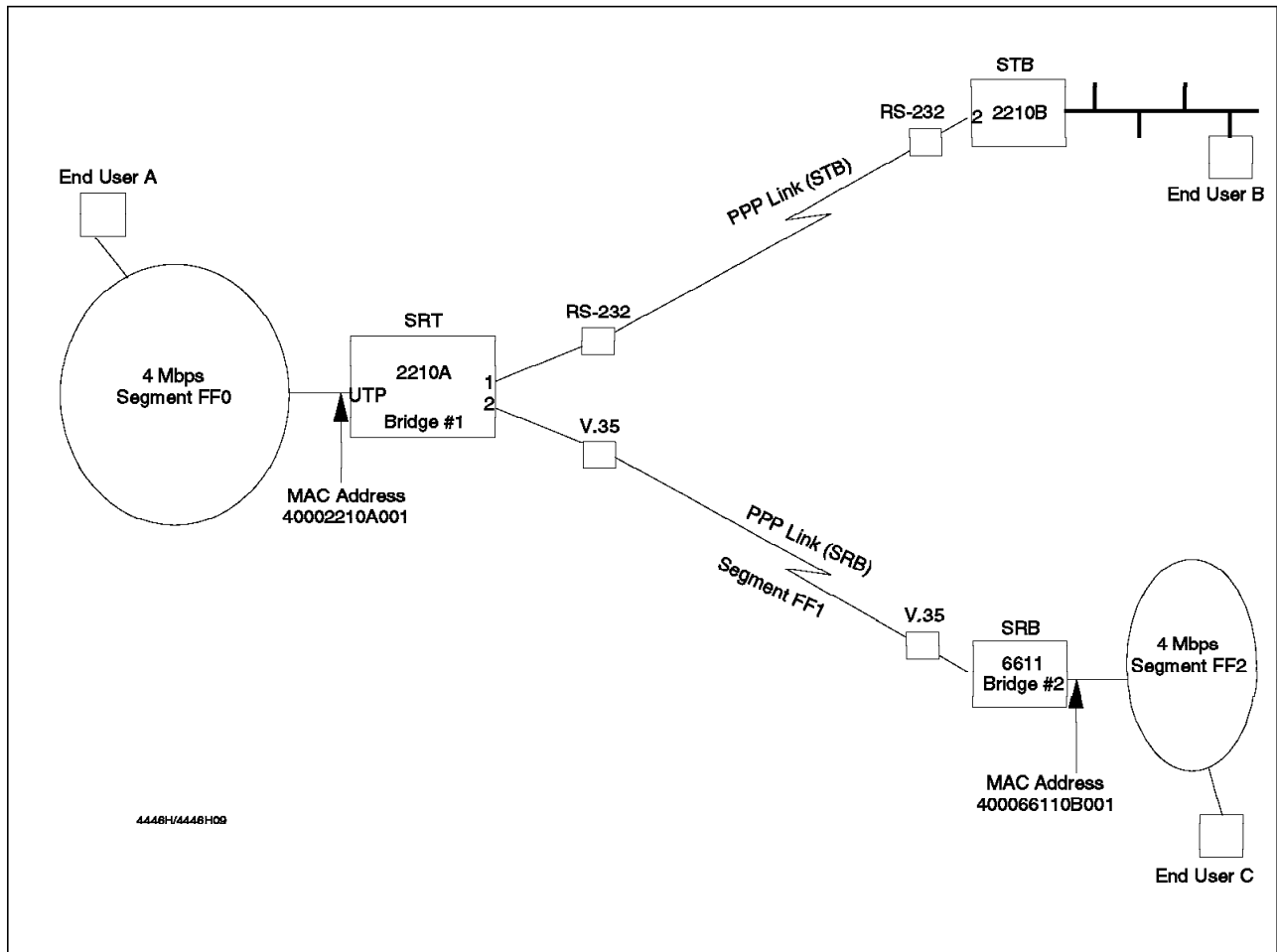


Figure 61. Scenario 5: SRT Bridge Configuration with the IBM 2210s and the IBM 6611 Network Processor

```

*
*talk 6 1

Config>network 0 2
Token-Ring interface configuration
TKR config>list 3
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                4 Mb/sec
Media:                Shielded

RIF Aging Timer:      120
Source Routing:       Enabled
MAC Address:          000000000000
IPX interface configuration record missing

TKR config>media unshielded 4
TKR config>set physical-address 5
MAC address in 00:00:00:00:00:00 form []? 40:00:22:10:A0:01
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                4 Mb/sec
Media:                Unshielded

RIF Aging Timer:      120
Source Routing:       Enabled
MAC Address:          40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 6
Point-to-Point user configuration
PPP Config>list all 7

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

:

```

Figure 62 (Part 1 of 5). Scenario 5: 2210A Customization via an ASCII Console

```

:
LCP Options
-----
Max Receive Unit:                2048   Magic Number:                Yes

NCP Parameters
-----
CONFIG Request Tries:            20     CONFIG Nak Tries:                10
Terminate Tries:                 10     Retry Timer:                    3000

IPCP Options
-----
IPCP Compression:                None
IP Address:                      Don't Send or Request
PPP Config>set hdlc cable rs-232 dte 8
PPP Config>list hdlc 9

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>exit
Config>network 2 10
Point-to-Point user configuration
PPP Config>list hdlc

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>set hdlc encoding nrzi 11
PPP Config>set hdlc cable v35 dte 12
:

```

Figure 62 (Part 2 of 5). Scenario 5: 2210A Customization via an ASCII Console

```

:
PPP Config>list all

Maximum frame size in bytes = 2048
Encoding: NRZI
Idle State: Flag
Clocking: External
Cable type: V.35 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Config>protocol asrt           13
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge      14
ASRT config>list bridge        15

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  0      No. of Source routing segments: 0
SRB: Max ARE Hop cnt:  0          Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE      Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 1
Port Number:  1    Interface Number:  0 Port Behaviour: STB Only

:

```

Figure 62 (Part 3 of 5). Scenario 5: 2210A Customization via an ASCII Console

```

:
ASRT config>enable source-routing      16
Port Number [1]? 1
Segment Number for the port in hex(1 - FFF) [1]? FF0
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>add port 1 2                17
ASRT config>add port 2 3                18
ASRT config>disable transparent         19
Port Number [1]? 3
ASRT config>enable source-routing      20
Port Number [1]? 3
Segment Number for the port in hex(1 - FFF) [1]? FF1
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:   ENABLED                      Bridge Behaviour: SRT
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 1        No. of Source routing segments: 2
SRB: Max ARE Hop cnt: 14               Max STE Hop cnt: 14
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE         Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED   FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d on all ports
DLS for the bridge: DISABLED
Number of ports added: 3
Port Number: 1   Interface Number: 0 Port Behaviour: STB & SRB
Port Number: 2   Interface Number: 1 Port Behaviour: STB Only
Port Number: 3   Interface Number: 2 Port Behaviour: SRB Only

ASRT config>exit
Config>protocol hst                    21
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address  22
IP-Host address [0.0.0.0]? 9.67.46.146
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

TCP/IP-Host config>list all            23

IP-Host IP address : 9.67.46.146
Address Mask       : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

:

```

Figure 62 (Part 4 of 5). Scenario 5: 2210A Customization via an ASCII Console

```

:
TCP/IP-Host config>exit
Config>Ctrl+p
*restart 24
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 25

CGW Operator Console

+protocol asrt 26
ASRT>list bridge 27
Bridge ID (prio/add): 32768/02-00-44-08-05-80
Bridge state: Enabled
Bridge type: SRT
Bridge capability: ASRT
Number of ports: 3
STP Participation: IEEE802.1d on all ports

Port Interface State MAC Address Modes Maximum MSDU Segment
1 TKR/0 Up 02-00-44-08-05-80 SR T 2096 FF0
2 PPP/0 Up 00-00-00-00-00-00 T 2052
3 PPP/1 Up 00-00-00-00-00-00 SR 1504 FF1

SR bridge number: 1
SR virtual segment: 000
Adaptive segment: 000
ASRT>exit
+Ctrl+p
*
```

Figure 62 (Part 5 of 5). Scenario 5: 2210A Customization via an ASCII Console

Notes:

- 1 Talk to the CONFIG process.
- 2 Customization of the network number 0. This is the token-ring LAN interface.
- 3 List the configuration for the token-ring interface.
- 4 The 2210 is connected to the token-ring LAN via a UTP cable. The default is STP.
- 5 This is the locally administered address of the token-ring interface.

- 6** Customization of network 1. This is the serial 1 interface.
- 7** List the configuration of the serial 1 interface.
- 8** Specify that an RS-232-DTE cable is used.
- 9** List the HDLC configuration of serial 1.
- 10** Customization of the Serial 2 interface (network 2).
- 11** The default encoding for the serial link on the IBM 6611 Network Processor is NRZI.
- 12** Specify that a V.35 DTE cable is used on the Serial 2 interface.
- 13** Access the bridging configuration.
- 14** Enable the bridging function at the box level.
- 15** List the bridging configuration.
- 16** Enable source routing bridge (SRB) on the token-ring interface. Assign the segment number FF0 to the token-ring segment, and assign the bridge number 1 to the 2210. Note that the token-ring interface has both SRB and STB bridging enabled.
- 17** Add a bridging port for the serial 1 interface (interface 1). The port number is 2 and by default, it is enabled for SRB.
- 18** Add a bridging port for the Serial 2 interface (interface 2). The port number is 3 and by default, it is enabled for SRB.
- 19** Disable transparent bridge (STB) on port 3.
- 20** Enable source route bridge (SRB) on port 3. Assign the segment number FF1 to the serial link interface.
- 21** Access the TCP/IP host protocol configuration.
- 22** Set an IP address at the box level.
- 23** List the TCP/IP host configuration.
- 24** Restart the 2210 to get the configuration running.
- 25** The configuration is now running on the 2210. We access the CGW operator console to monitor the running configuration.
- 26** Access the bridging monitoring function.
- 27** List the bridge configuration. Note that all the three interfaces are active.

```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 12T 2
  Select CONFIGURATION of Token-Ring line
  ENABLE INTERFACE
  MAC ADDRESS = 40002210A001 3
  Select SPEED
  Select 4
  Select PACKET SIZE
  Select 2052
  Select CABLE TYPE
  Select UTP 4
  RIF TIMER = 120
  DISABLE END NODE SOURCE ROUTING

Select the data-link protocol of Serial 1 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 1
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZ
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select RS-232 DTE 5
  Select subpanel LCP 6
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP 6
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP 6
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

  :

```

Figure 63 (Part 1 of 4). Scenario 5: 2210A Customization via the Nways MRS Configuration Program

```

:
Select the data-link protocol of Serial 2 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 2
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
      Select NRZI 7
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
      Select V35 DTE 8
    Select subpanel LCP 6
      RETRY TIMER = 3000
      CONFIG TRIES = 20
      NAK TRIES = 10
      TERMINATE TRIES = 10
      MAXIMUM RECEIVE UNIT = 2048
    Select subpanel BNCP 6
      ENABLE MAGIC NUMBER
      DISABLE TINYGRAM COMPRESSION
    Select subpanel IPCP 6
      DISABLE IP Compression
      Number of Slots = 16
      DISABLE SEND IP ADDRESS
      DISABLE REQUEST IP ADDRESS

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 9
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 1 10
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 1
  Select LF BIT INTERPRETATION
    Select EXTENDED
  ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
  DISABLE SR <=> TB CONVERSION

:

```

Figure 63 (Part 2 of 4). Scenario 5: 2210A Customization via the Nways MRS Configuration Program

:

In TRANSPARENT BRIDGE box
FILT. DBASE SIZE = 2048
AGING TIME = 300
RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :

ENABLE TOKEN-RING **11**

Select CONFIGURE of Token-Ring

Select INTERFACE SUPPORTS

Select **SR & TB** **12**

Select DUPLICATE FRAMES

Select STE&TSF

SEGMENT NUMBER = **FF0** **13**

MTU UNIT = 4399

ENABLE STE

ENABLE SERIAL 1 **14**

Select CONFIGURE of Serial 1

Select INTERFACE SUPPORTS

Select **STB** **15**

Select DUPLICATE FRAMES

Select STE&TSF

SEGMENT NUMBER = 1

MTU UNIT = 4399

ENABLE STE

ENABLE SERIAL 2 **16**

Select CONFIGURE of Serial 2

Select INTERFACE SUPPORTS

Select **SRB** **17**

Select DUPLICATE FRAMES

Select STE&TSF

SEGMENT NUMBER = **FF1** **18**

MTU UNIT = 4399

ENABLE STE

On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :

ENABLE IP-HOST SERVICES

ENABLE ROUTER DISCOVERY

DISABLE RIP-LISTENING

IP-HOST ADDRESS = **9.67.46.146** **19**

IP-HOST MASK = **255.255.255.240**

In DEFAULT GATEWAY IP ADDRESS

Nothing Customized

:

Figure 63 (Part 3 of 4). Scenario 5: 2210A Customization via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
    Select CREATE ROUTER CONFIGURATION 20

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
  Enter SRTA 21
  Select OK

```

Figure 63 (Part 4 of 4). Scenario 5: 2210A Customization via the Nways MRS Configuration Program

Notes:

- 1** Start the customization from an empty configuration.
- 2** This is a 2210 Model 12T with a token-ring interface, 4 MB of Flash, and 8 MB of RAM.
- 3** This is the locally administered address of the token-ring interface.
- 4** The 2210 is connected to the token-ring LAN using the UTP connector. The default is STP.
- 5** Specify that an RS-232 DTE cable is used for serial 1.
- 6** This subpanel has not been changed. Default settings are used for all the parameters.
- 7** The default encoding for the serial link on the IBM 6611 Network Processor is NRZI.
- 8** Specify that a V.35 DTE cable is used on the Serial 2.
- 9** Enable bridging function at the box level.
- 10** The bridge number of 2210 is 1.
- 11** Enable the token-ring interface for bridging.
- 12** Enable source route bridging and transparent bridging on the token-ring interface.
- 13** This is the segment number of the token-ring LAN to which the 2210 is attached.
- 14** Enable the serial 1 interface for bridging.
- 15** Enable transparent bridging on the serial 1 interface.
- 16** Enable the Serial 2 interface for bridging.
- 17** Enable source route bridging on the Serial 2 interface.
- 18** This is the segment number of the Serial 2 link.
- 19** Set an IP address at the box level.

20 Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.

21 This is the name of the configuration file stored in your workstation.

4.4.6 Scenario 6: SR-TB Implementation with NetBIOS Facilities

When you want to perform translational bridging between two IBM 2210s, only one has to enable the source route-translational bridge functionality. The other is either a transparent bridge, if the PPP link belongs to the transparent bridge domain, or a source route bridge, if the PPP link belongs to the source route bridge domain.

In this scenario, we have two IBM 2210s, 2210A with a token-ring LAN and 2210B with an Ethernet LAN.

2210A implements the NetBIOS Name Caching facility and NetBIOS Filtering facility.

2210A is a source route-translational bridge, with SRB on its token-ring interface, and STB on its Serial 2 interface. The segment number of the token-ring is FFB and the bridge number of the 2210 is 1. The transparent bridge domain is seen as segment number FFF from the source route bridge domain. The token-ring interface has a MAC address of 40002210A001. We have assigned the IP address of 9.67.46.146 (subnet mask 255.255.255.240) to the 2210A bridge.

2210A also implements the NetBIOS Name Caching facility and NetBIOS Filtering facility. For NetBIOS filtering, all packets with the NetBIOS host name WTR33338, which are received on the token-ring interface, are discarded.

The serial link between the two 2210s is a PPP link connected via RS-232 modems. This serial link belongs to the transparent bridge domain.

2210B with Ethernet LAN is a pure transparent bridge with STB on both Ethernet and Serial 2 interfaces. We have assigned the IP address of 9.67.46.145 (subnet mask 255.255.255.240) to the 2210B bridge.

For both 2210s, the serial 1 interface is unused.

Figure 64 on page 210 shows the configuration of the network used in this scenario.

The customization parameters we used to test this scenario are shown in:

- Figure 65 on page 211 (2210A configuration via an ASCII console)
- Figure 66 on page 220 (2210B configuration via an ASCII console)
- Figure 67 on page 224 (2210A configuration via Nways MRS)
- Figure 68 on page 230 (2210B configuration via Nways MRS)

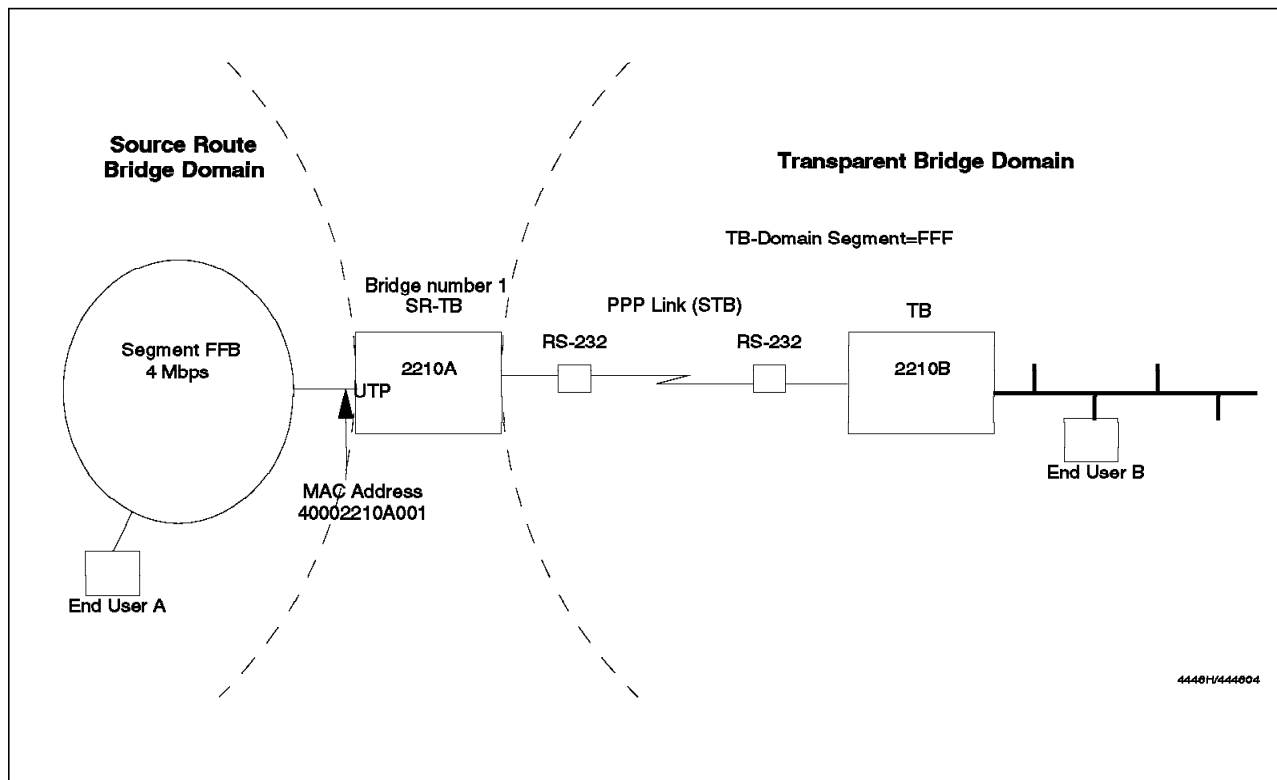


Figure 64. Scenario 6: SR-TB Configuration with IBM 2210s


```

*
*talk 6 1

Config>list devices 2
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>disable interface 1 3
Config>network 0 4
Token-Ring interface configuration
TKR config>list 5
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Shielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 000000000000
IPX interface configuration record missing

TKR config>media unshielded 6
TKR config>set physical-address 40:00:22:10:a0:10 7
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Unshielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 40002210A010
IPX interface configuration record missing

TKR config>exit
Config>network 2 8
Point-to-Point user configuration
PPP Config>list all 9

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0

:

```

Figure 65 (Part 1 of 7). Scenario 6: 2210A Configuration via an ASCII Console

```

:
LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>set hdlc cable rs-232 dte    10
PPP Config>list hdlc                11

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>exit
Config>protocol asrt            12
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge      13
ASRT config>list bridge        14

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                Bridge Behaviour: Unknown
Bridge Address: Not Specified By User   Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0         No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED   TB-Virtual Segment:0x0   MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE                Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED   FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 1
Port Number: 1    Interface Number: 0 Port Behaviour: STB Only

:

```

Figure 65 (Part 2 of 7). Scenario 6: 2210A Configuration via an ASCII Console

```

:
ASRT config>disable transparent 1 15
ASRT config>enable source-routing 1 ffb 16
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>add port 2 3 17
ASRT config>enable sr-tb-conversion 18
TB-Domain Segment Number in hex(1 - FFF) [1]? fff
TB-Domain's MTU [1470]?
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: SR<=>TB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 1        No. of Source routing segments: 1
SRB: Max ARE Hop cnt: 14               Max STE Hop cnt: 14
SR-TB Conversion: ENABLED  TB-Virtual Segment:0xFFFF  MTU for TB-Domain: 1470
1:N Source Routing:  NOT ACTIVE        Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED   FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d on TB ports and IBM-8209 on SR
ports
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number: 1   Interface Number: 0 Port Behaviour: SRB Only
Port Number: 3   Interface Number: 2 Port Behaviour: STB Only

ASRT config>list port 19
Port Id (dec)    : 128: 1, (hex): 80-01
Port State      : ENABLED
Port Supports: Source Routing Bridging Only
SRB: Segment Number: 0xFFFF  MTU: 4399  STE: ENABLED
Assoc Interface : 0
Path Cost       : 0
+++++
Port Id (dec)    : 128: 3, (hex): 80-03
Port State      : ENABLED
Port Supports: Transparent Bridging Only
Assoc Interface : 2
Path Cost       : 0
+++++
ASRT config>name-caching 20
Name Cache Config>list 21

Server name caching: Enabled
Server timeout: 3
Add name frame filtering: Enabled
Add name frame timeout: 7
Entry timeout: 900

:

```

Figure 65 (Part 3 of 7). Scenario 6: 2210A Configuration via an ASCII Console

```

:
Name Cache Config>port 1 22
Name Cache Port Config>list 23

  Server name caching:      Enabled
  Add name frame filtering: Enabled

Name Cache Port Config>exit
Name Cache Config>exit
ASRT config>netbios-filtering 24
NETBIOS Filtering configuration
NETBIOS Filter config>list 25

NETBIOS Filtering: Disabled

NETBIOS Filter Lists
-----

  Handle          Type

NETBIOS Filters
-----

  Port #      Direction      Filter List Handle(s)

NETBIOS Filter config>enable netbios-filtering 26
NETBIOS Filter config>create name-filter-list mylist 27
NETBIOS Filter config>update mylist 28
Name Filter List Configuration
NETBIOS Name mylist config>list 29

NAME Filter List Name: mylist
NAME Filter List Default: Inclusive

  Item #   Type   Inc/Ex   Hostname      Last Char

NETBIOS Name mylist config>add exclusive ascii WTR33338 30
Special 16th character in ASCII hex (<CR> for no special character) []?
NETBIOS Name mylist config>list

NAME Filter List Name: mylist
NAME Filter List Default: Inclusive

  Item #   Type   Inc/Ex   Hostname      Last Char

  1        ASCII   Ex       WTR33338

NETBIOS Name mylist config>exit

:

```

Figure 65 (Part 4 of 7). Scenario 6: 2210A Configuration via an ASCII Console

```

:
NETBIOS Filter config>filter-on input 1 mylist      31
NETBIOS Filter config>list

NETBIOS Filtering: Enabled

NETBIOS Filter Lists
-----

      Handle          Type
      mylist          Name

NETBIOS Filters
-----

      Port #          Direction      Filter List Handle(s)
      1              Input          mylist

NETBIOS Filter config>exit
ASRT config>exit
Config>protocol hst      32
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host 9.67.46.146 255.255.255.240      33
IP-Host address set.

TCP/IP-Host config>list all      34

IP-Host IP address : 9.67.46.146
Address Mask       : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

TCP/IP-Host config>exit
Config>Ctrl+p
*restart      35
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

:

```

Figure 65 (Part 5 of 7). Scenario 6: 2210A Configuration via an ASCII Console

:

*talk 5 36

CGW Operator Console

+protocol asrt 37

ASRT>name_caching 38

Name Cache>list add_names 39

Name	MAC	Add (Group) Name	
		Received	Filtered
-----	-----	-----	-----
WTR33338 <00>	40-00-00-03-33-38	9	8
WTR33338 <03>	40-00-00-03-33-38	9	8
WTRDM <00>	40-00-00-03-33-38	9	8
DIN <00>	10-00-5A-FA-40-B8	4	3
DIN <03>	10-00-5A-FA-40-B8	4	3
SU2_AELIAS####<00>	10-00-5A-FA-5B-D1	13	11
STIMPY <00>	10-00-5A-FA-40-B8	4	3
IHDLOTNO	40-00-00-05-90-33	9	8
IRISNAMESEVER	40-00-00-05-90-33	9	8
N\$SKURTZSTIMPY	10-00-5A-FA-40-B8	4	3
N\$SKURTZ <03>	10-00-5A-FA-40-B8	4	3
ATSSERV <00>	10-00-5A-8A-00-8F	6	5
ATSSERV	10-00-5A-8A-00-8F	6	5
AS400CC <00>	10-00-5A-8A-00-8F	6	5
KOREY PVRQ16D	00-01-E3-1F-33-2E	6	5
ATSSERV <03>	10-00-5A-8A-00-8F	6	5

Name Cache>list cache statistics 40

Server	Received	Broadcasts		
		Converted	Forwarded	Filtered
-----	-----	-----	-----	-----
LMUSRV.NSCS1SF0<00>	0	0	0	0
LMUSRV.NSCS1DET<00>	0	0	0	0
LMUSRV.NSCS1DAL<00>	0	0	0	0
LMUSRV.NSCS1CHG<00>	0	0	0	0
NSCS1DET	0	0	0	0
LMUSRV.NSCS1ATL<00>	0	0	0	0
LMUSRV.NSCS1NYC<00>	0	0	0	0
SU2_ASUPER####<00>	37	0	1	36
IBMPSCCMAIL	6	5	1	0
LMUSRV.NSCS1WAS<00>	0	0	0	0

:

Figure 65 (Part 6 of 7). Scenario 6: 2210A Configuration via an ASCII Console

```

:
Name Cache>list cache rifs 41

```

Server	MAC Address	Routing Information Field
LMUSRV.NSCS1SF0<00>	40-00-0A-BC-D1-26	FFB:0F/582:07/581:0D/C31:01/ 24F:01/3DA:01/2DA:00
LMUSRV.NSCS1DET<00>	40-00-0A-BC-D1-16	FFB:0F/582:07/581:0D/C31:01/ 24F:01/3DA:01/2DA:00
LMUSRV.NSCS1DAL<00>	40-00-0A-BC-D1-11	FFB:0F/582:07/581:0D/C31:01/ 24F:01/3DA:01/2DA:00
LMUSRV.NSCS1CHG<00>	40-00-0A-BC-D1-06	FFB:0F/582:07/581:0D/C31:01/ 24F:01/3DA:01/2DA:00
NSCS1DET	40-00-0A-BC-D1-17	FFB:0F/582:07/581:0D/C31:01/ 24F:01/3DA:01/2DA:00
LMUSRV.NSCS1ATL<00>	40-00-0A-BC-D1-01	FFB:0F/582:07/581:0D/C31:01/ 24F:01/3DA:01/2DA:00
LMUSRV.NSCS1NYC<00>	40-00-0A-BC-D1-21	FFB:0F/582:07/581:0D/C31:01/ 24F:01/3DA:01/2DA:00
SU2_ASUPER#####<00>	10-00-5A-F8-6D-5D	FFB:0F/582:07/581:0D/C31:0E/ B15:03/530:00
IBMPSCCMAIL	10-00-5A-8F-AF-93	FFB:0F/582:07/581:0D/C31:03/ C30:01/C10:01/B02:01/A35:00
LMUSRV.NSCS1WAS<00>	40-00-0A-BC-D1-31	FFB:0F/582:07/581:0D/C31:01/ 24F:01/3DA:01/2DA:00

```

Name Cache>exit
ASRT>netbios-filtering 42
NETBIOS Filter>list name-filter-lists 43
NAME Filter List Name: mylist
NAME Filter List Default: Inclusive
Filter Item #   Type   Inc/Ex   Hostname   Last Char
1             ASCII  Exclusive WTR33338
NETBIOS Filter>list filters 44
NETBIOS Filtering: Enabled
Port #   Direction   Filter List Handle(s)   Pkts Filtered
1         Input      mylist                   2
NETBIOS Filter>exit
ASRT>exit
+Ctrl+p
*

```

Figure 65 (Part 7 of 7). Scenario 6: 2210A Configuration via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** List the configuration of devices (interfaces).
- 3** This is the serial 1 interface.
- 4** Customization of the network number 0. This is the token-ring LAN interface.
- 5** List the configuration for the token-ring interface.
- 6** The 2210 is connected to the token-ring LAN via a UTP cable. The default is STP.
- 7** This is the locally administered address (MAC address) of the token-ring interface.
- 8** Customization of network 1. This is the Serial 2 interface.
- 9** List the configuration of the Serial 2.
- 10** Specify that an RS-232-DTE cable is used.
- 11** List the HDLC configuration of Serial 2.
- 12** Access the bridging configuration.
- 13** Enable the bridging function at the box level.
- 14** List the bridging configuration.
- 15** Disable transparent bridging (STB) on the token-ring interface.
- 16** Enable source route bridging (SRB) on the token-ring interface. Assign the segment number FF0 to the token-ring segment, and assign the bridge number 1 to the 2210.
- 17** Add a bridging port for the Serial 2 interface (interface 2). The port number is 3 and by default, it is enabled for SRB.
- 18** Enable source route-translational bridging (SR-TB) at box level.
- 19** List the port configuration.
- 20** Access the NetBIOS Name Caching facility configuration.
- 21** List the NetBIOS Name Caching facility configuration. Note that both the name caching process and duplicate frames filtering process are enabled by default. We keep the default timer settings.
- 22** Access the NetBIOS Name Caching facility of the token-ring interface.
- 23** List the NetBIOS Name Caching facility configuration for port 1. Note that both the name caching process and duplicate frames filtering process are enabled by default.

- 24** Access the NetBIOS Filtering facility configuration.
- 25** List the NetBIOS Filtering facility configuration. It is disabled.
- 26** Enable the NetBIOS Filtering facility.
- 27** Create a name filter list called mylist.
- 28** Access the configuration of the mylist name filter list.
- 29** List the mylist name filter list configuration.
- 30** Add a name filter item to mylist filter in order to exclude (discard) the packets with NetBIOS host name WTR33338.
- 31** Attach the mylist filter list to the INPUT traffic filter of the token-ring port.
- 32** Access the TCP/IP host configuration.
- 33** Set an IP address at the box level.
- 34** List the TCP/IP host configuration.
- 35** Restart the 2210A to get the configuration running.
- 36** Talk to the CGW operator console in order to monitor the running configuration of this IBM 2210.
- 37** Access the bridge (ASRT) protocol monitoring.
- 38** Access the NetBIOS Name Caching facility monitoring.
- 39** List the duplicate frame filtering process host names. It shows the number of filtered frames per MAC address/NetBIOS host name.
- 40** List the name caching process. It shows the number of converted filtered frames per NetBIOS name.
- 41** List the name caching process. It shows the route known for each NetBIOS server name/MAC address.
- 42** Access the NetBIOS Filtering facility monitoring.
- 43** List the running name filter lists.
- 44** List the number of filtered frames per filter.

```

*
*talk 6 1

Config>network 2
What is the network number [0]? 0
Ethernet interface configuration
ETH config>list 3
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 2 4
Point-to-Point user configuration
PPP Config>list all 5

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request

:

```

Figure 66 (Part 1 of 3). Scenario 1, 5 and 6: 2210B Configuration via an ASCII Console

```

:
PPP Config>set hdlc cable rs-232 dte      6
PPP Config>list hdlc      7

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>exit
Config>disable interface 1      8
Config>list devices      9
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
(Disabled)
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>protocol asrt      10
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge      11
ASRT config>list bridge      12

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: DISABLED
Number of ports added: 1
Port Number: 1 Interface Number: 0 Port Behaviour: STB Only

ASRT config>add port      13
Interface Number [0]? 2
Port Number [2]? 3

:

```

Figure 66 (Part 2 of 3). Scenario 1, 5 and 6: 2210B Configuration via an ASCII Console

```

:
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:   ENABLED                      Bridge Behaviour: STB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED    FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: DISABLED
Number of ports added: 2
Port Number: 1      Interface Number: 0 Port Behaviour: STB Only
Port Number: 3      Interface Number: 2 Port Behaviour: STB Only

ASRT config>exit
Config>protocol hst 14
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address 15
IP-Host address [0.0.0.0]? 9.67.46.145
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

TCP/IP-Host config>list all 16

IP-Host IP address : 9.67.46.145
Address Mask       : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

TCP/IP-Host config>exit
Config>Ctrl+p
*restart 17
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 66 (Part 3 of 3). Scenario 1, 5 and 6: 2210B Configuration via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Customization of the network number 0. This is the Ethernet LAN interface.
- 3** List the configuration of the Ethernet interface.
- 4** Customization of network 1. This is the Serial 2 interface.
- 5** List the configuration of the Serial 2 interface.
- 6** Specify that an RS-232 DTE cable is used.
- 7** List the HDLC configuration of Serial 2.
- 8** Interface 2 is not used in this scenario.
- 9** List the configuration of devices (interfaces).
- 10** Access the bridging configuration.
- 11** Enable the bridge function at the box level.
- 12** List the configuration of the bridging function.
- 13** Add a port for Serial 2 (interface 2) and assign port number 3 to it. This port is configured for STB by default.
- 14** Access the TCP/IP host configuration.
- 15** Set an IP address at the box level.
- 16** List the TCP/IP host configuration.
- 17** Restart the 2210B to get the configuration running.

On 2210 Navigation Window :

- Select CONFIGURE from the menu bar
- Select NEW CONFIGURATION **1**

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :

- Select MODEL
 - Select **MODEL 12T** **2**
- Select CONFIGURATION of Token-Ring line
 - ENABLE INTERFACE
 - MAC ADDRESS = **40002210A001** **3**
 - Select SPEED
 - Select 4
 - Select PACKET SIZE
 - Select 2052
 - Select CABLE TYPE
 - Select **UTP** **4**
 - RIF TIMER = 120
 - DISABLE END NODE SOURCE ROUTING
- Select CONFIGURATION of Serial 1
 - On GENERAL subpanel :
 - DISABLE INTERFACE** **5**
- Select the data-link protocol of Serial 2 (PPP by default)
 - Select PPP
- Select CONFIGURATION of Serial 2
 - On GENERAL subpanel :
 - ENABLE INTERFACE
 - MAXIMUM TRANSMISSION UNIT = 2048
 - Select ENCODING
 - Select NRZ
 - Select IDLE
 - Select FLAG
 - Select CLOCKING
 - Select EXTERNAL
 - CLOCK SPEED = 0
 - TRANSMIT DELAY = 0
 - Select CABLE TYPE
 - Select RS-232 DTE **6**
 - Select subpanel LCP **7**
 - RETRY TIMER = 3000
 - CONFIG TRIES = 20
 - NAK TRIES = 10
 - TERMINATE TRIES = 10
 - MAXIMUM RECEIVE UNIT = 2048
 - Select subpanel BNCP **7**
 - ENABLE MAGIC NUMBER
 - DISABLE TINYGRAM COMPRESSION

:

Figure 67 (Part 1 of 4). Scenario 6: 2210A Configuration via Nways MRS Configuration Program

```

:
    Select subpanel IPCP      7
        DISABLE IP Compression
        Number of Slots = 16
        DISABLE SEND IP ADDRESS
        DISABLE REQUEST IP ADDRESS

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING      8
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
    BRIDGE NUMBER = 1      9
    MAXIMUM ARE HOP COUNT = 14
    MAXIMUM STE HOP COUNT = 14
    INTERNAL VIRTUAL SEGMENT = 1
    Select LF BIT INTERPRETATION
        Select EXTENDED
    ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
    ENABLE SR <-> TB CONVERSION    10
    DISABLE IBM8209 STP
    TB: VIRTUAL SEGMENT = FFF      11
    TB: MAXIMUM FRAME SIZE = 1470

In TRANSPARENT BRIDGE box
    FILT. DBASE SIZE = 2048
    AGING TIME = 300
    RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE TOKEN-RING      12
Select CONFIGURE of Token-Ring
    Select INTERFACE SUPPORTS
        Select SRB      13
    Select DUPLICATE FRAMES
        Select STE&TSF
        SEGMENT NUMBER = FFB      14
    MTU UNIT = 4399
    ENABLE STE

    DISABLE SERIAL 1
    Box CONFIGURE of Serial 1 not customized

:

```

Figure 67 (Part 2 of 4). Scenario 6: 2210A Configuration via Nways MRS Configuration Program

```

:
ENABLE SERIAL 2 15
Select CONFIGURE of Serial 2
  Select INTERFACE SUPPORTS
    Select STB 16
    Select DUPLICATE FRAMES
    Select STE&TSF
    SEGMENT NUMBER = 1
    MTU UNIT = 4399
    ENABLE STE

On 2210 Navigation Window :
Select NAME CACHING panel of NETBIOS subdirectory of BRIDGING directory

On NETBIOS NAME CACHING Window :
  ENABLE NAME CACHING 17
  ENABLE NAME FILTERING 18
  SERVER TIMEOUT = 3
  ENTRY TIMEOUT = 900
  "ADD NAME" TIMEOUT = 7

On 2210 Navigation Window :
Select ENABLE panel of FILTERING subdirectory of NETBIOS subdirectory of BRIDGING directory

On NETBIOS FILTERING Window :
  ENABLE NETBIOS FILTERING 19

On 2210 Navigation Window :
Select NAME LISTS panel of FILTERING subdirectory of NETBIOS subdirectory of BRIDGING directory

On NETBIOS FILTER - NAME LISTS Window :
  On GENERAL subpanel:
    Select FILTER TYPE
    Select INCLUSIVE
    NAME LIST = mylist 20
    Select ADD 21

:

```

Figure 67 (Part 3 of 4). Scenario 6: 2210A Configuration via Nways MRS Configuration Program


```

:
On NAME LIST subpanel:
Select FILTER TYPE
    Select EXCLUSIVE 22
Select TYPE
    Select ASCII 23
DISABLE SPECIAL LAST CHARACTER
HOST NAME = WTR33338 24
Select ADD 25

Select CHANGE outside the NAME LIST subpanel 26

On 2210 Navigation Window :
Select INTERFACES panel of FILTERING subdirectory of NETBIOS subdirectory of BRIDGING directory

On NETBIOS INTERFACES LISTS Window :
Select INPUT FILTER of the token-ring line
    ENABLE FILTER 27
    Select SET FILTER ON INPUT
        Select mylist 28

On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
ENABLE IP-HOST SERVICES
ENABLE ROUTER DISCOVERY
DISABLE RIP-LISTENING
IP-HOST ADDRESS = 9.67.46.146 29
IP-HOST MASK = 255.255.255.240
In DEFAULT GATEWAY IP ADDRESS
    Nothing Customized

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
    Select CREATE ROUTER CONFIGURATION 30

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter SRTBA 31
Select OK

```

Figure 67 (Part 4 of 4). Scenario 6: 2210A Configuration via Nways MRS Configuration Program

Notes:

- 1** Start the customization from an empty configuration.
- 2** This is a 2210 Model 12T with a token-ring LAN interface, 4 MB of Flash, and 8 MB of RAM.
- 3** This is the locally administered address (MAC address) of the token-ring interface.
- 4** The 2210 is connected to the token-ring LAN using the UTP connector. The default is STP.
- 5** Interface 1 is not used in this scenario.

- 6** Specify that an RS-232 DTE cable is used for serial 1.
- 7** This subpanel has not been changed. Default settings are used for all the parameters.
- 8** Enable the bridging function at the box level.
- 9** The bridge number for source route bridging (SRB) is 1.
- 10** Enable source route-translational bridging (SR-TB) at box level.
- 11** The transparent bridge domain is seen as LAN segment number FFF.
- 12** Enable the token-ring interface for bridging.
- 13** Enable source route bridging (SRB) on the token-ring interface.
- 14** The LAN segment number of the token-ring is FFB.
- 15** Enable the Serial 2 interface for bridging.
- 16** Enable transparent bridging (STB) on the Serial 2 interface.
- 17** Name caching process is enabled by default.
- 18** Duplicate frame filtering process is enabled by default.
- 19** Enable NetBIOS filtering process. It is disabled by default.
- 20** This is the name of the name filter list.
- 21** Create the name filter list *mylist*. Note that the filter type is inclusive by default.
- 22** Set the name filter item action to exclusive in order to discard NetBIOS packets matching this name filter item.
- 23** Enter the NetBIOS host name in ASCII format. Selecting ASCII displays the special last character parameter. The special last character is disabled by default.
- 24** This is the NetBIOS host name. Entering the host name while the special last character is disabled will result in the NetBIOS host name to be padded with ASCII space characters until the 15th character is included, and with a "?" wildcard in the 16th character position.
- 25** Create this name filter item. At this time, the created name filter item does not belong to the *mylist* filter list.
- 26** This modification is required to attach all name filter items listed in the NAME LIST subpanel to the selected filter list *mylist*.
- 27** Enable the token-ring filter for input traffic.
- 28** Attach *mylist* filter list to this filter.
- 29** Set an IP address at the box level.

30 Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.

21 This is the name of the configuration file stored in your workstation.

```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 12E 2
  Select CONFIGURATION of Ethernet line
  ENABLE INTERFACE
  Select CONNECTOR TYPE
  Select AUTO-CONFIG
  Select IP ENCAPSULATION
  Select ETHERNET

Select CONFIGURATION of Serial 1
  On GENERAL subpanel :
    DISABLE INTERFACE 3

Select the data-link protocol of Serial 2 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 2
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZ
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select RS-232 DTE 4
  Select subpanel LCP 5
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP 5
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP 5
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

:
```

Figure 68 (Part 1 of 3). Scenario 1, 5 and 6: 2210B Configuration via Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 6
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
    BRIDGE NUMBER = 1
    MAXIMUM ARE HOP COUNT = 14
    MAXIMUM STE HOP COUNT = 14
    INTERNAL VIRTUAL SEGMENT = 1
    Select LF BIT INTERPRETATION
        Select EXTENDED
    ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
    DISABLE SR <=> TB CONVERSION

In TRANSPARENT BRIDGE box
    FILT. DBASE SIZE = 2048
    AGING TIME = 300
    RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE ETHERNET
Select CONFIGURE of Ethernet
    Select INTERFACE SUPPORTS
        Select STB 7
    Select DUPLICATE FRAMES
        Select STE&TSF
    SEGMENT NUMBER = 1

DISABLE SERIAL 1
Box CONFIGURE of Serial 1 not customized

ENABLE SERIAL 2
Select CONFIGURE of Serial 2
    Select INTERFACE SUPPORTS
        Select STB 8
    Select DUPLICATE FRAMES
        Select STE&TSF
    SEGMENT NUMBER = 1
    MTU UNIT = 4399
    ENABLE STE

:

```

Figure 68 (Part 2 of 3). Scenario 1, 5 and 6: 2210B Configuration via Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
ENABLE IP-HOST SERVICES
ENABLE ROUTER DISCOVERY
DISABLE RIP-LISTENING
IP-HOST ADDRESS = 9.67.46.145    9
IP-HOST MASK = 255.255.255.240
In DEFAULT GATEWAY IP ADDRESS
Nothing Customized

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION    10

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter SRTBB    11
Select OK

```

Figure 68 (Part 3 of 3). Scenario 1, 5 and 6: 2210B Configuration via Nways MRS Configuration Program

Notes:

- 1 Start the customization from an empty configuration.
- 2 This is a 2210 Model 12E with an Ethernet LAN interface, 4 MB of Flash, and 8 MB of RAM.
- 3 Interface 1 is not used in this scenario.
- 5 Specify the type of cable used on the Serial 2 interface.
- 5 This subpanel has not been changed. Default settings are used for all the parameters.
- 6 Enable the bridging function at the box level.
- 7 Enable transparent bridging (STB) on the Ethernet interface.
- 8 Enable transparent bridging (STB) on the Serial 2 interface.
- 9 Set an IP address at the box level.
- 10 Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.
- 18 This is the name of the configuration file stored in your workstation.

4.4.7 Scenario 7: SR-TB Interoperability with the IBM 6611 Network Processor

In this scenario, we have a 2210 Model 12E with an Ethernet LAN, and a 6611 Model 170 with a token-ring LAN.

The 2210 is a source route-translational bridge, with STB on its Ethernet interface, and SRB on its serial 1 interface. The transparent bridge domain is seen as segment number FFF from the source route bridge domain. The 2210 bridge number is 1. We have assigned the IP address of 9.67.46.145 (subnet mask 255.255.255.240) for the 2210 bridge.

The serial link between the 2210 and the 6611 is a PPP link connected via V.35 modems. This serial link belongs to the source route bridge domain. Its segment number is FF0.

The 6611 with token-ring LAN is a pure source route bridge with SRB on both token-ring and serial interfaces. We have assigned a MAC address of 40006611B001 for the token-ring interface. The 6611 bridge number is 2. The segment number of token-ring is F00.

For the 2210, the Serial 2 interface is unused.

Figure 69 shows the configuration of the network used in this scenario.

The customization parameters we used to test this scenario are shown in:

- Figure 70 on page 234 (2210 configuration via an ASCII console)
- Figure 71 on page 241 (2210 configuration via Nways MRS)
- Figure 72 on page 245 (6611 configuration via IBM 6611 MPNP)

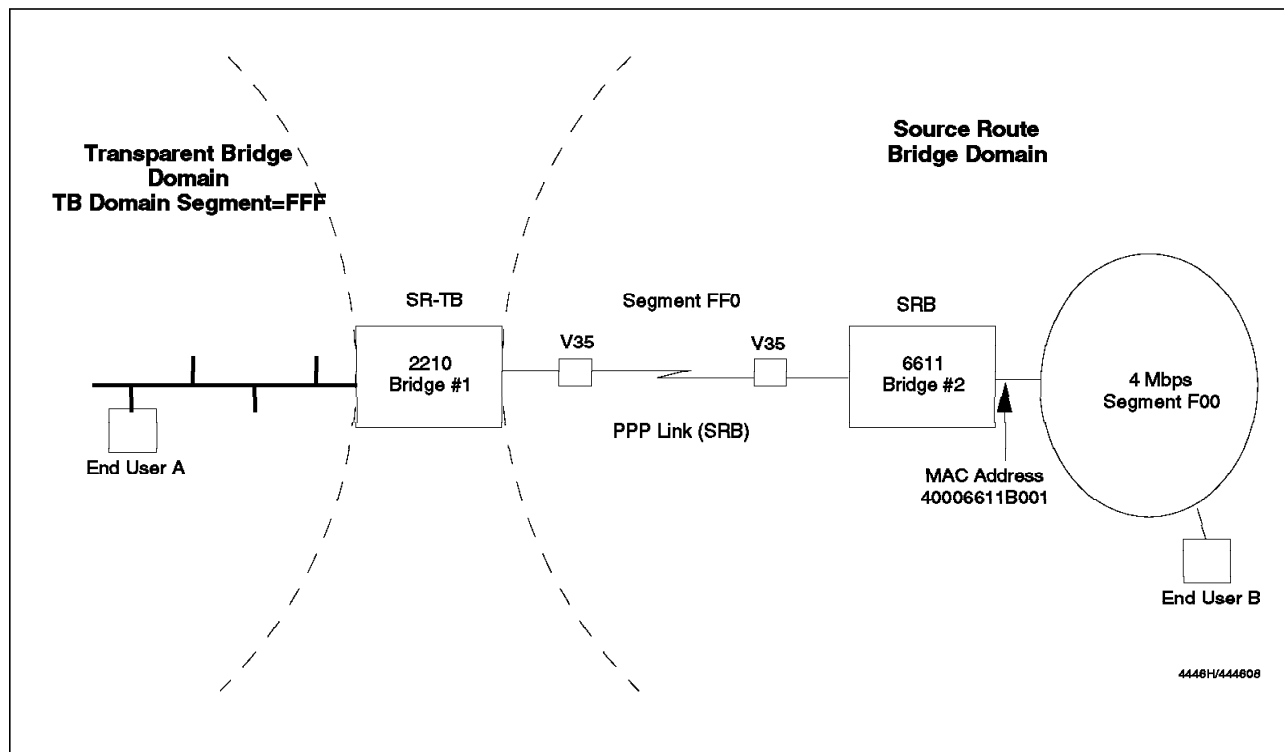


Figure 69. Scenario 7: SR-TB Configuration Between the IBM 2210 and the IBM 6611 Network Processor

```

*
*talk 6 1

Config>list devices 2
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>network 0 3
Ethernet interface configuration
ETH config>list 4
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 1 5
Point-to-Point user configuration
PPP Config>list all 6

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request

:

```

Figure 70 (Part 1 of 6). Scenario 7: 2210 Customization via an ASCII Console


```

:
PPP Config>set hdlc encoding nrzi 7
PPP Config>set hdlc cable v35 dte 8
PPP Config>list hdlc 9

Maximum frame size in bytes = 2048
Encoding: NRZI
Idle State: Flag
Clocking: External
Cable type: V.35 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>exit
Config>disable interface 2 10
Config>protocol asrt 11
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 12
ASRT config>add port 1 2 13
ASRT config>list bridge 14

Source Routing Transparent Bridge Configuration
=====

Bridge: ENABLED Bridge Behaviour: STB
Bridge Address: Not Specified By User Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0 No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0 Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: DISABLED
Number of ports added: 2
Port Number: 1 Interface Number: 0 Port Behaviour: STB Only
Port Number: 2 Interface Number: 1 Port Behaviour: STB Only

ASRT config>disable transparent 15
Port Number [1]? 2
ASRT config>enable source-routing 2 16
Segment Number for the port in hex(1 - FFF) [1]? FF0
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>enable sr-tb-conversion 17
TB-Domain Segment Number in hex(1 - FFF) [1]? FFF
TB-Domain's MTU [1470]?

:

```

Figure 70 (Part 2 of 6). Scenario 7: 2210 Customization via an ASCII Console

```

:
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:   ENABLED                      Bridge Behaviour: SR<->TB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 1        No. of Source routing segments: 1
SRB: Max ARE Hop cnt: 14              Max STE Hop cnt: 14
SR-TB Conversion: ENABLED  TB-Virtual Segment:0xFFFF  MTU for TB-Domain: 1470
1:N Source Routing:  NOT ACTIVE        Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED   FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d on TB ports and IBM-8209 on SR
ports
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number: 1      Interface Number:  0 Port Behaviour: STB Only
Port Number: 2      Interface Number:  1 Port Behaviour: SRB Only

ASRT config>exit
Config>protocol hst      18
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address      19
IP-Host address [0.0.0.0]? 9.67.46.145
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

TCP/IP-Host config>list all      20

IP-Host IP address : 9.67.46.145
Address Mask       : 255.255.255.240

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.

TCP/IP-Host config>exit
:

```

Figure 70 (Part 3 of 6). Scenario 7: 2210 Customization via an ASCII Console

```

:
Config>Ctrl+p
*restart 21
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 22

CGW Operator Console

+protocol asrt 23
ASRT>list bridge 24
Bridge ID (prio/add): 32768/00-00-93-80-80-D0
Bridge state: Enabled
Bridge type: SR-TB
Bridge capability: ASRT
Number of ports: 2
STP Participation: IEEE802.1d on TB ports and IBM-8209 on SR ports

Port Interface State MAC Address Modes Maximum MSDU Segment
1 Eth/0 Up 00-00-93-80-80-D0 T 1514
2 PPP/0 Up 00-00-00-00-00-00 SR 1504 FF0

SR bridge number: 1
SR virtual segment: 000
Adaptive segment: FFF
ASRT>exit
+network 1 25
Point-to-Point Console

:

```

Figure 70 (Part 4 of 6). Scenario 7: 2210 Customization via an ASCII Console

:
PPP>list all **26**

Version: 1
LCP State: Open
Previous State: Ack Rcvd
Time Since Change: 36 minutes and 23 seconds

LCP Option	Local	Remote
-----	-----	-----
Max Receive Unit:	1500	1500
Async Char Mask:	FFFFFFFF	FFFFFFFF
Authentication:	None	None
Magic Number:	24373E2	None
Protocol Compr:	No	No
Addr/Cntl Compr:	No	No
32-Bit Checksum:	No	No

IPCP State: Listen
Previous State: Closed
Time Since Change: 36 minutes and 29 seconds

IPCP Option	Local	Remote
-----	-----	-----
IP Address	0.0.0.0	None
Compression Slots	None	None

DNCP State: Closed
Previous State: Closed
Time Since Change: 36 minutes and 36 seconds

No IPX control protocol information available

BNCP State: Open
Previous State: Ack Rcvd
Time Since Change: 36 minutes and 35 seconds

BNCP Option	Local	Remote
-----	-----	-----
Tinygram Compression	DISABLED	DISABLED

:

Figure 70 (Part 5 of 6). Scenario 7: 2210 Customization via an ASCII Console

```

:
Source-route Info:  Local Bridge#  Remote Bridge#  Line ID
                   1                2            FF0

ATCP State:          Listen
Previous State:      Req Sent
Time Since Change:   35 minutes and 41 seconds

AppleTalk Address Info:
Common network number = 0
Local node ID = 0
Remote node ID = 0
No OSI control protocol information available

LCP Statistic          In              Out
-----
Packets:               27              27
Octets:                918             918
Cfg Req:                0              0
Cfg Ack:                0              0
Cfg Nak:                0              0
Cfg Rej:                0              0
Term Req:              0              0
Term Ack:              0              0
Echo Req:              0              27
Echo Resp:             27              0
Disc Req:              0              0
Code Rej:              0              0

IPCP Statistic          In              Out
-----
Packets:               0              0
Octets:                0              0
Prot Rejects:          0              -

PPP>exit
+Ctrl+p
*
```

Figure 70 (Part 6 of 6). Scenario 7: 2210 Customization via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** List the configuration devices (interfaces).
- 3** Customization of the network number 0. This is the token-ring LAN interface.
- 4** List the configuration for the Ethernet interface.

- 5** Customization of network 1. This is the serial 1 interface.
- 6** List the configuration of serial 1 interface.
- 7** The default encoding for the serial link on the IBM 6611 Network Processor is NRZI.
- 8** Specify that a V.35 DTE cable is used.
- 9** List the HDLC configuration for the serial 1 interface.
- 10** Interface 2 is not used in this scenario.
- 11** Access the bridging configuration.
- 12** Enable the bridging function at the box level.
- 13** Add a bridging port for serial 1 interface (interface 1). The port number is 2.
- 14** List the bridge configuration.
- 15** Disable transparent bridging (STB) on port 2.
- 16** Enable source route bridging (SRB) on port 2. Assign LAN segment number FF0 for this link. Assign bridge number 1 to the 2210.
- 17** Enable source route-translational bridging (SR-TB) at the box level. The transparent bridge domain is seen as LAN segment number FFF from the source route bridge domain.
- 18** Access the TCP/IP host configuration.
- 19** Set an IP address at the box level.
- 20** List the TCP/IP host configuration.
- 21** Restart the 2210 to get this configuration running.
- 22** The configuration is now running on the 2210. We access the CGW operator console to monitor the running configuration.
- 23** Access the bridging monitoring function.
- 24** List the bridge configuration. Note that both bridge ports are active.
- 25** Access the serial 1 monitoring function.
- 26** List the serial 1 monitoring. Note the local and remote statistics.

On 2210 Navigation Window :

- Select CONFIGURE from the menu bar
- Select NEW CONFIGURATION **1**

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :

- Select MODEL
 - Select **MODEL 12E** **2**
- Select CONFIGURATION of Ethernet line
 - ENABLE INTERFACE
 - Select CONNECTOR TYPE
 - Select **AUTO-CONFIG**
 - Select IP ENCAPSULATION
 - Select ETHERNET

Select the data-link protocol of Serial 1 (PPP by default)

- Select PPP

Select CONFIGURATION of Serial 1

On GENERAL subpanel :

- ENABLE INTERFACE
- MAXIMUM TRANSMISSION UNIT = 2048
- Select ENCODING
 - Select **NRZI** **3**
- Select IDLE
 - Select FLAG
- Select CLOCKING
 - Select EXTERNAL
- CLOCK SPEED = 0
- TRANSMIT DELAY = 0
- Select CABLE TYPE
 - Select **V35 DTE** **4**

Select subpanel LCP **5**

- RETRY TIMER = 3000
- CONFIG TRIES = 20
- NAK TRIES = 10
- TERMINATE TRIES = 10
- MAXIMUM RECEIVE UNIT = 2048

Select subpanel BNCP **5**

- ENABLE MAGIC NUMBER
- DISABLE TINYGRAM COMPRESSION

Select subpanel IPCP **5**

- DISABLE IP Compression
- Number of Slots = 16
- DISABLE SEND IP ADDRESS
- DISABLE REQUEST IP ADDRESS

Select CONFIGURATION of Serial 2

On GENERAL subpanel :

- DISABLE INTERFACE** **6**

:

Figure 71 (Part 1 of 3). Scenario 7: 2210 Customization via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 7
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 1 8
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 1
  Select LF BIT INTERPRETATION
  Select EXTENDED
  ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
ENABLE SR <-> TB CONVERSION 9
DISABLE IBM8209 STP
TB: VIRTUAL SEGMENT = FFF 10
TB: MAXIMUM FRAME SIZE = 1470

In TRANSPARENT BRIDGE box
  FILT. DBASE SIZE = 2048
  AGING TIME = 300
  RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE ETHERNET 11
Select CONFIGURE of Ethernet
  Select INTERFACE SUPPORTS
    Select STB 12
  Select DUPLICATE FRAMES
  Select STE&TSF
  SEGMENT NUMBER = 1

ENABLE SERIAL 1 13
Select CONFIGURE of Serial 1
  Select INTERFACE SUPPORTS
    Select SRB 14
  Select DUPLICATE FRAMES
  Select STE&TSF
  SEGMENT NUMBER = FFO 15
  MTU UNIT = 4399
  ENABLE STE

DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

:

```

Figure 71 (Part 2 of 3). Scenario 7: 2210 Customization via the Nways MRS Configuration Program


```

:
On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
  ENABLE IP-HOST SERVICES
  ENABLE ROUTER DISCOVERY
  DISABLE RIP-LISTENING
  IP-HOST ADDRESS = 9.67.46.145      16
  IP-HOST MASK = 255.255.255.240
  In DEFAULT GATEWAY IP ADDRESS
    Nothing Customized

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
    Select CREATE ROUTER CONFIGURATION      17

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
  Enter SRTBBI      18
  Select OK

```

Figure 71 (Part 3 of 3). Scenario 7: 2210 Customization via the Nways MRS Configuration Program

Notes:

- 1 Start the customization from an empty configuration.
- 2 This is a 2210 Model 12E with an Ethernet interface, 4 MB of Flash, and 8 MB of RAM.
- 3 The default encoding for the serial link on the IBM 6611 Network Processor is NRZI.
- 4 Specify that a V35 DTE cable is used for serial 1.
- 5 This subpanel has not been changed. Default settings are used for all the parameters.
- 6 Interface 2 is not used in this scenario.
- 7 Enable the bridging function at the box level.
- 8 Bridge number of the 2210 is 1.
- 9 Enable source route-translational bridging (SR-TB) at box level.
- 10 The transparent bridge domain is seen as LAN segment number FFF from the source route bridge domain.
- 11 Enable bridging on the Ethernet interface.
- 12 Enable transparent bridging (STB) on the Ethernet interface.
- 13 Enable bridging on the serial 1 interface.

- 14** Enable source route bridging (SRB) on the serial 1 interface.
- 15** The segment number of the serial 1 interface is FF0.
- 16** Set an IP address at the box level.
- 17** Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.
- 18** This is the name of the configuration file stored in your workstation.

```

Select TOKEN-RING ADAPTER CONFIGURATION
  Enable PHYSICAL INTERFACE 1

  Select PHYSICAL INTERFACE CONFIGURATION
    LOCALLY ADMINISTERED ADDRESS = 40006611B001 2
    MAC ADDRESS FORMAT = NONCANONICAL
    TOKEN-RING DATA RATE = 4 Mbps 3
    BROADCAST-TYPE = NON LOCAL

  Enable SR BRIDGE 4

  Select SR BRIDGE
    SPANNING TREE MODE = AUTOMATIC
    RING NUMBER = F00 5
    MAXIMUM TRANSMISSION UNIT = 2052

  Select SR BRIDGE FILTERS
    Select SOURCE SAP INBOUND FILTER
      Delete the SAP = AA from the LIST OF INBOUND SOURCE SAP FILTER 6

Select SERIAL ADAPTER CONFIGURATION

  Select PPP
    Enable PHYSICAL INTERFACE 7

    Select PHYSICAL INTERFACE CONFIGURATION
      INTERFACE CABLE = V35, V36, or EIA232 8
      TRANSMIT CLOCK SOURCE = DCE
      DATA ENCODING = NRZI 9

    Enable PPP CONFIGURATION 10

    Enable SOURCE ROUTE BRIDGE 11

    Select SOURCE ROUTE BRIDGE
      SPANNING TREE MODE = AUTOMATIC
      RING NUMBER = FFO 12
      MAXIMUM TRANSMISSION UNIT = 2052

Select NODE CONFIGURATION
  Enable SOURCE ROUTE BRIDGING 13

  Select SOURCE ROUTE BRIDGING
    BRIDGE NUMBER = 2 14
    Disable LAN BRIDGING PROTOCOL

```

Figure 72. Scenario 7: 6611 Customization via the IBM 6611 MPNP Configuration Program

Notes:

- 1** Enable the token-ring interface.
- 2** This is the locally administered address of the token-ring interface.
- 3** This is the token-ring speed.
- 4** Enable source route bridging on the token-ring interface.

- 5** This is the segment number of the token-ring LAN.
- 6** To be able to bridge the IP protocol, we have to remove this SAP filter.
- 7** Enable the serial interface.
- 8** Specify that a V.35 DTE cable is used in the serial interface.
- 9** The default encoding for the serial link of the IBM 6611 Network Processor is NRZI.
- 10** Enable the PPP configuration for the serial interface.
- 11** Enable source route bridging for the serial interface.
- 12** This is the segment number of the serial link.
- 13** Enable source route bridging at the box level.
- 14** This is the bridge number of the 6611.

4.4.8 Scenario 8: IP Tunnel Bridge Implementation via X.25 Network

In this scenario, we have a 2210A Model 12T with a token-ring LAN, and a 2210B Model 12E with an Ethernet LAN.

The 2210A is a source route-translational bridge, with SRB on the token-ring interface and STB via IP tunnel on serial 1 interface. The 2210A bridge number is 1. The 2211A serial link 1 routes IP and has IP address of 9.67.46.146 with a subnet mask of 255.255.255.240. The segment number of the 2210A token-ring is FFB. The locally administered address of the token-ring interface is 40002210A001. The X.25 address on the 2210A side is 201002600.

The serial link between both is an X.25 link connected via RS-232 modems. This serial link is an IP tunnel encapsulating STB frames. The transparent bridge domain is seen from the source route bridge domain as segment number FFF.

The 2210B with Ethernet LAN is a pure transparent bridge with STB on the Ethernet interface and STB via IP tunnel on serial 1 interface. The 2210B serial link 1 routes IP and has an IP address of 9.67.46.145 with a subnet mask of 255.255.255.240. The X.25 address on the 2210A side is 201002700.

For both 2210s, Serial 2 interface is not used.

In the notes of this scenario, the X.25 interface and IP protocol customization are not fully described. For more information about X.25 interface customization, see 3.4.1, "The X.25 Interface" on page 78. For more information about IP protocol customization, see Chapter 8, "The IBM 2210 as an IP Router" on page 329.

Figure 73 on page 248 shows the configuration of the network used in this scenario.

The customization parameters we used to test this scenario are shown in:

- Figure 74 on page 249 (2210A configuration via an ASCII console)
- Figure 75 on page 257 (2210B configuration via Nways MRS)

Note

We could not bridge IP in this scenario, whereas OS2PING, IPX, NetBIOS, and SNA were bridged with no problem.

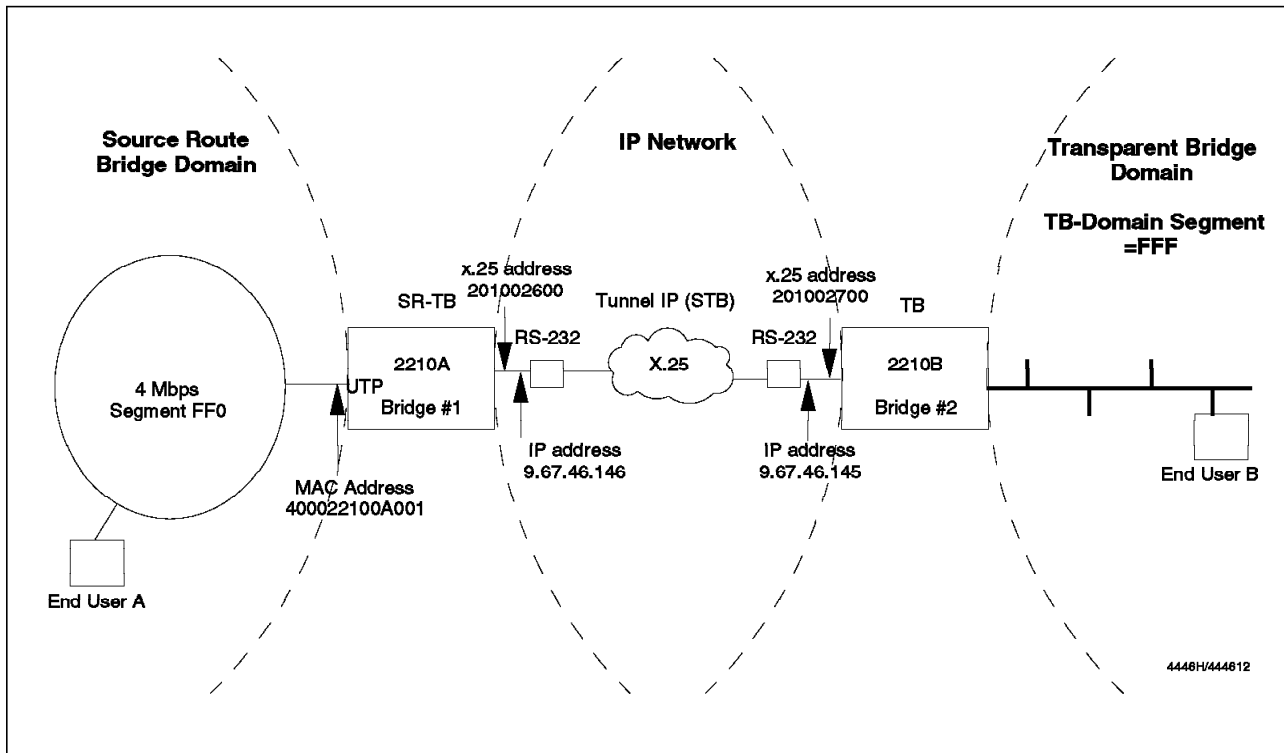


Figure 73. Scenario 8: Tunnel Bridge Configuration with IBM 2210s

```

*
*talk 6 1

Config>list devices 2
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>set data-link x25 1 3
Config>disable interface 2 4
Config>list devices
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN X.25): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
      (Disabled)
Config>network 0 5
Token-Ring interface configuration
TKR config>list 6
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Shielded

RIF Aging Timer:         120
Source Routing:          Enabled
MAC Address:              000000000000
IPX interface configuration record missing

TKR config>media unshielded 7
TKR config>set physical-address 40:00:22:10:a0:01 8
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         120
Source Routing:          Enabled
MAC Address:              40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 9
X.25 User Configuration
:

```

Figure 74 (Part 1 of 6). Scenario 8: 2210A Customization via an ASCII Console

```

:
X.25 Config>list all 10

X.25 Configuration Summary

Node Address:      <none>
Max Calls Out:     4           Inter-Frame Delay: 1
Speed:             9600        Clocking:          External
Cable:             Unknown, assuming DTE (other than X.21)
Default Window:    2           SVC idle:          30 seconds
National Personality: GTE Telenet (DTE)
PVC                low: 0      high: 0
Inbound            low: 0      high: 0
Two-Way            low: 1      high: 64
Outbound           low: 0      high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400

X.25 National Personality Configuration

Follow CCITT: on      OSI 1984:   on      OSI 1988:   off
Clear w/diag: on      Reset w/diag: on      Restart w/diag: on
Request Reverse Charges: on      Accept Reverse Charges: on
Allow Packet Restarts: on      Suppress Calling Addresses: off
Suppress Cause Fields: on      Suppress Frame Idle RRs: off
Frame Extended seq mode: off    Packet Extended seq mode: off
Use Multi-link Addresses: off    Disable Interface Resets: off
Incoming Calls Barred: off      Outgoing Calls Barred: off
Throughput Negotiation: on      Flow Control Negotiation: on
DDN Address Translation: off
Call Request Timer:      20 decaseconds
Clear Request Timer:     18 decaseconds (1 retries)
Reset Request Timer:     18 decaseconds (1 retries)
Restart Request Timer:   18 decaseconds (1 retries)
T1 Timer: 4 seconds      N2 timeouts: 20
T2 Timer: 2 seconds      DP Timer: 500 milliseconds
Standard Version: 1984    Network Type: CCITT
Disconnect Procedure: passive
Window Size      Frame: 7      Packet: 2
Packet Size      Default: 128   Maximum: 256

X.25 protocol configuration

No protocols defined

X.25 PVC configuration

No PVCs defined

X.25 address translation configuration

No address translations defined

:

```

Figure 74 (Part 2 of 6). Scenario 8: 2210A Customization via an ASCII Console


```

:
X.25 Config>set cable rs-232 dte 11
X.25 Config>set address 201002600 12
X.25 Config>set calls-out 1 13
X.25 Config>set default-window-size 7 14
X.25 Config>set svc low-two-way 1 15
X.25 Config>set svc high-two-way 1
X.25 Config>national-personality set packet-size max 512 16
X.25 Config>national-personality disable accept-reverse-charges
X.25 Config>national-personality disable request-reverse-charges
X.25 Config>national-personality disable throughput-class-negotiation
X.25 Config>national-personality disable flow-control-negotiation
X.25 Config>add address ip 17
IP Address [0.0.0.0]? 9.67.46.145
X.25 Address []? 201002700
X.25 Config>add protocol ip 18
Window Size [2]? 7
Default Packet Size [128]? 512
Maximum Packet Size [256]? 512
Circuit Idle Time [30]?
Max VCs [4]? 1
X.25 Config>list all

X.25 Configuration Summary

Node Address:      201002600
Max Calls Out:     1      Inter-Frame Delay: 1
Speed:             9600    Clocking:         External
Cable:             RS-232 DTE
Default Window:    7      SVC idle:         30 seconds
National Personality: GTE Telenet (DTE)
PVC                low: 0   high: 0
Inbound             low: 0   high: 0
Two-Way             low: 1   high: 1
Outbound            low: 0   high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400

X.25 National Personality Configuration

Follow CCITT: on      OSI 1984:   on      OSI 1988:   off
Clear w/diag: on      Reset w/diag: on    Restart w/diag: on
Request Reverse Charges: off  Accept Reverse Charges: off
Allow Packet Restarts: on    Suppress Calling Addresses: off
Suppress Cause Fields: on    Suppress Frame Idle RRs: off
Frame Extended seq mode: off  Packet Extended seq mode: off
Use Multi-link Addresses: off Disable Interface Resets: off
Incoming Calls Barred: off    Outgoing Calls Barred: off
Throughput Negotiation: off   Flow Control Negotiation: off
DDN Address Translation: off

:

```

Figure 74 (Part 3 of 6). Scenario 8: 2210A Customization via an ASCII Console

```

:
Call Request Timer:      20 decaseconds
Clear Request Timer:     18 decaseconds (1 retries)
Reset Request Timer:     18 decaseconds (1 retries)
Restart Request Timer:   18 decaseconds (1 retries)
T1 Timer: 4   seconds    N2 timeouts: 20
T2 Timer: 2   seconds    DP Timer:   500 milliseconds
Standard Version:       1984      Network Type: CCITT
Disconnect Procedure: passive
Window Size      Frame: 7      Packet: 2
Packet Size      Default: 128   Maximum: 512

X.25 protocol configuration

Prot      Window      Packet-size      Idle      Max
Number    Size         Default Maximum   Time      VCs
  0        7          512    512        30        1

X.25 PVC configuration

No PVCs defined

X.25 address translation configuration

IF #      Prot #  Protocol -> X.25 address
  1         0      9.67.46.145 -> 201002700

X.25 Config>exit
Config>protocol asrt      19
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 20
ASRT config>list bridge   21

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: DISABLED
Number of ports added: 1
Port Number: 1    Interface Number: 0 Port Behaviour: STB Only

ASRT config>disable transparent 1      22
ASRT config>enable source-routing 1 FFB 23
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>add tunnel 2              24

:

```

Figure 74 (Part 4 of 6). Scenario 8: 2210A Customization via an ASCII Console

```

:
ASRT config>enable sr-tb-conversion 25
TB-Domain Segment Number in hex(1 - FFF) [1]? FFF
TB-Domain's MTU [1470]?
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: SR<->TB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 1        No. of Source routing segments: 1
SRB: Max ARE Hop cnt: 14              Max STE Hop cnt: 14
SR-TB Conversion: ENABLED  TB-Virtual Segment:0xFFFF  MTU for TB-Domain: 1470
1:N Source Routing:  NOT ACTIVE        Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d on TB ports and IBM-8209 on SR
ports
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number: 1      Interface Number: 0 Port Behaviour: SRB Only
Port Number: 2      Interface Number: Tunnel Port Behaviour: STB Only

ASRT config>list port 26
Port Id (dec)      : 128: 1, (hex): 80-01
Port State         : ENABLED
Port Supports: Source Routing Bridging Only
SRB: Segment Number: 0xFFB          MTU: 4399      STE: ENABLED
Assoc Interface    : 0
Path Cost          : 0
+++++
Port Id (dec)      : 128: 2, (hex): 80-02
Port State         : ENABLED
Port Supports: Transparent Bridging Only
Assoc Interface    : Tunnel
Path Cost          : 0
+++++
ASRT config>tunnel 27
Tunnel interface configuration
TNL config>list all 28
Using multicast tunnel
Base multicast address: 224.186.0.0

TNL config>add address 9.67.46.145 29
TNL config>list all

IP Tunnel Addresses

9.67.46.145

TNL config>exit
ASRT config>exit

:

```

Figure 74 (Part 5 of 6). Scenario 8: 2210A Customization via an ASCII Console

```

:
Config>protocol ip      30
Internet protocol user configuration
IP config>add address 1 9.67.46.146 255.255.255.240      31
IP config>set internal-ip-address 9.67.46.146      32
IP config>list all      33
Interface addresses
IP addresses for each interface:
    intf 0                                IP disabled on this interface
    intf 1  9.67.46.146      255.255.255.240 Network broadcast,    fill 0
    intf 2                                IP disabled on this interface
Internal IP address: 9.67.46.146

Routing

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
    Per-interface address flags:
        intf 0      IP & RIP are disabled on this interface
        intf 1  9.67.46.146      Send net and subnet routes
        intf 2      IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

EGP: disabled

IP config>exit
Config>Ctrl+p
*restart      34
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 74 (Part 6 of 6). Scenario 8: 2210A Customization via an ASCII Console

Notes:

- 1 Talk to the CONFIG process.

- 2** List the configuration of devices (interfaces).
- 3** Set the data link protocol for the serial 1 interface to X.25.
- 4** Interface 2 is not used in this scenario.
- 5** Customization of the network number 0. This is the token-ring LAN interface.
- 6** List the configuration for the token-ring interface.
- 7** The 2210 is connected to the token-ring via the UTP connector. Default is STP.
- 8** This is the locally administered address of the token-ring interface.
- 9** Customization of network 1. This is the serial 1 interface.
- 10** List the entire X.25 configuration of the serial 1 interface.
- 11** Specify that an RS-232 DTE cable is used.
- 12** This is the local X.25 address.
- 13** Set the maximum call-out to 1.
- 14** Set the default window size to 7.
- 15** The range of the SVC number is 1-1. There is only one SVC defined on this interface.
- 16** Set the facilities used for X.25.
- 17** Match a remote IP address with its corresponding remote X.25 address.
- 18** Allow IP protocol to be used via the X.25 link.
- 19** Access the bridging configuration.
- 20** Enable the bridging function at the box level.
- 21** List the bridging configuration.
- 22** Disable transparent bridging (STB) on the token-ring interface.
- 23** Enable source route bridging (SRB) on the token-ring interface port 1 and assign segment number FFB to this interface. Assign bridge number to the 2210.
- 24** Add a tunnel port as port number 2 (STB by default).
- 25** Enable source route-translational bridging (SR-TB) at box level. The transparent bridge domain is seen as LAN segment number FFF from the source route bridge domain.
- 26** List the bridge port configuration.

- 27** Access the tunnel configuration.
- 28** List the tunnel configuration.
- 29** Add the destination IP address of an IP tunnel.
- 30** Access IP protocol configuration.
- 31** Add an IP address for serial link 1. This also enables IP routing on this interface.
- 32** Set the internal IP address equal to the IP address of interface 1.
- 33** List the IP configuration.
- 34** Restart the 2210 to get the configuration running.

```

*
*talk 6 1

Config>list devices 2
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>set data-link x25 1 3
Config>disable interface 2 4
Config>list devices
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN X.25): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
      (Disabled)
Config>network 0 5
Ethernet interface configuration
ETH config>list 6
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 1 7
X.25 User Configuration
X.25 Config>set cable rs-232 dte 8
X.25 Config>set address 201002700 9
X.25 Config>set calls-out 1 10
X.25 Config>set default-window-size 7 11
X.25 Config>set svc low-two-way 1 12
X.25 Config>set svc high-two-way 1
X.25 Config>national-personality set packet-size max 512 13
X.25 Config>national-personality disable accept-reverse-charges
X.25 Config>national-personality disable request-reverse-charges
X.25 Config>national-personality disable throughput-class-negotiation
X.25 Config>national-personality disable flow-control-negotiation
X.25 Config>add address ip 14
IP Address [0.0.0.0]? 9.67.46.146
X.25 Address []? 201002600
X.25 Config>add protocol ip 15
Window Size [2]? 7
Default Packet Size [128]? 512
Maximum Packet Size [256]? 512
Circuit Idle Time [30]?
Max VCs [4]? 1
X.25 Config>list all 16

:

```

Figure 75 (Part 1 of 5). Scenario 8: 2210B Customization via an ASCII Console

```

:
X.25 Configuration Summary

Node Address:      201002700
Max Calls Out:     1      Inter-Frame Delay: 1
Speed:             9600    Clocking:         External
Cable:             RS-232 DTE
Default Window:    7      SVC idle:         30 seconds
National Personality: GTE Telenet (DTE)
PVC                low: 0   high: 0
Inbound            low: 0   high: 0
Two-Way            low: 1   high: 1
Outbound           low: 0   high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400

X.25 National Personality Configuration

Follow CCITT: on      OSI 1984:   on      OSI 1988:   off
Clear w/diag: on      Reset w/diag: on    Restart w/diag: on
Request Reverse Charges: off  Accept Reverse Charges: off
Allow Packet Restarts:  on    Suppress Calling Addresses: off
Suppress Cause Fields:  on    Suppress Frame Idle RRs: off
Frame Extended seq mode: off  Packet Extended seq mode: off
Use Multi-link Addresses: off Disable Interface Resets: off
Incoming Calls Barred:  off    Outgoing Calls Barred:  off
Throughput Negotiation: off    Flow Control Negotiation: off
DDN Address Translation: off
Call Request Timer:     20 decaseconds
Clear Request Timer:    18 decaseconds (1 retries)
Reset Request Timer:    18 decaseconds (1 retries)
Restart Request Timer:  18 decaseconds (1 retries)
T1 Timer: 4   seconds   N2 timeouts: 20
T2 Timer: 2   seconds   DP Timer: 500 milliseconds
Standard Version: 1984   Network Type: CCITT
Disconnect Procedure: passive
Window Size   Frame: 7   Packet: 2
Packet Size   Default: 128 Maximum: 512

X.25 protocol configuration

Prot      Window      Packet-size      Idle      Max
Number    Size         Default Maximum   Time      VCs
  0        7          512    512         30        1

X.25 PVC configuration

No PVCs defined

X.25 address translation configuration

IF #      Prot #  Protocol -> X.25 address
  1         0     9.67.46.146 -> 201002600

:

```

Figure 75 (Part 2 of 5). Scenario 8: 2210B Customization via an ASCII Console


```

:
X.25 Config>exit
Config>protocol asrt 17
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 18
ASRT config>list bridge 19

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: DISABLED
Number of ports added: 1
Port Number: 1    Interface Number: 0 Port Behaviour: STB Only

ASRT config>add tunnel 2 20
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: STB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: DISABLED
Number of ports added: 2
Port Number: 1    Interface Number: 0 Port Behaviour: STB Only
Port Number: 2    Interface Number: Tunnel Port Behaviour: STB Only

ASRT config>tunnel 21
Tunnel interface configuration
TNL config>list all 22
Using multicast tunnel
Base multicast address: 224.186.0.0

TNL config>add address 9.67.46.146 23
:

```

Figure 75 (Part 3 of 5). Scenario 8: 2210B Customization via an ASCII Console

```

:
TNL config>list all

IP Tunnel Addresses

    9.67.46.146

TNL config>exit
ASRT config>exit
Config>protocol ip      24
Internet protocol user configuration
IP config>add address 1 9.67.46.145 255.255.255.240      25
IP config>set internal-ip-address 9.67.46.145      26
IP config>list all      28
Interface addresses
IP addresses for each interface:
    intf 0                                IP disabled on this interface
    intf 1  9.67.46.145      255.255.255.240 Network broadcast, fill 0
    intf 2                                IP disabled on this interface
Internal IP address: 9.67.46.145

Routing

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
    Per-interface address flags:
        intf 0                                IP & RIP are disabled on this interface
        intf 1  9.67.46.145      Send net and subnet routes
        intf 2                                IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

EGP: disabled

:

```

Figure 75 (Part 4 of 5). Scenario 8: 2210B Customization via an ASCII Console

```

:
IP config>exit
Config>Ctrl+p
*restart 29
Are you sure you want to restart the gateway? (Yes or [No]): Yes

```

```

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

```

```

MOS Operator Control

```

```

*
```

Figure 75 (Part 5 of 5). Scenario 8: 2210B Customization via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** List the configuration of devices (interfaces).
- 3** Set the data link protocol for the serial 1 interface to X.25.
- 4** Interface 2 is not used in this scenario.
- 5** Customization of the network number 0. This is the Ethernet LAN interface.
- 6** List the configuration for the Ethernet interface.
- 7** Customization of network 1. This is the serial 1 interface.
- 8** Specify that an RS-232 DTE cable is used.
- 9** This is the local X.25 address.
- 10** Set the maximum call-out to 1.
- 11** Set the default window size to 7.
- 12** The range of the SVC number is 1-1. There is only one SVC defined on this interface.
- 13** Set the facilities used for X.25.
- 14** Match a remote IP address with its corresponding remote X.25 address.
- 15** Allow IP protocol to be used via the X.25 link.
- 16** List the entire X.25 configuration for serial 1.

- 17** Access the bridging configuration.
- 18** Enable the bridging function at the box level.
- 19** List the bridging configuration.
- 20** Add a tunnel port as port number 2 (STB by default).
- 21** Access the tunnel configuration.
- 22** List the tunnel configuration.
- 23** Add the destination IP address of the IP tunnel.
- 24** Access IP protocol configuration.
- 25** Add an IP address for serial link 1. This enables IP routing on this interface.
- 26** Set the internal IP address equal to the IP address of the interface 1.
- 27** List the IP configuration.
- 27** Restart the 2210 to get the configuration running.

4.4.9 Scenario 9: SRB Source Routing Bridge with Frame Relay

In this scenario, we have two 2210 Model 121T with frame relay with a token-ring LAN.

Both 2210s are connected to each other over a FR link via a pair of V.35 modems. Both 2210s are configured for SRB (Source Route Bridging) over their respective token-ring LANs and the FR link.

Figure 76 shows the configuration of the network used in this scenario.

The customization parameters we used to test this scenario are shown in:

- Figure 77 on page 264 (2210 configuration via an ASCII console)
- Figure 78 on page 271 (2210 configuration via Nways MRS)

The 2210 token-ring LAN interface is attached to the segment number FF0 and the bridge number of the 2210A is 1. The locally administered address of the 2210A token-ring interface is 40002210A001. We have assigned the IP address of 9.67.46.146 (subnet mask is 255.255.255.240).

The 2210 token-ring LAN interface is attached to the segment number FF2 and the bridge number of 2210B is 2. The locally administered address of the 2210B token-ring interface is 40006611B001.

The segment number for the FR link is FF1.

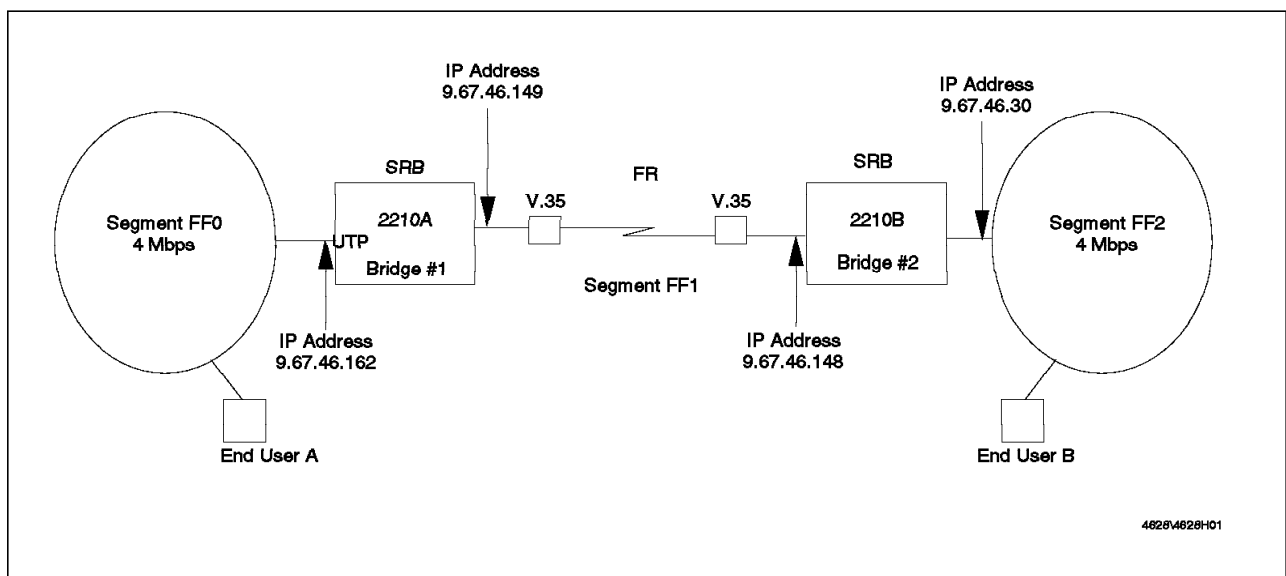


Figure 76. Scenario 9: SRB Configuration between Two IBM 2210s with FR

```

*
*talk 6 1

Config>list devices 2
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN FR): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN SDLC): CSR 81640, CSR2 80E00, vector 92
Config>network 0 3
Token-Ring interface configuration
TKR config>list 4
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                4 Mb/sec
Media:                Shielded

RIF Aging Timer:      120
Source Routing:       Enabled
MAC Address:          440022101201
IPX interface configuration record missing

TKR config>media unshielded 5
TKR config>set physical-address 40:00:22:10:A0:01 6
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                4 Mb/sec
Media:                Unshielded

RIF Aging Timer:      120
Source Routing:       Enabled
MAC Address:          440022101201
IPX interface configuration record missing

TKR config>exit
Config>network 1 7
Frame Relay user configuration
FR Config>list hdlc 8
Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0
FR Config>list all 9

```

Figure 77 (Part 1 of 5). Scenario 9: 2210 Customization via an ASCII Console

Frame Relay HDLC Configuration

```

Encoding      = NRZ IDLE          = Flag
Clocking      = External
Cable type    = V.35 DTE
Line access rate bps = 64000  Interface MTU in bytes = 2048
Transmit delay = 0

```

Frame Relay Configuration

```

LMI enabled = Yes  LMI DLCI      = 0
LMI type    = ANSI LMI Orphans OK = Yes

Protocol broadcast = Yes  Congestion monitoring = Yes
Emulate multicast  = Yes  CIR monitoring        = No

PVCs P1 allowed   = 64  CIR monitor adjustment = 1
Timer T1 seconds  = 10  Counter N1 increments  = 6
LMI N2 error threshold = 3  LMI N3 error threshold window = 4

```

```

Maximum PVCs allowable = 64
Total PVCs configured  = 1

```

Circuit Name	Circuit Number	Circuit Type	CIR in bps	Burst Size	Ex Bu
-----	-----	-----	-----	-----	---
2210b	492	Permanent	64000	64000	0

FR Config>exit

Config>disable interface 2 **12**

Config>list devices

```

Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN FR): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN SDLC): CSR 81640, CSR2 80E00, vector 92
(Disabled)

```

Config>protocol asrt **13**

Adaptive Source Routing Transparent Bridge user configuration

Figure 77 (Part 2 of 5). Scenario 9: 2210 Customization via an ASCII Console

```

ASRT config>enable bridge 14
ASRT config>list bridge 15

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  0      No. of Source routing segments: 0
SRB: Max ARE Hop cnt:  0      Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE      Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 1
Port Number:  1      Interface Number:  0 Port Behaviour: STB Only

ASRT config>disable transparent 16
Port Number [1]? 1
ASRT config>enable source-routing 17
Port Number [1]? 1
Segment Number for the port in hex(1 - FFF) [1]? FF0
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>add port 18
Interface Number [0]? 1
Port Number [2]? 2
ASRT config>disable transparent 19
Port Number [1]? 2
ASRT config>enable source-routing 20
Port Number [1]? 2
Segment Number for the port in hex(1 - FFF) [1]? FF1
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: SRB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  1      No. of Source routing segments: 2
SRB: Max ARE Hop cnt:  14      Max STE Hop cnt: 14
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE      Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IBM-SRB proprietary
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number:  1      Interface Number:  0 Port Behaviour: SRB Only
Port Number:  2      Interface Number:  1 Port Behaviour: SRB Only

```

Figure 77 (Part 3 of 5). Scenario 9: 2210 Customization via an ASCII Console


```

ASRT config>exit
Config>protocol hst      21
TCP/IP-Host Services user configuration
TCP/IP-Host config>set ip-host address      22
IP-Host address [0.0.0.0]? 9.67.46.30
Address mask [255.0.0.0]? 255.255.255.240
IP-Host address set.

TCP/IP-Host config>list all      23

IP-Host IP address : 9.67.46.30
Address Mask       : 255.255.255.240

Default Gateway IP address
0.0.0.0.0
9.67.46.20

TCP/IP-Host Services Enabled.

RIP-LISTENING Enabled.
Router Discovery Enabled.

TCP/IP-Host config>exit
Config>Ctrl+p
*restart      24
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control
*talk 5      25

CGW Operator Console

:

```

Figure 77 (Part 4 of 5). Scenario 9: 2210 Customization via an ASCII Console

```

:
+protocol asrt 26
ASRT>list bridge 27
Bridge ID (prio/add): 32768/02-00-44-08-05-80
Bridge state: Enabled
Bridge type: SRB
Bridge capability: ASRT
Number of ports: 2
STP Participation: IBM-SRB proprietary

Port Interface State MAC Address Modes Maximum MSDU Segment
1 TKR/0 Up 02-00-44-08-05-80 SR 2096 FF0
2 PPP/0 Up 00-00-00-00-00-00 SR 1504 FF1

SR bridge number: 1
SR virtual segment: 000
Adaptive segment: 000

-----
LMI enabled = Yes LMI DLCI = 0
LMI type = ANSI LMI Orphans OK = Yes
LMI sequence interval seconds = 10

Protocol broadcast = Yes Congestion monitoring = Yes
Emulate multicast = Yes CIR monitoring = No
PVCs P1 allowed = 64 Interface MTU in bytes = 2048
Line access rate bps = 64000 CIR monitor adjustment = 1
Timer T1 seconds = 10 Counter N1 increments = 6
LMI N2 threshold = 3 LMI N3 threshold window = 4

Current receive sequence = 240
Current transmit sequence = 8
Total status enquires = 214 Total status responses = 21
Total sequence requests = 1069 Total responses = 106

PVC Status:
-----
Total allowed = 64 Total configured = 1
Total active = 1 Total congested = 0
Total left net = 0 Total join net = 0

Circuit# Circuit Name Orphan Type/ Frames Fra
-----
460 Unassigned Yes P/I 0
492 2210b No P/A 91495
502 Unassigned Yes P/I 0

A - Active I - Inactive R - Removed
P - Permanent M - Multicast C - Congested
FR>exit
+Ctrl+p

```

Figure 77 (Part 5 of 5). Scenario 9: 2210 Customization via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** List the configuration of devices (interfaces).
- 3** Customization of the network number 0. This is the token-ring LAN interface.
- 4** List the configuration of the token-ring interface.
- 5** The 2210 is connected to the token-ring LAN via a UTP cable. Default is STP.
- 6** This is the locally administrated address of the token-ring interface.
- 7** Customization of network 1. This is the serial 1 interface.
- 8** List the configuration of HDLC parameters for the serial 1 interface.
- 9** The default encoding for the serial link on the IBM 2210 is NRZI.
- 10** Specify that a V.35 DTE cable is used.
- 11** List the configuration of serial 1.
- 12** Interface 2 is not used in this scenario.
- 13** Access the bridging configuration.
- 14** Enable the bridging function at the box level.
- 15** List the bridging configuration.
- 16** Disable transparent bridging (STB) on the token-ring interface.
- 17** Enable source route bridging (SRB) on the token-ring interface. Assign the segment number FF0 to the token-ring segment, and assign the bridge number 1 to the 2210.
- 18** Add a bridging port for the serial 1 interface (interface 1). The port number is 2.
- 19** Disable transparent bridging (STB) on the serial 1 interface.
- 20** Enable source route bridging (SRB) on the serial 1 interface. Assign the segment number FF1 to the serial interface. This is the same segment number assigned to the serial interface on the 2210.
- 21** Access the TCP/IP host configuration.
- 22** Set an IP address at the box level.
- 23** List the TCP/IP host configuration.
- 24** Restart the 2210A to get the configuration running.

25 The configuration is now running on the 2210A. We access the CGW operator console to monitor the running configuration.

26 Access the bridging monitoring function.

27 List the bridge configuration. Note that both interfaces are active.

28 Access the serial 1 monitoring.

29 List the serial 1 configuration. Note the local and remote statistics.

On 2210 Navigation Window

Select CONFIGURE from the menu bar
Select NEW CONFIGURATION **1**

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :

Select MODEL

Select **MODEL 12T** **2**

Select CONFIGURATION of Token-Ring line

ENABLE INTERFACE

MAC ADDRESS = **40002210A001** **3**

Select SPEED

Select 4

Select PACKET SIZE

Select 2052

Select CABLE TYPE

Select **UTP** **4**

RIF TIMER = 120

DISABLE END NODE SOURCE ROUTING

Select the Frame Relay protocol of Serial 1 (FR by default)

Select FR

Select CONFIGURATION of Serial 1

On GENERAL subpanel :

ENABLE INTERFACE

MAXIMUM TRANSMISSION UNIT = 2048

Select ENCODING

Select **NRZI** **5**

Select IDLE

Select FLAG

Select CLOCKING

Select EXTERNAL

CLOCK SPEED = 0

TRANSMIT DELAY = 0

Select CABLE TYPE

Select **V35 DTE** **6**

Select subpanel LCP **7**

RETRY TIMER = 3000

CONFIG TRIES = 20

NAK TRIES = 10

TERMINATE TRIES = 10

MAXIMUM RECEIVE UNIT = 2048

Select subpanel BNCP **7**

ENABLE MAGIC NUMBER

DISABLE TINYGRAM COMPRESSION

Select subpanel IPCP **7**

DISABLE IP Compression

Number of Slots = 16

DISABLE SEND IP ADDRESS

DISABLE REQUEST IP ADDRESS

:

Figure 78 (Part 1 of 3). Scenario 9: 2210 Customization via the Nways MRS Configuration Program

```

:
  Select CONFIGURATION of Serial 2
    On GENERAL subpanel :
      DISABLE INTERFACE 8

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 9
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 1 10
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 1
  Select LF BIT INTERPRETATION
    Select EXTENDED
  ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
  DISABLE SR <-> TB CONVERSION

In TRANSPARENT BRIDGE box
  FILT. DBASE SIZE = 2048
  AGING TIME = 300
  RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE TOKEN-RING 11
Select CONFIGURE of Token-Ring
  Select INTERFACE SUPPORTS
    Select SRB 12
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = FF0 13
  MTU UNIT = 4399
  ENABLE STE

ENABLE SERIAL 1 14
Select CONFIGURE of Serial 1
  Select INTERFACE SUPPORTS
    Select SRB 15
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = FF1 16
  MTU UNIT = 4399
  ENABLE STE
:

```

Figure 78 (Part 2 of 3). Scenario 9: 2210 Customization via the Nways MRS Configuration Program

```

:
DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

On 2210 Navigation Window :
Select TCP/IP Host Services panel of TCP/IP Host Services subdirectory of BRIDGING directory

On TCP/IP Host Services Window :
ENABLE IP-HOST SERVICES
ENABLE ROUTER DISCOVERY
DISABLE RIP-LISTENING
IP-HOST ADDRESS = 9.67.46.146      17
IP-HOST MASK = 255.255.255.240
In DEFAULT GATEWAY IP ADDRESS
Nothing Customized

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION      18

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter SRBBI      19
Select OK

```

Figure 78 (Part 3 of 3). Scenario 9: 2210 Customization via the Nways MRS Configuration Program

Notes:

- 1 Start the customization from an empty configuration.
- 2 This is a 2210 Model 12T with a token-ring interface, 4 MB of Flash, and 8 MB of RAM.
- 3 This is the locally administered address of the token-ring interface.
- 4 The 2210 is connected to the token-ring LAN using the UTP connector. The default is STP.
- 5 The default encoding for the serial link on the IBM 6611 Network Processor is NRZI.
- 6 Specify that an RS-232 DTE cable is used for serial 1.
- 7 This subpanel has not been changed. Default settings are used for all the parameters.
- 8 This interface 2, corresponding to WAN 2 (Serial 2) is unused.
- 9 Interface 2 is not used in this scenario.
- 10 The bridge number of 2210 is 1.
- 11 Enable the token-ring interface for bridging.
- 12 Enable source route bridging on the token-ring interface.

- 13** This is the segment number for the token-ring LAN interface.
- 14** Enable the serial 1 interface for bridging.
- 15** Enable source route bridging on the serial 1 interface.
- 16** This is the segment number for the serial link interface.
- 17** Set an IP address at the box level.
- 18** Create the configuration file that will be loaded to the IBM 2210 using TFTP. Note that TFTP must be initiated from the IBM 2210.
- 19** This is the name of the configuration file stored in your workstation.

Chapter 5. Frame Relay Boundary Access Node

This chapter describes the boundary access node (BAN) feature on the IBM 2210. BAN provides a reliable low-cost way for attached PU Type 2.0 and 2.1 endstations to communicate with an SNA environment across wide area links. It includes the following sections:

- About the Boundary Access Node Feature
- Benefits of BAN
- How BAN Works
- Bridged Versus DLCw BAN
- Which Method Should You Use
- Using the BAN Feature
- Using Multiple DLCIs

Note: NCP support for FR BAN has been introduced with NCP Version 7 Release 3. V7R1 or V7R2 will require PTFs, which provide the BAN support (IR28273 MVS-IR28274 VM-IR28274 VSE). NCP FR BAN does not support connections to SNA type 4 and type 5 nodes.

5.1 About the Boundary Access Node Feature

BAN can be used to attach to any of the following SNA node types:

- End nodes
- Network nodes
- Subarea nodes

NCP is an example of a subarea node, that in conjunction with VTAM compose an APPN network node.

The BAN feature is an enhancement of the frame relay, DLSw, and Adaptive Source Route Bridging (ASRT) capabilities of the IBM 2210 software. This feature enables IBM Type 2.0 and 2.1 endstations connected to an IBM 2210 to make a direct connection via frame relay to an SNA node supporting the RFC 1490 Bridged 802.5 (token-ring) Frame format. The BAN feature provides a better, less costly way of communication with the IBM SNA environment. IBM has modified the IBM Network Control Program software in the IBM 3745 (NCP) to support this enhancement.

When using BAN, endstations function as if they are directly connected to an SNA node via token-ring, Ethernet, or SDLC lines as shown in Figure 79 on page 276. Though their data actually passes through an IBM 2210 and over a frame relay network, this is transparent to the endstations.

Note: For more information about NCP, look at *NCP Version 7 Release 3 Redbook*, SG24-2592-00.

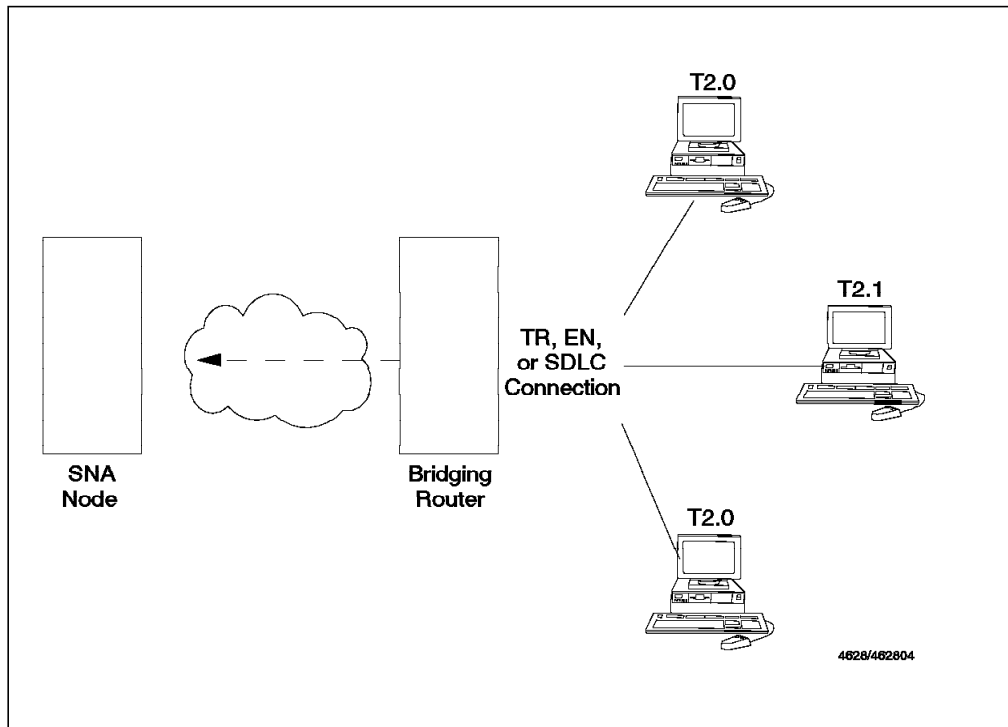


Figure 79. Boundary Access Node

5.2 Benefits of BAN

Designed to meet the needs of customers who do not require a full DLSw implementation, BAN provides an economical method for connection to IBM environments. Offering a path to full DLSw capability, BAN provides the following three major benefits to customers who need to internetwork with the IBM environment:

- Ability to bridge Ethernet or token-ring traffic directly to the SNA node without frame conversion by another DLSw router. This can save capital equipment costs by eliminating the need for another router and a host at a central site.
- No architectural limits to the number of multiplexed LLC Type 2 (LLC connections over a single frame relay data link connection identifier (DLCI). In contrast, the existing NCP frame relay boundary network node (BNN) support limits the number of LLC2 connections per DLCI to 127. This can save significantly on frame relay DLCI provider costs.
- Eliminates the need to configure endstation addresses on the DLSw router that is local to the endstations. This makes it easier to configure and manage the BAN setup.

Note: You can use BAN DLCI for IP traffic. This allows you to manage the router (via SNMP) over the same DLCI you are using for SNA (via BAN).

5.3 How BAN Works

The BAN feature in the router works by filtering the frames sent by type 2.0 or 2.1 endstations. Each BAN frame is modified by the router to comply with bridged 802.5 (token-ring) frame format. The router examines each frame and allows only those with the BAN DLCI MAC address to pass over a DLCI to the mainframe. The destination MAC address in the bridge 802.5 frame is replaced with the boundary node identifier in frames destined for the SNA node.

With BAN, only one DLCI ordinary is needed. However, BAN may use many DLCI connections between the router and the IBM environment. In some cases you may want to set up more than one DLCI to handle BAN traffic.

There are two ways to use the BAN feature:

- Straight bridging using the IBM 2210's bridging capability
- DLSw terminated in which BAN terminates the LLC2 connection at the router running DLSw

The sections that follow explain how to configure each method.

5.4 Bridged versus DLSw BAN

You can implement BAN in two ways: straight bridging and DLSw terminated. With straight bridging, you configure BAN to bridge LLC2 frames from Type 2.0 or Type 2.1 endstations straight into the SNA node. With DLSw terminated, BAN terminates the LLC2 connection at the router running DLSw.

In this discussion, we refer to straight bridging as BAN Type 1 and DLSw terminated as BAN Type 2.

Figure 80 on page 278 shows a BAN Type 1 (Bridged) connection. In this figure, notice that the router does not terminate the LLC2 traffic received from attached endstations. Instead, the router converts the frames it receives to bridged token-ring format (RFC 1490) frames and bridges directly to the SNA node.

SDLC devices can be supported using BAN Type 1 connections via DLSw. In this case, the router converts the LLC2 frames to bridged token-ring format frames (RFC 1490) and bridges directly to the SNA node.

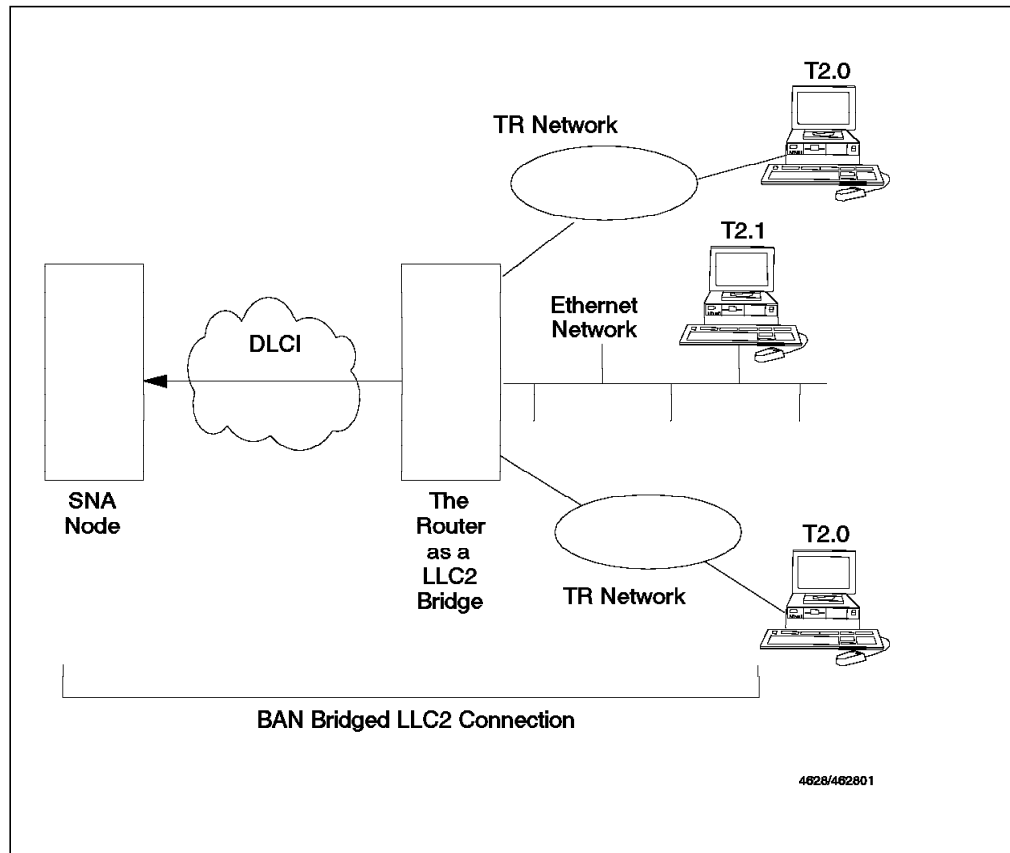


Figure 80. Bridged BAN

The router acts as a bridge between the SNA node and the endstations. A DLSw does not terminate LLC2 sessions at the router, as does BAN Type 2 Endstation frames can be token-ring, SDLC (not pictured) or Ethernet format, provided the bridge is configured to support that type of frame.

Figure 81 on page 279 shows a BAN Type 2 (Virtual BAN DLSw) connection. In this figure, notice that the DLSw router does not function as a bridge. The router terminates the LLC2 traffic received from attached endstations. At the same time, the router establishes a new LLC2 connection to the SNA node over the frame relay network. Thus, though two LLC2 connections exist within the transaction, the break between them is transparent for both the SNA node and the endstations. The result is a virtual LLC2 between the SNA node and the endstations.

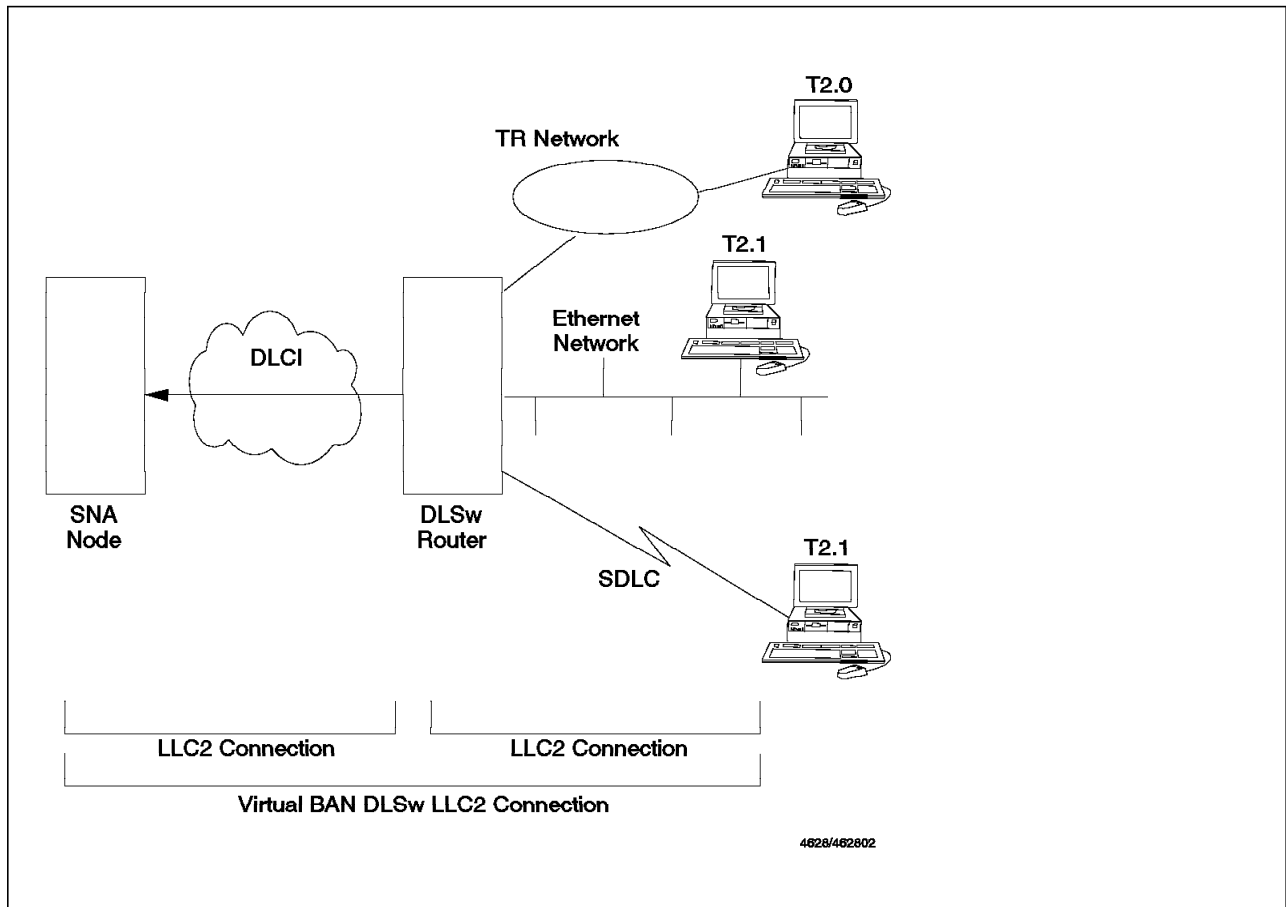


Figure 81. LLC2 Terminated

The SDLC session is terminated in the router, and a separate LLC2 session exists between the router and the SNA node. The SDLC station appears to the SNA node as a frame-relay attached station.

Remote DLSw is supported for both types of BAN. Either BAN type connections can be used by routers functioning as DLSw partners to connect.

5.4.1 Which Method Should You Use

Straight bridging of frames (BAN Type 1) is generally preferred because it provides fast delivery of data with minimal network overhead. However, there are exceptions. If usage on a DLCI is too high, session timeout might occur in a bridged configuration. Conversely, session timeouts rarely occur in a DLSw configuration (BAN Type 2) since this type of configuration terminates and then recreates LLC2 sessions at the local router (DLSw).

5.5 Using the BAN Feature

To use the BAN feature, you must:

1. Configure the router for frame relay (FR)
2. Configure the router for Adaptive Source Route Bridging (ASRT)
3. Configure the router for BAN
4. Open service access points (SAPs) on the frame relay and LAN interfaces

5.6 Using Multiple DLCIs for BAN Traffic

Setting up multiple DLCIs is simple, particularly if you do this during the initial BAN configuration. When setting up multiple connections, remember that each frame relay DLCI corresponds to a specific SNA node in the IBM environment. To pass BAN frames to that SNA node, you must specify the correct circuit number when establishing the frame relay connection. Your frame relay provider can give you the circuit number for each of your connections.

While one DLCI is usually sufficient to handle BAN traffic to and from the IBM environment, setting up two or more DLCIs may prove useful in some circumstances.

5.7 BAN Scenario

Figure 82 on page 281 shows how to configure BAN on the 2210.

Configuring the Router for Frame Relay

***t 6**

Config>**net 0**

Token-Ring interface configuration

TKR config>**speed 4**

TKR config>**media shield**

TKR config>**list all**

Token-Ring configuration:

Packet size (INFO field): 2052

Speed: 4 Mb/sec

Media: Shielded

RIF Aging Timer: 120

Source Routing: Enabled

MAC Address: 000000000000

IPX interface configuration record missing

TKR config>**exit**

Config>**set data-link frame-relay 1**

Config>**network 1**

Frame Relay user configuration

FR Config>**add permanent**

Circuit number <16>? **32**

Committed Information Rate (CIR) in bps <64000>?

Committed Burst Size (Bc) in bits <64000>?

Excess Burst Size (Be) in bits <0>?

Assign circuit name <>? **testban**

FR Config>**set clocking external**

FR Config>**list all**

Frame Relay HDLC Configuration

Encoding	= NRZ	IDLE	= Flag
Clocking	= External		
Cable type	= V.35	DTE	
Line access rate bps	= 64000	Interface MTU in bytes	= 2048
Transmit delay	= 0		

Frame Relay Configuration

LMI enabled	= Yes	LMI DLCI	= 0
LMI type	= ANSI	LMI Orphans OK	= Yes
Protocol broadcast	= Yes	Congestion monitoring	= Yes
Emulate multicast	= Yes	CIR monitoring	= No
PVCs P1 allowed	= 64	CIR monitor adjustment	= 1
Timer T1 seconds	= 10	Counter N1 increments	= 6
LMI N2 error threshold	= 3	LMI N3 error threshold window	= 4

--More--

Figure 82 (Part 1 of 5). Configuring 2210 for BAN from the ASCII Console

```
Maximum PVCs allowable = 64
Total PVCs configured = 1
```

Circuit Name	Circuit Number	Circuit Type	CIR in bps	Burst Size	Excess Burst
testban	32	Permanent	64000	64000	0

No address translations configured

Configuring The Router For ASRT

```
FR Config> exit
config>
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port
Interface Number <0>?
Port Number <1>?1
ASRT config>disable transparent
Port Number <1>?
ASRT config>enable source-routing
Port Number <1>?
Segment Number for the port in hex(1 - FFF) <1>? 101
Bridge number in hex (1 - 9, A - F) <1>? 1
ASRT config>
ASRT config>add port
Interface Number <0>? 1
Port Number <2>?
Assign circuit name <>? testban
ASRT config>disable transparent
Port Number <1>? 2
ASRT config>enable source-routing
Port Number <1>?2
Segment Number for the port in hex(1 - FFF) <1>? 9FF
ASRT config>
```

Note: The number that you assign will be the FR interface number of the bridge.

Figure 82 (Part 2 of 5). Configuring 2210 for BAN from the ASCII Console

ASRT config>**List bridge**

Source Routing Transparent Bridge Configuration

=====

```
Bridge:                Enabled                Bridge Behaviour: SRB
+-----+
| SOURCE ROUTING INFORMATION |-----+
+-----+

Bridge Number:         01                Segments:         2
Max ARE Hop Cnt:       14                Max STE Hop cnt:  14
1:N SRB:               Not Active        Internal Segment: 0x000
LF-bit interpret:      Extended

+-----+
| SR-TB INFORMATION |-----+
+-----+

SR-TB Conversion:      Disabled
TB-Virtual Segment:    0x000                MTU of TB-Domain:  0

+-----+
| SPANNING TREE PROTOCOL INFORMATION |-----+
+-----+

Bridge Address:        Default            Bridge Priority:   32768/0x8000
STP Participation:     IBM-SRB proprietary

+-----+

+-----+
| TRANSLATION INFORMATION |-----+
+-----+

FA<=>GA Conversion:     Enabled            UB-Encapsulation: Disabled
DLS for the bridge:     Disabled

+-----+
| PORT INFORMATION |-----+
+-----+

Number of ports added: 2
Port:  1      Interface:    0      Behaviour:   SRB Only   STP: Enabled
Port:  2      Interface:    1      Behaviour:   SRB Only   STP: Enabled
Circuit name: testban
```

Configuring The Router For BAN

```
ASRT config>
ASRT config>BAN
BAN (Boundary Access Node) configuration
BAN config>ADD
Port Number <0>? 2
Enter the BAN DLCI MAC Address <?> 400000000002
Enter the Boundary Node Identifier MAC Address <4FFF00000000>?
Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) <b>?
BAN port record added.
Reminder: enable source-routing on the port if you have not already done so.
BAN config>
```

Figure 82 (Part 3 of 5). Configuring 2210 for BAN from the ASCII Console

BAN config>**List**

bridge	BAN	Boundary	bridged or	
port	DLCI	MAC Address	Node Identifier	DLSw terminated
2	40:00:00:00:00:02	4F:FF:00:00:00:00	bridged	

Note: NCP Version 7 Release 3, the 2210 and 6611 all default the NCP virtual MAC ADDRESS TO HEXADECIMAL 4FFF00000000, so in practically all cases, configuration of the address is not required.

Opening SAPs

BAN config>**Exit**

Config>protocol dls

DLSw protocol user configuration

DLSw config>**open**

Interface # <1>?

Enter SAP in hex (range 0-ff) <0>? 4

DLSw config>**open**

Interface # <1>? 0

Enter SAP in hex (range 0-ff) <0>? 4

DLSw config>**list open**

Interface SAP

1 4

0 4

DLSw config>

Enabling Event Logging System

Config>**Ev**

Event logging system user configuration

ELS config>**Display Subsystem Ban All**

ELS config>

Note: Entering this command you will be able to display all BAN messages

*** restart**

Are you sure you want to restart the gateway? (Yes or <N>): Y

Figure 82 (Part 4 of 5). Configuring 2210 for BAN from the ASCII Console

Copyright Notices:
 Copyright 1985-1995 Proteon, Inc.
 Copyright 1984-1987, 1989 by J. Noel Chiappa
 Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

***t 5**

+protocol asrt

ASRT>**ban**

BAN (Boundary Access Node) console

BAN>**list**

bridge	BAN	Boundary	bridged or	
port	DLCI MAC Address	Node Identifier	DLSw terminated	Status
2	40:00:00:00:00:02	4F:FF:00:00:00:00	bridged	U

BAN>**Exit**

T5

+network 1

Frame Relay Console

FR>**list circuit**

Circuit number <16>? **32**

Circuit name = testban

Circuit state	=	Active	Circuit is orphan	=	No
Frames transmitted	=	32	Bytes transmitted	=	3367
Frames received	=	15	Bytes received	=	1926
Total FECNs	=	0	Total BECNs	=	0
Times congested	=	0	Times Inactive	=	0
CIR in bits/second	=	64000	Current Info Rate	=	64000
Committed Burst (Bc)	=	64000	Excess Burst (Be)	=	0

Xmit frames dropped due to queue overflow	=	0
---	---	---

FR>**Exit**

Figure 82 (Part 5 of 5). Configuring 2210 for BAN from the ASCII Console

On 2210 Navigation Window select

CONFIGURE from the menu bar
NEW CONFIGURATION

On panel of DEVICE INTERFACES window select

Model 12T
0 Token Ring Configure
Enable interface
Mac Address 000000000000
Speed 4
Packet Size 2052
Cable-Type STP
Rif Timer 120

Serial 1 Frame Relay
Frame Relay Configure

In option GENERAL

Enable interface
Encoding NRZ
Clocking External
Transmit Delay 0
Idle Flag
Clock Speed 0
Cable Type V.35DTE

In Option LMI

LMI Type ANSI
Enable:
Orphan Circuits
Protocol Broadcast
Multicast Emulation
Congestion Monitor

Frame Size (MTU) 2048
P1 64 T1 10 N1 6
N2 3 N3 4

Cir adjustment 1
Line Speed 64000

In Option PVCs

Line Speed 64000
Committed 64000
Excess 0

Protocol IP

Figure 83 (Part 1 of 3). Configuring 2210 for BAN from the Configuration Program

```

In Option BAN
Boundary Node  4FFF00000000
Termination    Bridged
Segment Numb   1
ADD

Disable Serial 2

On Panel Navigation window Select
Bridging and Interfaces

In Option General
Enable Bridging

In Option SRB
Bridge Numb     1
Max ARE         14
Max STE         14
Internal Virt    0B0
LF Bit          Extended
Enable          FA-GA

In Option SRTB
Disable

In Option TB
Filt Dbase      2048
Aging Time      300
Resolution      5

On Panel NAVIGATION WINDOW select
Bridging Interfaces

In Option Interface
Enable interface 0 Token-Ring

In Option Configure
Interface        SRB
Duplicate        STETSF
Segment          101
MTU Size         4399
Enable STE
Enable Spanning Tree

```

Figure 83 (Part 2 of 3). Configuring 2210 for BAN from the Configuration Program

Configuring BAN for Data Link Switch

***t 6**

Config>**Protocol ASRT**

Adaptive Source Routing Transparent Bridge user configuration

ASRT config>**BAN**

BAN (Boundary Access Node) configuration

BAN config>**Delete port**

Port number <0>? **2**

BAN config>

BAN config>**Add port**

Port number <0>? **2**

Enter the BAN DLCI MAC Address <>? **400000000002**

Enter the Boundary Node Identifier MAC Address <4FFF00000000>?

Do you want the traffic bridged(b) or DLSw terminated (t) (b/t) **t**

BAN port record added

Reminder: enable source-routing on the port if you have not already done so

BAN config>**Exit**

ASRT config> **Enable DLS**

ASRT config>

ASRT config> **Disable bridge**

ASRT config> **Exit**

Config> **Ctrl+p**

***restart**

Are you sure that you want to restart the gateway? (Yes or <N>) **Y**

bridge	BAN	Boundary	bridged or
port	DLCI MAC Address	Node Identifier	DLSw terminated
2	40:00:00:00:00:02	4F:FF:00:00:00:00	terminated

Figure 83 (Part 3 of 3). Configuring 2210 for BAN from the Configuration Program

Chapter 6. LAN Network Manager Support

This chapter describes the LAN Network Manager feature implemented in the IBM 2210. The LNM support allows the possibility of using LNM Network Management in a bridged IBM 2210 network as it is used for other SR bridges. This chapter includes the following sections:

- LNM Implementation in the IBM 2210
- LNM Configuring Commands
- LNM Scenarios and Configuration

LNM is supported only in the Nways MRS code with the additional protocol option. The basic IP/DLSw code does not support it.

6.1 LNM Implementation in IBM 2210

The IBM 2210/MRS LNM support is a source routing (SR) bridging option that enables LAN Network Manager agents on the IBM 2210 bridge. The LNM function supports the following LNM agents:

- Configuration Report Server (CRS)

The CRS agent collects and reports MAC ring topology changes to the IBM LNM application. It will send out CRS MAC requests to query the status of other ring stations when requested by the LAN Network Manager.

- Ring Error Monitor (REM)

The REM agent collects MAC error reports from ring stations. When thresholds are exceeded, REM forwards error information to the LAN Network Manager.

- Ring Parameter Server (RPS)

The RPS agent services MAC requests from ring stations for ring parameter information and informs the LAN Network Manager of ring insertions.

- LAN Bridge Server (LBS)

Limited LBS support is provided. Bridge statistics, in the form of number of outgoing packets, may be displayed via the LAN Network Manager. However, the configuration of the IBM 2210 may not be changed by the LAN Network Manager.

The LAN Network Manager establishes an LLC-2 connection to the IBM 2210/MRS LNM agent. Then they communicate using the prescribed LNM management requests and responses per the standards listed below.

The MAC frames used in the LNM support conform to the ANSI/IEEE 802.5-1989 standard. The LLC frames conform to the ANSI/IEEE 802.2-1989 standard for Class I and Class II LLC frames. The LNM frames conform to the *IBM Token-Ring Network Architecture Reference*, SC30-3374-02.

6.2 LNM Configurations Commands

All the LNM commands can be found under protocol ASRT.

Table 54. Process Description

Command	Function
?(Help)	Lists all the LNM commands or actions associated with the specific command
Enable	Enables functions in configuration mode only, LNM, CRS, RPS, REM
List	Displays LNM agents and password configured for the bridge
SET	Sets the password in configuration mode only
EXIT	Returns to previous prompt

6.2.1 LNM Scenarios and Configuration

LNM must have a link between every bridge in the network that should report to LNM. The link is set up from the LNM with the two MAC addresses that each bridge or bridge pair must have. At the LNM you give a link command with the two MAC addresses and, when the bridge answers the link command, the link will be established and the bridge is linked to the LNM. In this simple scenario three bridges will be linked to LNM 2210A, 2210B and 2210C.

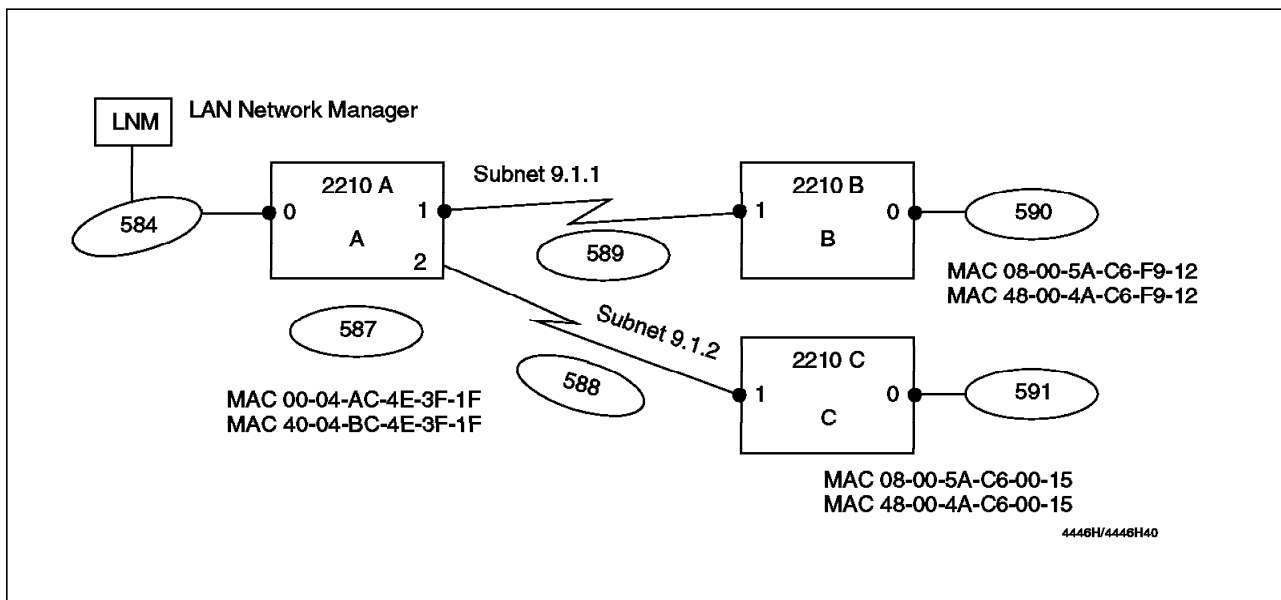


Figure 84. LNM Scenario

The following LNM configuration output is for 2210A.


```

*t 6

Config>proto asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>lnm
LNM configuration
LNM config>enable lnm
*restart 1
Are you sure you want to restart the gateway? (Yes or No): y

Copyright Notices:
Copyright 1985-1995 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*t 5
CGW Operator Console
+proto asrt
ASRT>list lnm ports 2
Port 1
LNM Agents Enabled: RPS CRS REM
Reporting Link      State      LNM Station Address
0                   ACTIVE    40-00-52-00-52-50 3
1                   AVAILABLE
2                   AVAILABLE
3                   AVAILABLE
MAC Addresses to use when configuring LNM Manager:
00-04-AC-4E-3F-1F 4
40-04-BC-4E-3F-1F 5
LNM not enabled on port 3
ASRT>

```

Figure 85. LNM Configuration Output from 2210A

1 2210A needs to be restarted to get the LNM configuration to become active.

2 This command must be processed to obtain the two MAC addresses needed to link the bridge to LNM.

3 At this point an LNM was linked to this 2210. (This display was done after the configuration and the LNM had been linked to the 2210A.) An LNM at the first position 0 is always a controlling LNM and the three others could be *observing*.

4 This is the first MAC address you should use when linking the bridge LNM.

5 This is the second MAC address you should use when linking the bridge to LNM.

The same criteria is applied to 2210B and 2210C.

```

Config>
Config>proto asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>lnm
LNM configuration
LNM config>
LNM config>ena lnm
Port Number 1? 1
LNM config>list ?
PASSWORD
PORT(S)
LNM config>list port
LNM Agents Enabled on port 1: RPS CRS REM
LNM config>
*t 5

+proto asrt
ASRT>list lnm ports
Port 1
LNM Agents Enabled: RPS CRS REM
Reporting Link      State      LNM Station Address
    0              AVAILABLE
    1              AVAILABLE
    2              AVAILABLE
    3              AVAILABLE
MAC Addresses to use when configuring LNM Manager:
    08-00-5A-C6-F9-12
    48-00-4A-C6-F9-12
LNM not enabled on port 2
ASRT>

```

Figure 86. LNM Configuration Output from 2210B

```

config>proto asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>lnm
LNM configuration
LNM config>enable lnm
Port Number 1? 1
LNM config>

*restart
Are you sure you want to restart the gateway? (Yes or No): y

Copyright Notices:
Copyright 1985-1995 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*t 5

CGW Operator Console

+proto asrt

ASRT>list lnm ports
Port 1
LNM Agents Enabled: RPS CRS REM
Reporting Link      State      LNM Station Address
      0             AVAILABLE
      1             AVAILABLE
      2             AVAILABLE
      3             AVAILABLE
MAC Addresses to use when configuring LNM Manager:
      08-00-5A-C6-00-15
      48-00-4A-C6-00-15
LNM not enabled on port 2
ASRT>

```

Figure 87. LNM Configuration Output from 2210C

6.2.2 LNM Considerations

When the three link commands have been sent to the bridges and the three bridges are linked, the following segment will be shown at LNM 584, 587, 588, 589, and 591.

In the LNM graphic screen the bridges 2210B and 2210C will show up as isolated bridges with no connections to the rest of the network. LNM assumes that bridge 2210A is a local bridge sitting at ring 584 and connecting the ring 587 at the other side. LNM also assumes that bridge 2210B is a bridge between the two rings (589 and 590) and 2210C is a bridge between 588 and 591.

In this case, LNM does not have references on how the network is tied together, so you must do it at the LNM graphics screen.

LNМ is not designed for multiport bridges and always assumes that the MAC addresses are in a real token-ring not in a virtual ring, as it is with rings 587, 588 and 589.

Chapter 7. IP Routing Protocols

This chapter describes the following routing protocols which are all supported by the IBM 2210:

- RIP
- OSPF
- BGP-4

Additionally, it covers an introduction to IP multicasting and two IP Multicast routing protocols, Multicast OSPF (MOSPF) and Distance Vector Multicast Routing Protocol (DVMRP), as well as a brief description of static routing and ARP Subnet routing which are also supported by the IBM 2210.

The dynamic routing protocols can be divided into two groups:

- Interior Gateway Protocols (IGPs)

Examples of these protocols are Open Short Path First (OSPF) and Routing Information Protocol (RIP).

- Exterior Gateway Protocols (EGPs):

An example of these routing protocols is Border Gateway Protocol Version 4 (BGP-4).

In this book, the term gateway is used to imply an IP router.

7.1 Interior and Exterior Gateway Protocols

Gateway protocols are referred to as interior or exterior depending on whether they are used within or between autonomous systems (ASs).

Interior gateway protocols allow routers to exchange routing information within an AS. Exterior gateway protocols allow the exchange of summary reachability information between separately administered ASs.

An autonomous system is defined as a logical portion of larger IP networks that are administered by a single authority. The autonomous system would normally comprise the internetwork within an organization, and would be designated as such to allow communication over public IP networks with autonomous systems belonging to other organizations. It is mandatory to register an organization's internetwork as an AS in order to use these public IP services.

Figure 88 on page 296 illustrates two interconnected autonomous systems. It shows that IGPs are used within each autonomous system, and an EGP is used between the two autonomous systems.

Autonomous systems must be registered publicly. If you require an autonomous system number, or an IP network address, to allow your network to connect to public IP services you should contact:

Network Information Center
GSI
14200 Park Meadow Drive, Suite 200
Chantilly, VA 22021

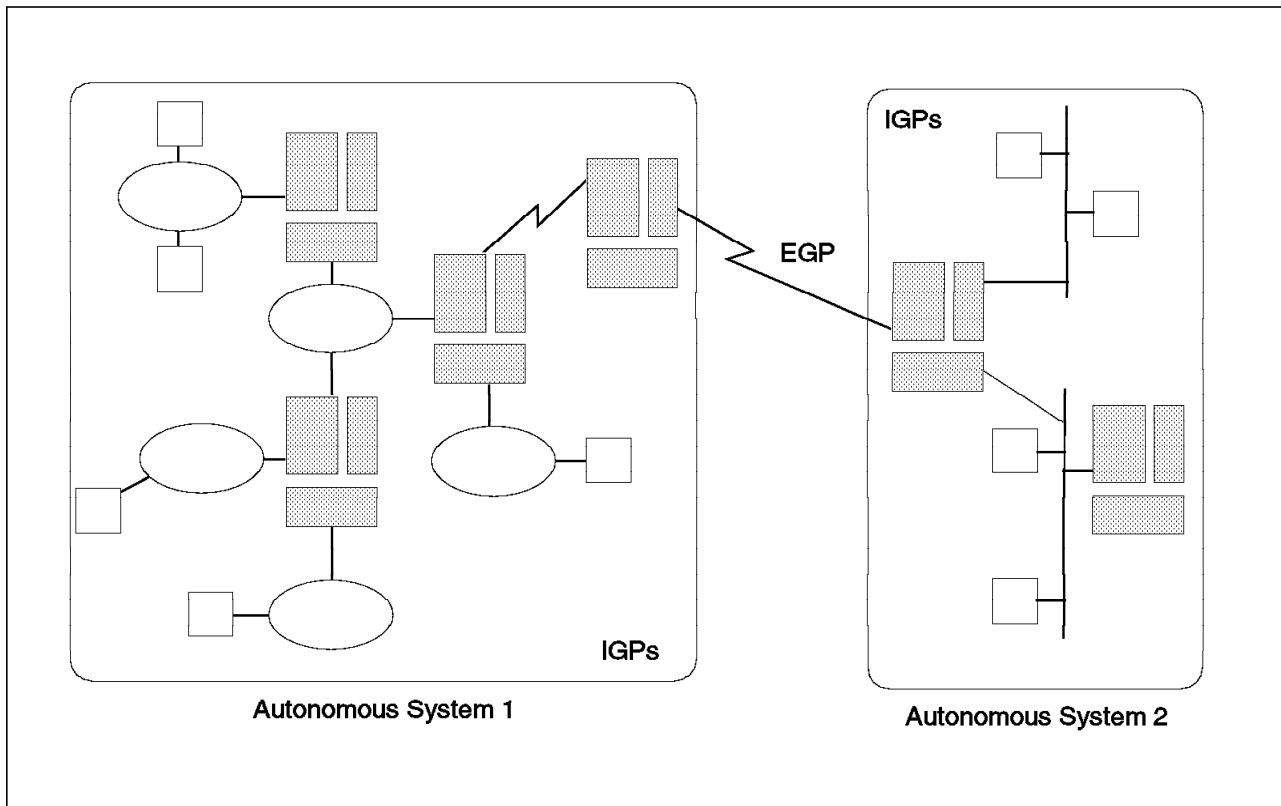


Figure 88. Autonomous Systems

7.2 Routing Algorithms

Interior and exterior gateway protocols currently implemented in the IBM 2210 use one of two generic classes of dynamic routing algorithm. These are known as *distance vector* and *link state* routing algorithms.

Dynamic routing algorithms allow routers to exchange route or link information, from which the best paths to reach destinations in an internetwork are calculated.

Static routing may also be used to supplement dynamic routing.

7.2.1 Static Routing

Static routing requires that routes be configured manually for each router.

To simplify the task of network administrators, normally the manual configuration of routes is avoided. However, there are circumstances when static routing can be attractive. For example, static routes can be used:

- To define a default route, or a route that is not being advertised within a network
- To supplement or replace exterior gateway protocols when:

- Line tariffs between autonomous systems make it desirable to avoid the cost of routing protocol traffic
- Complex routing policies are to be implemented
- It is desirable to avoid disruption caused by faulty exterior gateways in other autonomous systems

7.2.2 Distance Vector Routing

The principle behind *distance vector* routing is very simple. Each router in an internetwork maintains the distance from itself to every known destination in a *distance vector table*. Distance vector tables consist of a series of destinations (vectors) and costs (distances) to reach them and define the least costs to destinations at the time of transmission.

The distances in the tables are computed from information provided by neighbor routers. Each router transmits its own distance vector table across the shared network. The sequence of operations for doing this is as follows:

- Each router is configured with an identifier and a cost for each of its network links. The cost is normally fixed at 1, reflecting a single hop, but can reflect some other measurement taken for the link such as the traffic, speed, etc.
- Each router initializes with a distance vector table containing zero for itself, one for directly attached networks, and infinity for every other destination.
- Each router periodically (typically every 30 seconds) transmits its distance vector table to each of its neighbors. It may also transmit the table when a link first comes up or when the table changes.
- Each router saves the most recent table it receives from each neighbor and uses the information to calculate its own distance vector table.
- The total cost to each destination is calculated by adding the cost reported to it in a neighbor's distance vector table to the cost of the link to that neighbor.
- The distance vector table (the routing table) for the router is then created by taking the lowest cost calculated for each destination.

Figure 89 on page 298 shows the distance vector tables for three routers within a simple internetwork.

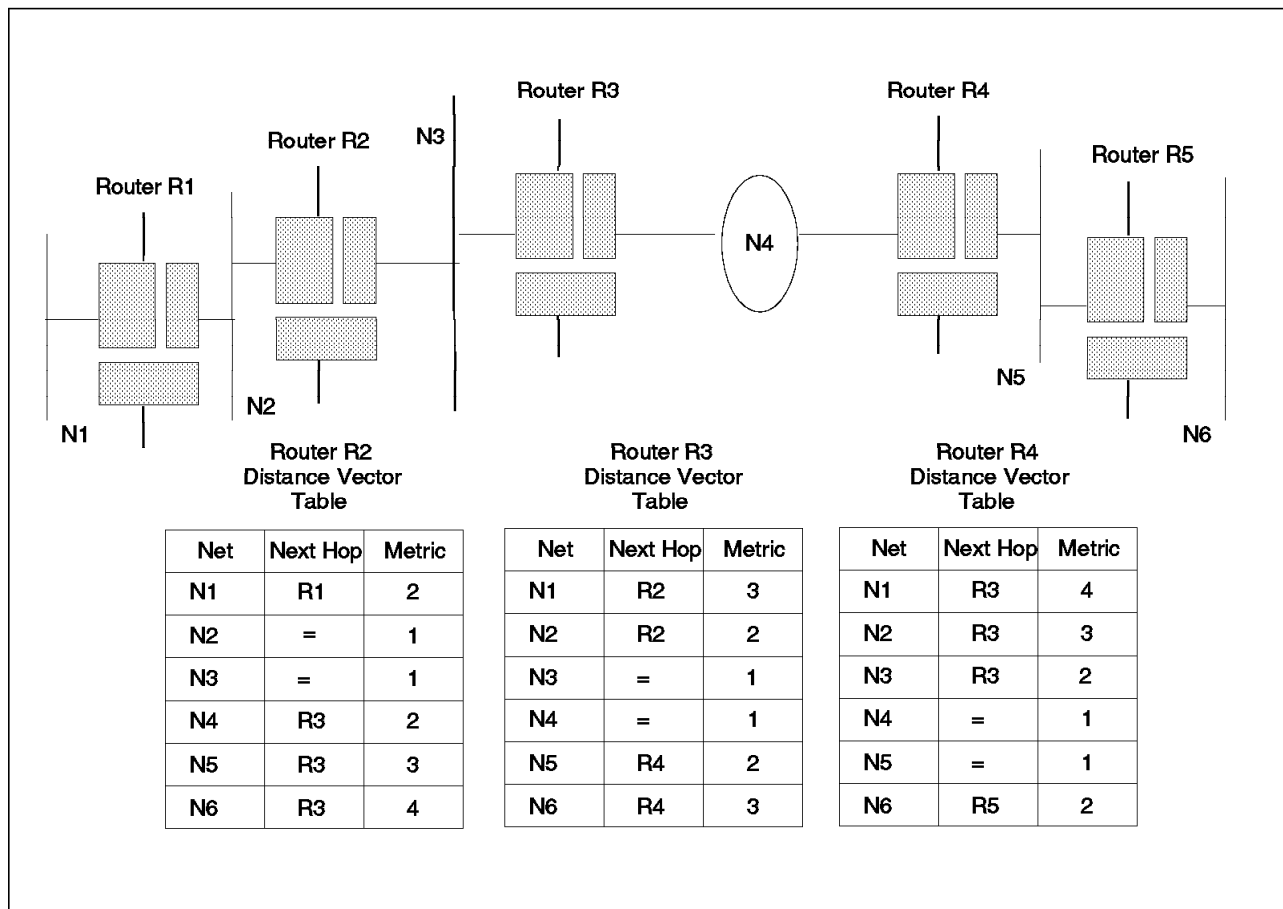


Figure 89. Distance Vector - Routing Table Calculation

The distance vector algorithm produces a stable routing table after a period directly related to the number of routers across the network. This period is referred to as the *convergence time* and represents the time it takes for distance vector information to traverse the network. In a large internetwork, this time may become too long to be useful.

Routing tables are recalculated if a changed distance vector table is received from a neighbor, or if the state of a link to a neighbor changes. If a network link goes down, the distance vector tables that have been received over it are discarded and the routing table is recalculated.

The chief advantage of distance vector is that it is very easy to implement. There are also the following significant disadvantages:

- The instability caused by old routes persisting in an internetwork
- The long convergence time on a large internetworks
- The limit to the size of an internetwork imposed by maximum hop counts
- The fact that distance vector tables are always transmitted even if their contents have not changed

Enhancements to the basic algorithm have evolved to overcome the first two of these problems. They are described in the following subsections.

7.2.2.1 Split Horizon

The basic distance vector algorithm will always allow a router to correctly calculate its distance vector table.

Using the example shown in Figure 90 you can see one of the problems of distance vector protocols known as *counting to infinity*.

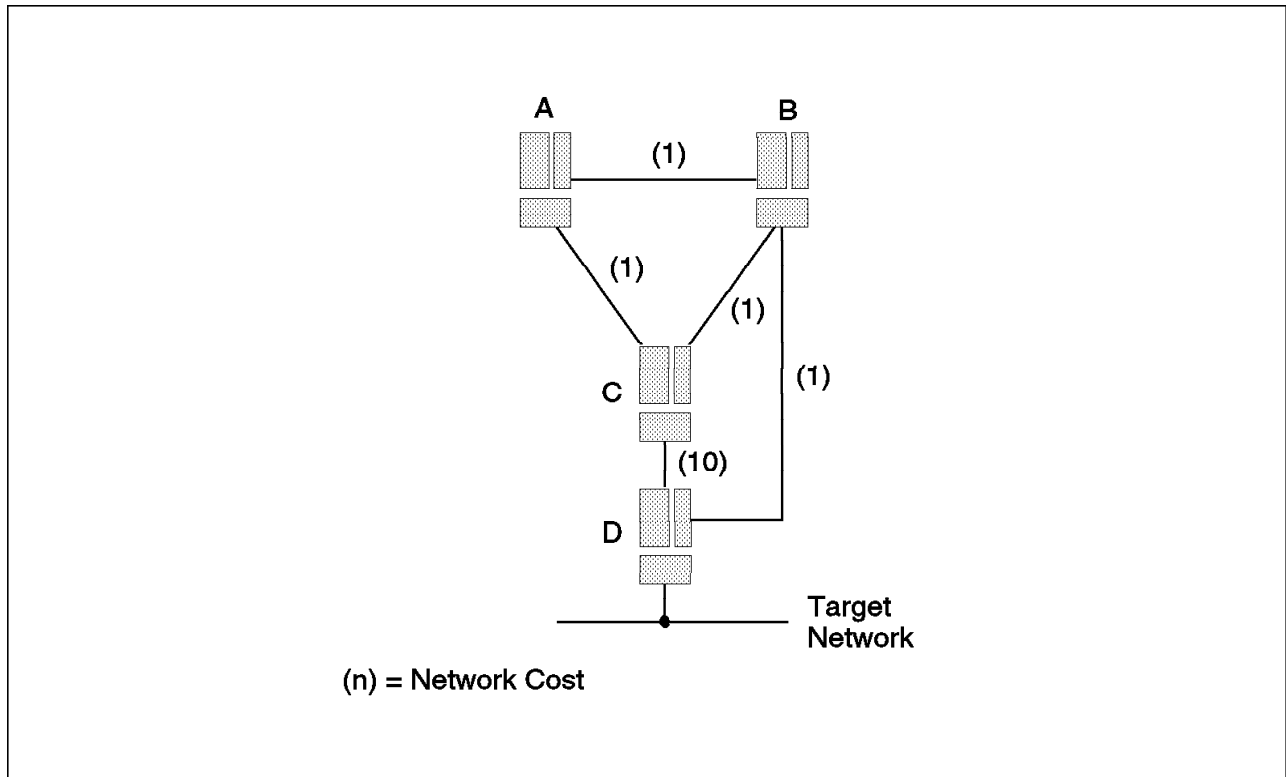


Figure 90. Counting to Infinity - Example Network

Counting to infinity occurs when a network becomes unreachable, but erroneous routes to that network persist because of the time for the distance vector tables to converge.

The example network shows four routers interconnected by five network links. The networks all have a cost of 1 except for that from C to D which has a cost of 10.

Each of the routers A, B, C and D has routes to all networks. If we show only the routes to the target network, we will see they are as follows:

For D : Directly connected network. Metric 1



For B : Route via D. Metric 2

For C : Route via B. Metric 3

For A : Route via B. Metric 3

If the link from B to D fails, then all routes will adjust in time to use the link from C to D. The convergence time for this, however, may be considerable.

Distance vector tables begin to change when B notices that the route to D has become unavailable. Figure 91 on page 300 shows how the routes to the target

Time								
D:	Direct	1	Direct	1	Direct	1	Direct	1
B:	Unreachable		Unreachable		Unreachable		C	12
C:	B	3	A	4	D	11	D	11
A:	B	3	C	4	Unreachable		C	12

Note: Faster routing table convergence

Figure 92. Split Horizon

7.2.2.2 Split Horizon with Poison Reverse

Poison reverse is an enhancement to split horizon whereby routes learned from a neighbor router are reported back to it but with a metric of infinity (that is, network unreachable).

The use of poison reverse is safer than split horizon alone because it breaks erroneous looping routes immediately.

If two routers receive routes pointing at each other, and they are advertised with a metric of infinity, the routes will be eliminated immediately as unreachable. If the routes are not advertised in this way, they must be eliminated by the timeout that results from a route not being reported by a neighbor router for several periods (for example, six periods for RIP).

Poison reverse does have one disadvantage. It significantly increases the size of distance vector tables that must be exchanged between neighbor routers because all routes are included in the distance vector tables. While this is generally not a problem on LANs, it can cause real problems on point-to-point connections in large internetworks.

7.2.2.3 Triggered Updates

Split horizon with poison reverse will break routing loops involving two routers. It is still possible, however, for there to be routing loops involving three or more routers. For example, A may believe it has a route through B, B through C, and C through A. This loop can only be eliminated by the timeout that results from counting to infinity.

Triggered updates are designed to reduce the convergence time for routing tables, and hence reduce the period during which such erroneous loops are present in an internetwork.

When a router changes the cost for a route in its distance vector table, it must send the modified table immediately to neighbor routers. This simple mechanism ensures that topology changes in a network are propagated quickly, rather than at a rate dependent on normal periodic updates.

7.2.3 Link State Routing

The growth in the size of internetworks in recent years has necessitated the replacement of distance vector routing algorithms with alternatives that address the shortcomings identified in 7.2.2, “Distance Vector Routing” on page 297.

These new protocols have been based on *link state* or shortest path first algorithms. The best example is the OSPF Interior Gateway Protocol.

The principle behind link state routing is straightforward, although its implementation can be complex:

- Routers are responsible for contacting neighbors and learning their identities.
- Routers construct link state packets which contain lists of network links and their associated costs.
- Link state packets are transmitted to all routers in a network.
- All routers therefore have an identical list of links in a network, and can construct identical topology maps.
- The maps are used to compute the best routes to all destinations.

Routers contact neighbors by sending *hello* packets on their network interfaces. Hello packets are sent directly to neighbors on point-to-point links and non-broadcast networks. On LAN networks, hello packets are sent to a predefined group or multicast IP address that can be received by all routers. Neighbors who receive hellos from a router should reply with hello packets that include the identity of that originating router.

Once neighbors have been contacted in this way, link state information can be exchanged.

Link state information is sent in the form of *link state packets* (LSPs), also known as link state advertisements. LSPs provide the database from which network topology maps can be calculated at each router. LSPs are normally sent only under the following specific circumstances:

- When a router discovers a new neighbor
- When a link to a neighbor goes down
- When the cost of a link changes

Once a router has generated an LSP it is critical that it is received successfully by all other routers in a network. If this does not happen, routers on the network will calculate network topology based on incorrect link state information.

Distribution of LSPs would normally be on the basis of each router’s routing tables. However, this leads to a *chicken and egg* situation. Routing tables would rely on LSPs for their creation and LSPs would rely on routing tables for their distribution. A simple scheme called *flooding* overcomes this, and ensures that LSPs are successfully distributed to all routers in a network.

Flooding requires that a router that receives an LSP transmits it to all neighbors except the one from which it was received. All LSPs must be explicitly acknowledged to ensure successful delivery, and they are sequenced and timestamped to ensure duplicates are not received and retransmitted.

When a router receives an LSP it looks in its database to see the sequence number of the last LSP from the originator. If the sequence number is the same as, or earlier than, the sequence number of the LSP in its database then the LSP is discarded. Otherwise the LSP is added to the database.

The flooding process ensures that all routers in a network have the same link state information. All routers are then able to compute the same shortest path tree topology map for the network, and hence select best routes to all destinations.

7.3 Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is an interior gateway protocol defined in RFC 1058.

It is an IAB standard protocol; its status is elective. This means that it is one of several interior gateway protocols available, and it may or may not be implemented on a system. If a system does implement it, however, the implementation should be in line with the RFC.

RIP is based on the Xerox PUP and XNS routing protocols. The RFC was issued after many RIP implementations had been completed. For this reason some do not include all the enhancements to the basic distance vector routing protocol (such as poison reverse and triggered updates).

RIP is very widely used because the code (known as *ROUTED*) was incorporated on the Berkeley Software Distribution (BSD) UNIX operating system, and in other UNIX systems based on it.

7.3.1 Protocol Description

RIP is a standard distance vector routing protocol, as described in 7.2.2, “Distance Vector Routing” on page 297.

RIP packets are transmitted onto a network in *User Datagram Protocol* (UDP) datagrams, which in turn are carried in IP datagrams. RIP sends and receives datagrams using UDP port 520. RIP datagrams have a maximum size of 512 octets and tables larger than this must be sent in multiple UDP datagrams.

RIP datagrams are normally broadcast onto LANs using the LAN MAC all-stations broadcast address and the IP network or subnetwork broadcast address. They are specifically addressed on point-to-point and multi-access non-broadcast networks, using the destination router IP address.

Routers normally run RIP in *active mode*; that is, advertising their own distance vector tables and updating them based on advertisements from neighbors. End nodes, if they run RIP, normally operate in *passive (or silent) mode*; that is, updating their distance vector tables on the basis of advertisements from neighbors, but not in turn advertising them.

RIP specifies two packet types; *request* and *response*.

A request packet is sent by routers to ask neighbors to send part of their distance vector table (if the packet contains destinations), or all their table (if no destinations have been specified).

A response packet is sent by routers to advertise their distance vector table in the following circumstances:

- Every 30 seconds
- In response to a request packet
- When distance vector tables change (if triggered updates are supported)

Active and passive systems listen for all response packets and update their distance vector tables accordingly. A route to a destination, computed from a neighbor's distance vector table, is kept until an alternate is found with lower cost, or it is not re-advertised in six consecutive RIP responses. In this case the route is timed out and deleted.

When RIP is used with IP, the address family identifier is 2 and the address fields are 4 octets. To reduce problems of counting to infinity the maximum metric is 16 (unreachable) and directly connected networks are defined as having a metric of one.

The RIP packet format for IP is shown in Figure 93.

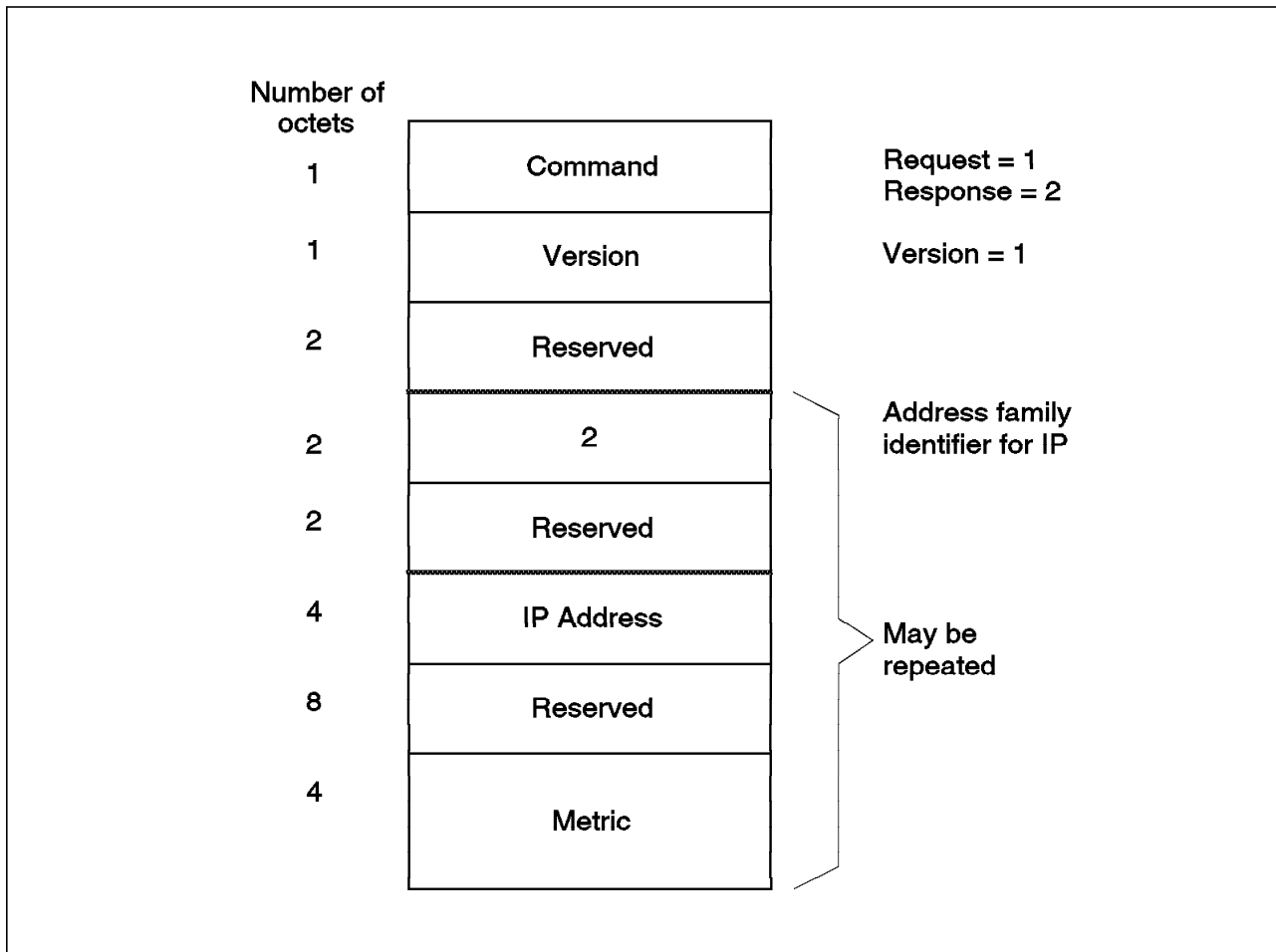


Figure 93. IP Specific RIP Packet Format

RIP makes no provision for passing subnet masks with its distance vector tables. A router receiving a RIP response must already have subnet mask information to allow it to interpret the network identifier and host identifier portions of the IP address correctly.

In the absence of subnet mask information a router will interpret routes as best as it can. If it knows an IP network has a specific subnet mask, it will interpret all other route information for that network on the basis of that single mask. If it receives a packet with bits set in the field that it regards as the host field, it will interpret it as a route to a host with a mask of 255.255.255.255.

The above makes it impossible for RIP to be used in an internetwork with variable length subnet masks.

Note

RIP Version 2 provides support for variable subnet mask. However, since RIP Version 2 is not supported by IBM 2210, it will not be discussed in this book.

7.4 Open Shortest Path First (OSPF)

The *Open Shortest Path First* (OSPF) V2 Protocol is an interior gateway protocol defined in RFC 1247. A report on the use of OSPF V2 is contained in RFC 1246 *Experience with the OSPF Protocol*.

It is an IAB standard protocol; its status is elective.

OSPF is important because it has a number of features not found in other interior gateway protocols. Support for these additional features makes OSPF the preferred choice for new IP internetwork implementations. The following features are covered within OSPF:

- Support for *type of service (TOS)* routing
- Provides *load balancing*
- Allows site partitioning into subsets by using *areas*
- Information exchange between routers requires *authentication*
- Support for *host-specific routes* as well as network-specific routes
- Reduces table maintenance overhead to a minimum by implementing a *designated router*
- Allows definition of *virtual links* to provide support to a non-contiguous area
- Allows the usage of *variable length subnet masks*
- Will *import* RIP and EGP routes into its database

7.4.1 OSPF Terminology

OSPF uses specific terminology which must be understood before the protocol can be described.

7.4.1.1 Areas

OSPF internetworks are organized into *areas*.

An OSPF area consists of a number of networks and routers that are logically grouped together. Areas may be defined on a per location or a per region basis, or they may be based on administrative boundaries.

All OSPF networks consist of at least one area, the backbone, plus as many additional areas as are demanded by network topology and other design criteria.

Within an OSPF area all routers maintain the same topology database, exchanging link state information to maintain their synchronization. This ensures that all routers calculate the same network map for the area.

Information about networks outside an area is summarized by *area border* or *AS boundary routers* (see 7.4.1.3, “Intra-Area, Area Border and AS Boundary Routers”) and flooded into the area. Routers within an area have no knowledge of the topology of networks outside the area, only of routes to destinations provided by area border and AS boundary routers.

The importance of the area concept is that it limits the size of the topology database that must be held by routers. This has direct impact on the processing to be carried out by each router, and on the amount of link state information that must be flooded into individual networks.

7.4.1.2 The OSPF Backbone

All OSPF networks must contain at least one area, the *backbone*, which is assigned an area identifier of *0.0.0.0*.

The backbone has all the properties of an area, but has the additional responsibility of distributing routing information between areas attached to it.

Normally an OSPF backbone should be contiguous, that is with all backbone routers attached one to another. This may not be possible because of network topology, in which case backbone continuity must be maintained by the use of *virtual links*.

Virtual links are backbone router-to-backbone router connections that traverse a non-backbone area.

Routers within the backbone operate identically to other intra-area routers and maintain full topology databases for the backbone area.

7.4.1.3 Intra-Area, Area Border and AS Boundary Routers

There are three possible types of routers in an OSPF network.

Routers that are situated entirely within an OSPF area are called *intra-area routers*. All intra-area routers flood router links advertisements into the area to define the links they are attached to. If elected designated or backup-designated router (see 7.4.1.6, “Designated and Backup Designated Router” on page 308) they also flood network links advertisements to define the identity of all routers attached to the network. Intra-area routers maintain a topology database for the area in which they are situated.

Routers that connect two or more areas are referred to as *area border routers*. Area border routers maintain topology databases for each area to which they are attached, and exchange link state information with other routers in those areas. Area border routers also flood summary link state advertisements into each area to inform them of inter-area routes.

Routers that are situated at the periphery of an OSPF internetwork and exchange reachability information with routers in other ASs using exterior gateway protocols are called *AS boundary routers*. Routers that import static routes or

routes from other IGPs, such as RIP or HELLO, into an OSPF network are also AS boundary routers. AS boundary routers are responsible for flooding AS external link state advertisements into all areas within the AS to inform them of external routes.

Figure 94 shows the location of intra-area, area border and AS boundary routers within an OSPF internetwork.

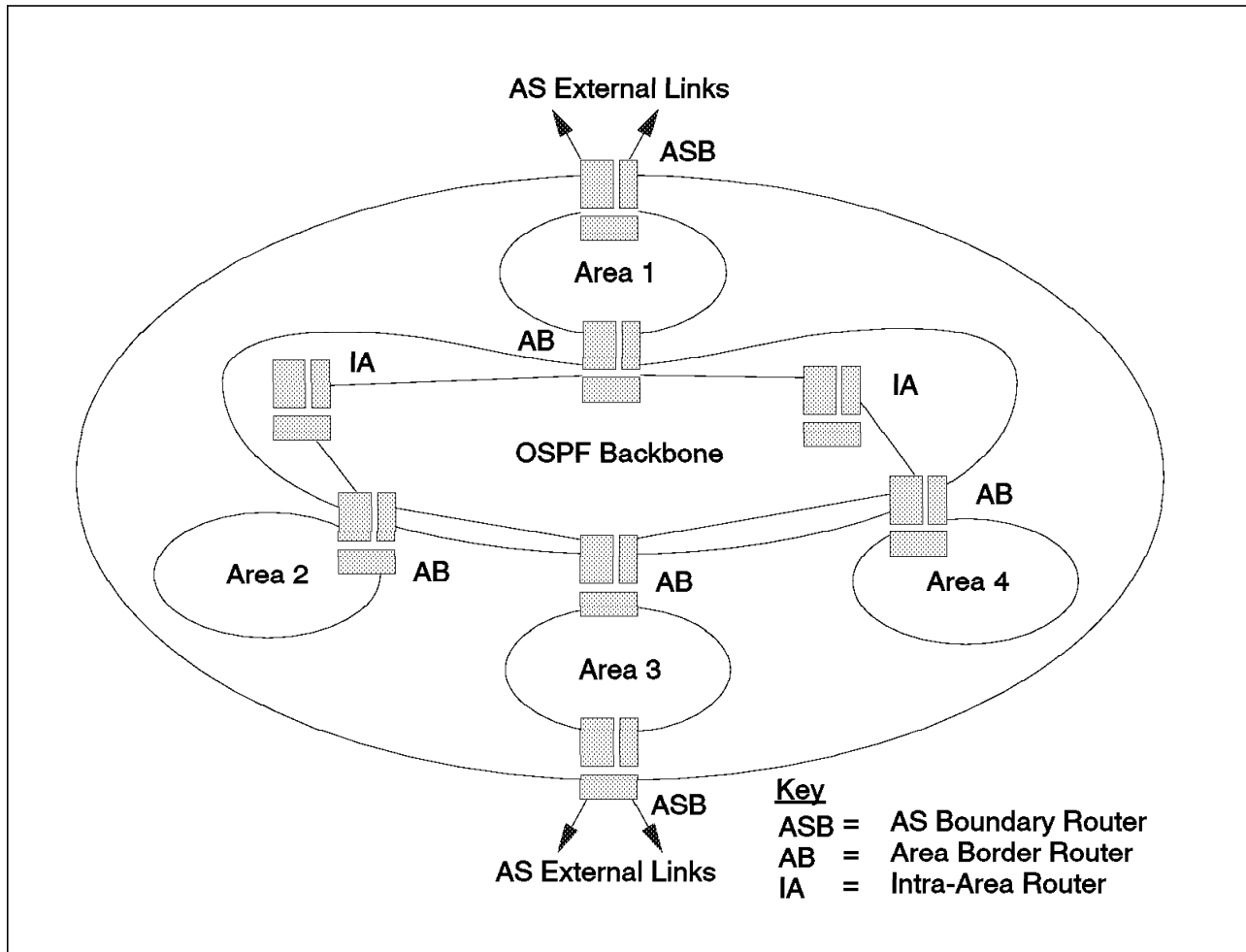


Figure 94. OSPF Network

7.4.1.4 Neighbor Router

Two routers that have interfaces to a common network are said to be *neighbors*.

Neighbor routers are discovered by the OSPF Hello protocol which is described in 7.4.2.1, "Discovering Neighbors - The OSPF Hello Protocol" on page 311.

7.4.1.5 Adjacent Router

Neighbor routers may become *adjacent*. They are said to be adjacent when they have synchronized their topology databases through the exchange of link state information.

Link state information is exchanged only between adjacent routers, not between neighbor routers.

Not all neighbor routers become adjacent. Neighbors on point-to-point links do so, but on multi-access networks adjacencies are only formed between individual routers and the designated and backup designated routers.

The exchange of link state information between neighbors can create significant amounts of network traffic. Limiting the number of adjacencies on multi-access networks in this way achieves considerable reductions in network traffic.

7.4.1.6 Designated and Backup Designated Router

All multi-access networks have a *designated* and a *backup designated* router.

These routers are elected automatically for each network once neighbor routers have been discovered by the Hello protocol.

The designated router performs two key roles for a network:

- It generates network links advertisements that list the routers attached to a multi-access network.
- It forms adjacencies with all routers on a multi-access network and therefore becomes the focal point for forwarding of all link state advertisements.

The backup designated router forms the same adjacencies as the designated router. It therefore has the same topology database and is able to assume designated router functions should it detect that the designated router has failed.

7.4.1.7 Point-to-Point and Multi-Access Networks

All OSPF areas consist of aggregates of networks linked by routers. OSPF categorizes networks into two different types.

Point-to-point networks directly link two routers. OSPF packets on a point-to-point network are multicast to the neighbor router. *Multicasting* is the term used for transmitting IP datagrams to a functional rather than a specific IP address. A functional address will typically be recognized by a number of systems and can be considered a form of limited broadcast. The OSPF RFC defines the use of two multicast addresses for OSPF router interactions.

Multi-access networks are those which support the attachment of more than two routers. They are further subdivided into two types:

- Broadcast
- Non-broadcast

Broadcast networks have the capability of directing OSPF packets to all attached routers, using an address that is recognized by all of them. An Ethernet LAN is an example of a broadcast multi-access network.

Non-broadcast networks do not have this capability and all packets must be specifically addressed to routers on the network. This requires that routers on a non-broadcast network be configured with the addresses of neighbors. Examples of a non-broadcast multi-access network are the X.25 public data network or a frame relay network.

7.4.1.8 Link State Advertisements

Link state information is exchanged by adjacent OSPF routers to allow area topology databases to be maintained, and inter-area and inter-AS routes to be advertised.

Link state information consists of five types of *link state advertisement*. Together these provide all the information needed to describe an OSPF network and its external environment:

1. Router Links
2. Network Links
3. Summary Links (Type 3 and 4)
4. AS External Links

Router links advertisements are generated by all OSPF routers and describe the state of the router's interfaces (links) within the area. They are flooded throughout a single area only.

Network links advertisements are generated by the designated router on a multi-access network and list the routers connected to the network. They are flooded throughout a single area only.

Summary links advertisements are generated by area border routers. There are two types; one describes routes to destinations in other areas, the other routes to AS boundary routers. They are flooded throughout a single area only.

AS external links advertisements are generated by AS boundary routers and describe routes to destinations external to the OSPF network. They are flooded throughout all areas in the OSPF network.

7.4.2 Protocol Description

The OSPF protocol is an implementation of a *link state* routing protocol, as described in 7.2.3, "Link State Routing" on page 302.

OSPF packets are transmitted directly in IP datagrams. IP datagrams containing OSPF packets can be distinguished by their use of *protocol identifier 89* in the IP header. OSPF packets are not, therefore, contained in TCP or UDP headers. OSPF packets are always sent with IP *type of service* set to 0, and the IP *precedence field* set to internetwork control. This is to aid them in getting preference over normal IP traffic.

Further details of IP protocol identifiers, type of service and precedence can be found in RFC 791 *Internet Protocol*.

OSPF packets are sent to a standard multicast IP address on point-to-point and broadcast networks. This address is 224.0.0.5, referred to as *AllSPFRouters* in the RFC. They are sent to specific IP addresses on non-broadcast networks using neighbor network address information that must be configured for each router.

All OSPF packets share a common header, which is shown in Figure 95 on page 310.

This header provides general information such as area identifier and originating router identifier, and also includes a checksum and authentication information. A type field defines each OSPF packet as one of five possible types:

1. Hello
2. Database Description
3. Link State Request
4. Link State Update
5. Link State Acknowledgement

The router identifier, area identifier, and authentication information are configurable for each OSPF router.

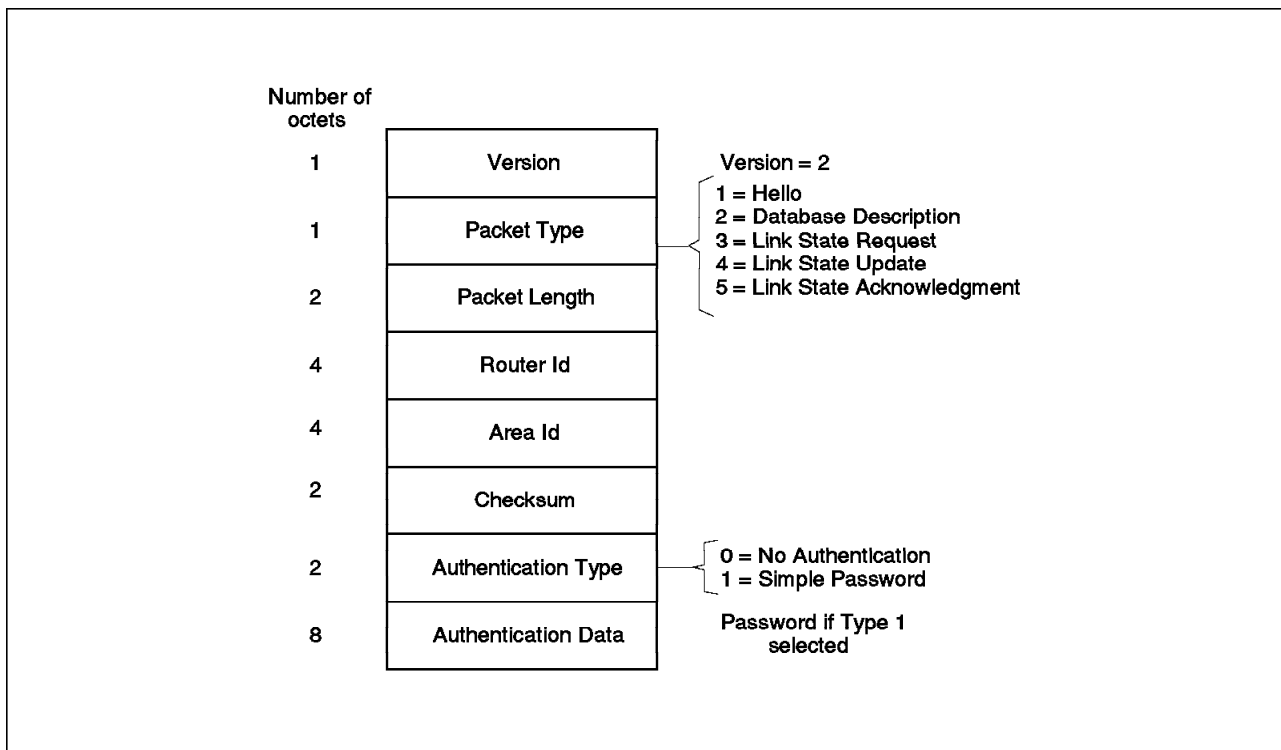


Figure 95. OSPF Common Header

The OSPF protocol defines a number of stages which must be executed by individual routers. They are as follows:

- Discovering neighbors
- Electing the designated router
- Initializing neighbors
- Propagating link state information
- Calculating routing tables

The use of the five OSPF packet types to implement stages of the OSPF protocol are described in the following subsection.

During OSPF operation a router cycles each of its interfaces through a number of *states* from *Down*, through *Waiting*, to *DR Other*, *BackupDR* or *DR* (DR stands for *designated router*) depending on the status of each attached network and the identity of the designated router elected for each of them. A detailed description

of these states is outside the scope of this document, but can be found in RFC 1247.

At the same time a router cycles each neighbor interface (interaction) through a number of states as it discovers them and then becomes adjacent. These states are; *Down*, *Attempt*, *Init*, *2-Way*, *ExStart*, *Exchange*, *Loading* and *Full*. Once again a description of these is outside the scope of this document but can be found in the RFC.

7.4.2.1 Discovering Neighbors - The OSPF Hello Protocol

The Hello protocol is responsible for discovering neighbor routers on a network, and establishing and maintaining relationships with them.

Note

The OSPF Hello Protocol is entirely separate from the HELLO Routing Protocol defined in RFC 891. They should not be confused.

Hello packets are sent out periodically on all router interfaces. The format of these is shown in Figure 96.

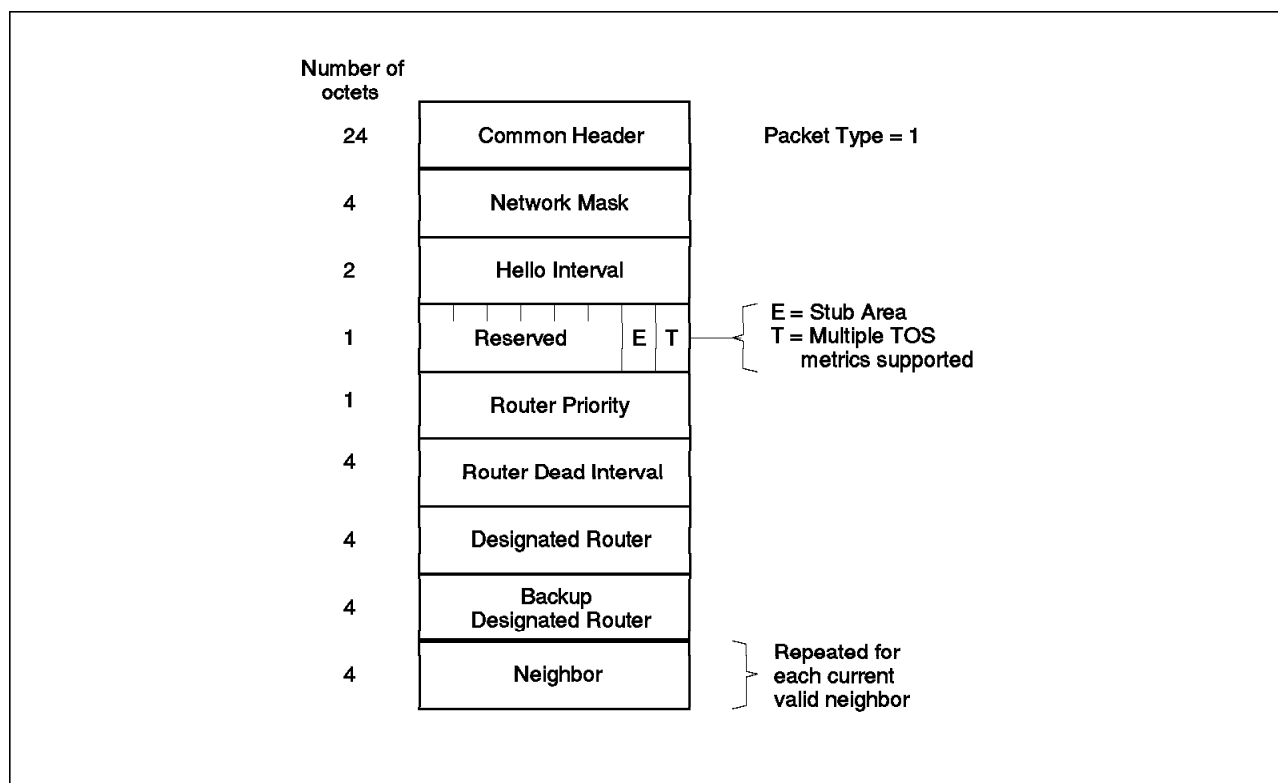


Figure 96. OSPF Hello Packet

Hello packets contain the identities of neighbor routers whose hello packets have already been received over a specific interface. They also contain the *network mask*, and *router priority*, *designated router identifier* and *backup designated router identifier*. The final three parameters are used to elect the designated router on multi-access networks.

The network mask, router priority, hello interval and router dead interval are configurable for each interface on an OSPF router.

A router interface changes state from *Down* to *Point-to-Point* (if the network is point-to-point), to *DR Other* (if the router is ineligible to become designated router), or otherwise to *Waiting* as soon as hello packets are sent over it.

A router receives hello packets from neighbor routers via its network interfaces. When this happens the neighbor interface state changes from *Down* to *Init*. Bidirectional communication is established between neighbors when a router sees itself listed in a hello packet received from another router. Only at this point are the two routers defined as true neighbors, and the neighbor interface changes state from *Init* to *2-Way*.

7.4.2.2 Electing the Designated Router

All multi-access networks have a designated router. There is also a backup designated router that takes over in the event that the designated router fails.

The use of a backup, which maintains an identical set of adjacencies and an identical topology database to the designated router, ensures there is no extended loss of routing capability if the designated router fails.

The designated router performs two major functions on a network:

- It originates network links advertisements on behalf of the network.
- It establishes adjacencies with all other routers on the network. Only routers with adjacencies exchange link state information and synchronize their databases.

The designated router and backup designated router are elected on the basis of the *router identifier*, *router priority*, *designated router* and *backup designated router* fields in hello packets. Router priority is a single octet field that defines the priority of a router on a network. The lower the value of the priority field the more likely the router is to become the designated router, hence the higher its priority. A zero value means the router is ineligible to become designated or backup designated router.

The process of designated router election is as follows:

1. The current values for designated router and backup designated router on the network are initialized to *0.0.0.0*.
2. The current values for router identifier, router priority, designated router and backup designated router in hello packets from neighbor routers are noted. Local router values are included.
3. Backup designated router election:

Routers that have been declared as designated router are ineligible to become backup designated router.

The backup designated router will be declared to be:

- The highest priority router that has been declared as backup designated router
- The highest priority router if no backup designated router has been declared

If equal priority routers are eligible, the one with the highest router identifier is chosen.

4. Designated router election:

The designated router will be declared to be:

- The highest priority router that has been declared designated router
 - The highest priority router if no designated router has been declared
5. If the router carrying out the above determination is declared the designated or backup designated router then the above steps are re-executed. This ensures that no router can declare itself both designated and backup designated router.

Once designated and backup designated routers have been elected for a network, they proceed to establish adjacencies with all routers on the network.

Completion of the election process for a network causes the router interface to change state from *Waiting* to *DR*, *BackupDR*, or *DR Other* depending on whether the router is elected the designated router, the backup designated router or neither of these.

7.4.2.3 Establishing Adjacencies - Database Exchange

A router establishes adjacencies with a subset of neighbor routers on a network.

Routers connected by point-to-point networks and virtual links always become *adjacent*. Routers on multi-access networks form adjacencies with the designated and backup designated routers only.

Link state information flows only between adjacent routers. Before this can happen it is necessary for them to have the same topological database, and to be synchronized.

This is achieved in OSPF by a process called *database exchange*.

Database exchange between two neighbor routers occurs as soon as they attempt to bring up an adjacency. It consists of the exchange of a number of database description packets that define the set of link state information present in the database of each router. The link state information in the database is defined by the list of link state headers for all link state advertisement in the database (see Figure 101 on page 317 for information on the link state header).

The format of database description packets is shown in Figure 97 on page 314.

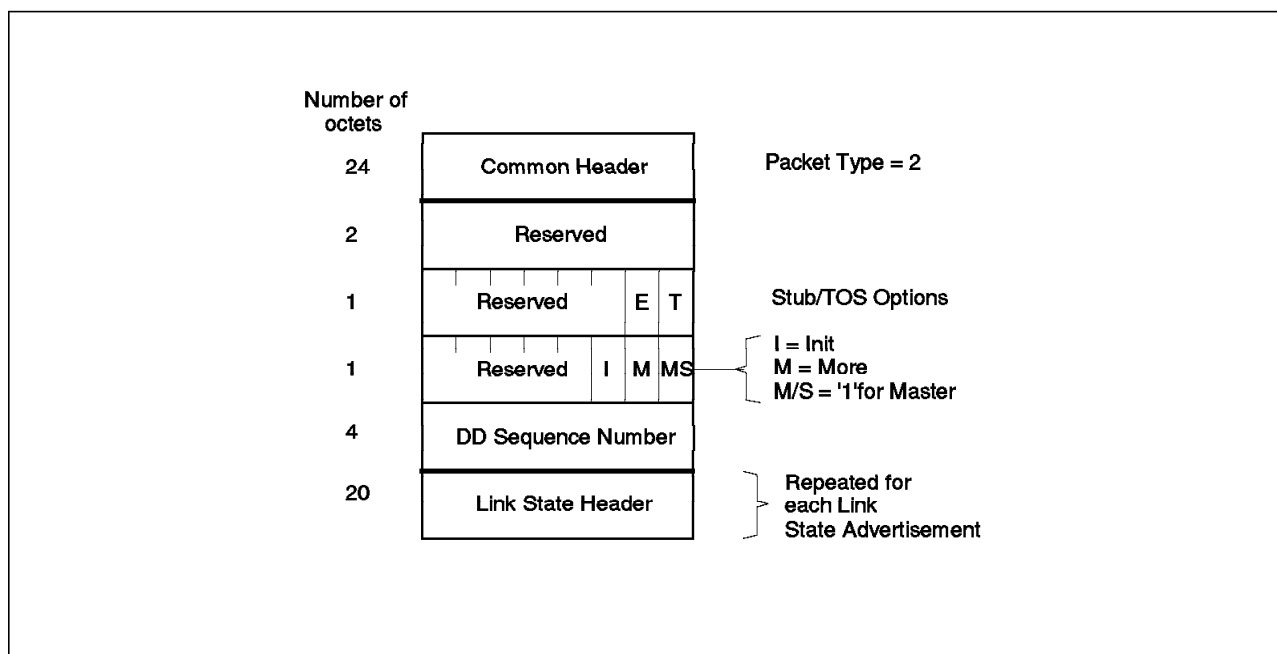


Figure 97. OSPF Database Description Packet

During the database exchange process the routers form a *master/slave* relationship, the master being the first to transmit. The master sends database description packets to the slave to describe its database of link state information. Each packet is identified by a sequence number and contains a list of the link state headers in the master's database. The slave acknowledges each packet by sequence number and includes its own database of headers in the acknowledgements.

Flags in database description packets indicate whether they are from a master or slave (the M/S bit), the first such packet (the I bit) and if there are more packets to come (the M bit). Database exchange is complete when a router receives a database description packet from its neighbor with the M bit off.

During database exchange each router makes a list of the link state advertisements for which the adjacent neighbor has a more up-to-date instance (all advertisements are sequenced and time stamped). Once the process is complete each router requests these more up-to-date instances of advertisements using link state requests.

The format of link state request packets is shown in Figure 98 on page 315.

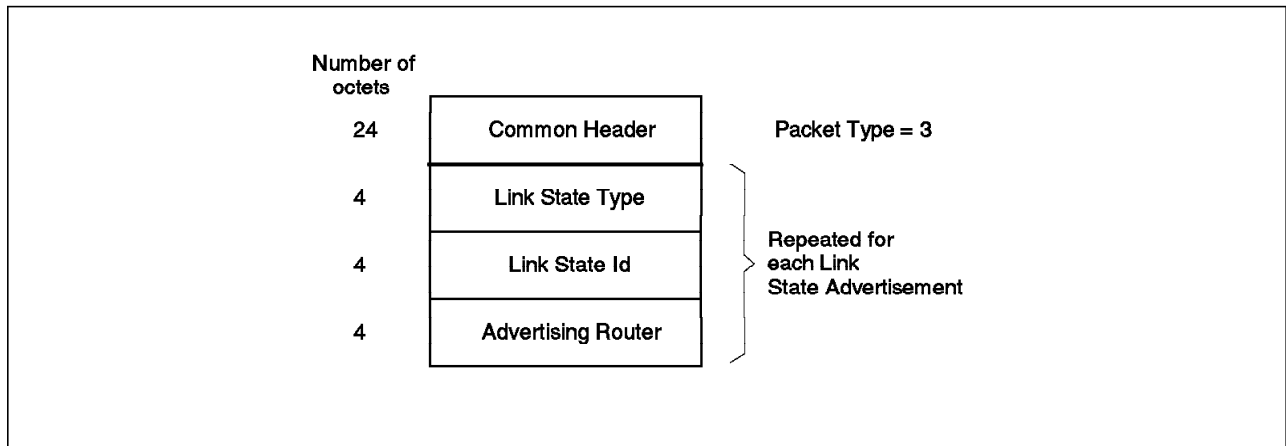


Figure 98. OSPF Link State Request Packet

The database exchange process sequences the neighbor interface state from 2-Way through:

- *ExStart* as the adjacency is created and the master agreed upon
- *Exchange* as the topology databases are being described
- *Loading* as the link state requests are being sent and responded to
- And finally to *Full* when the neighbors are fully adjacent

In this way, the two routers synchronize their topology databases and are able to calculate identical network maps for their OSPF area.

7.4.2.4 Link State Propagation

Information about the topology of an OSPF network is passed from router to router in link state advertisements.

Link state advertisements pass between adjacent routers in the form of *link state update* packets, the format of which is shown in Figure 99.

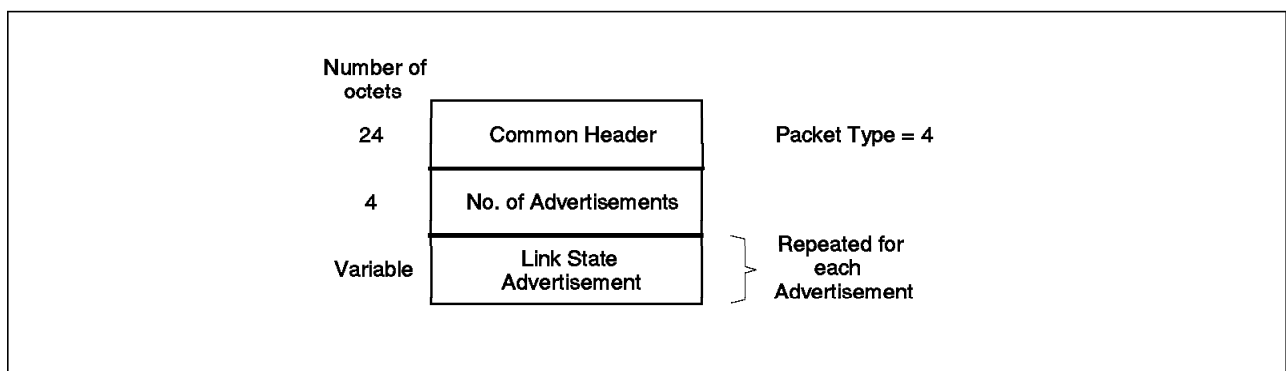


Figure 99. OSPF Link State Update Packet

Link state advertisements are of five types: router links, network links, summary links (two types) and AS external links as noted earlier in this section.

Link state updates pass as a result of link state requests during database exchange, and also in the normal course of events when routers wish to indicate a change of network topology. Individual link state update packets can contain multiple link state advertisements.

It is essential that each OSPF router in an area has the same network topology database, and hence the integrity of link state information must be maintained.

For that reason link state update packets must be passed without loss or corruption throughout an area. The process by which this is done is called *flooding*.

A link state update packet floods one or more link state advertisements one hop further away from their originator. To make the flooding procedure reliable each link state advertisement must be acknowledged separately. Multiple acknowledgements can be grouped together into a single *link state acknowledgement packet*. The format of the link state acknowledgement packet is shown in Figure 100.

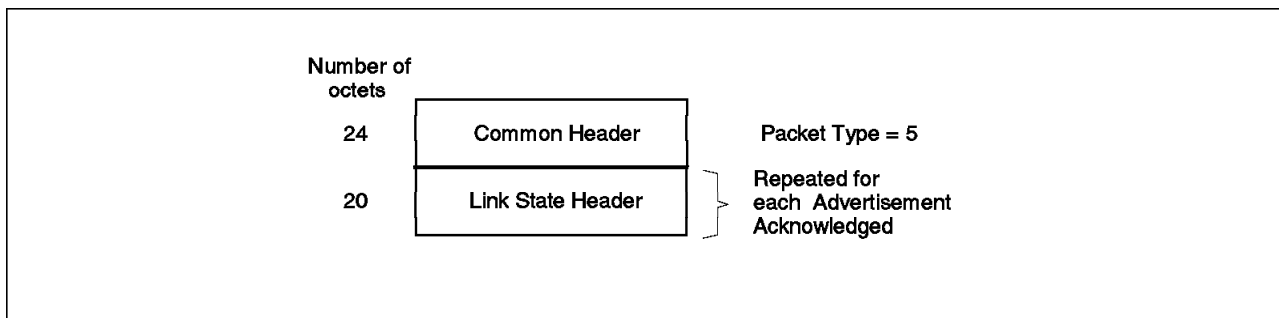


Figure 100. OSPF Link State Acknowledgement Packet

In order to maintain database integrity it is essential that all link state advertisements are rigorously checked to ensure validity.

The following checks are applied and the advertisement discarded if:

- The link state checksum is incorrect.
- The link state type is invalid.
- The advertisement's age has reached its maximum.
- The advertisement is older than or the same as one already in the database.

If an advertisement passes the above checks, then an acknowledgement is sent back to the originator. If no acknowledgement is received by the originator then the original link state update packet is retransmitted after a timer has expired.

Once accepted an advertisement is flooded onward over the router's other interfaces until it has been received by all routers within an area.

Advertisements are identified by their *link state type*, *link state ID* and the *advertising router*. They are further qualified by their *link state sequence number*, *link state age* and *link state checksum number*.

The age of a link state advertisement must be calculated to determine if it should be installed into a router's database. Only a more recent advertisement should be accepted and installed. Advertisements are only considered more recent if they have a newer sequence number, or if sequence numbers are equal if they have the larger checksum, or if checksums are equal if they have their age set to *max age*.

Valid link state advertisements are installed into the topology database of the router. This causes the topology map or graph to be recalculated and the routing table to be updated.

Link state advertisements all have a common header. This is shown in Figure 101. The five link state advertisement types are shown in Figure 102 on page 318, in Figure 103 on page 318, in Figure 104 on page 319, and in Figure 105 on page 319.

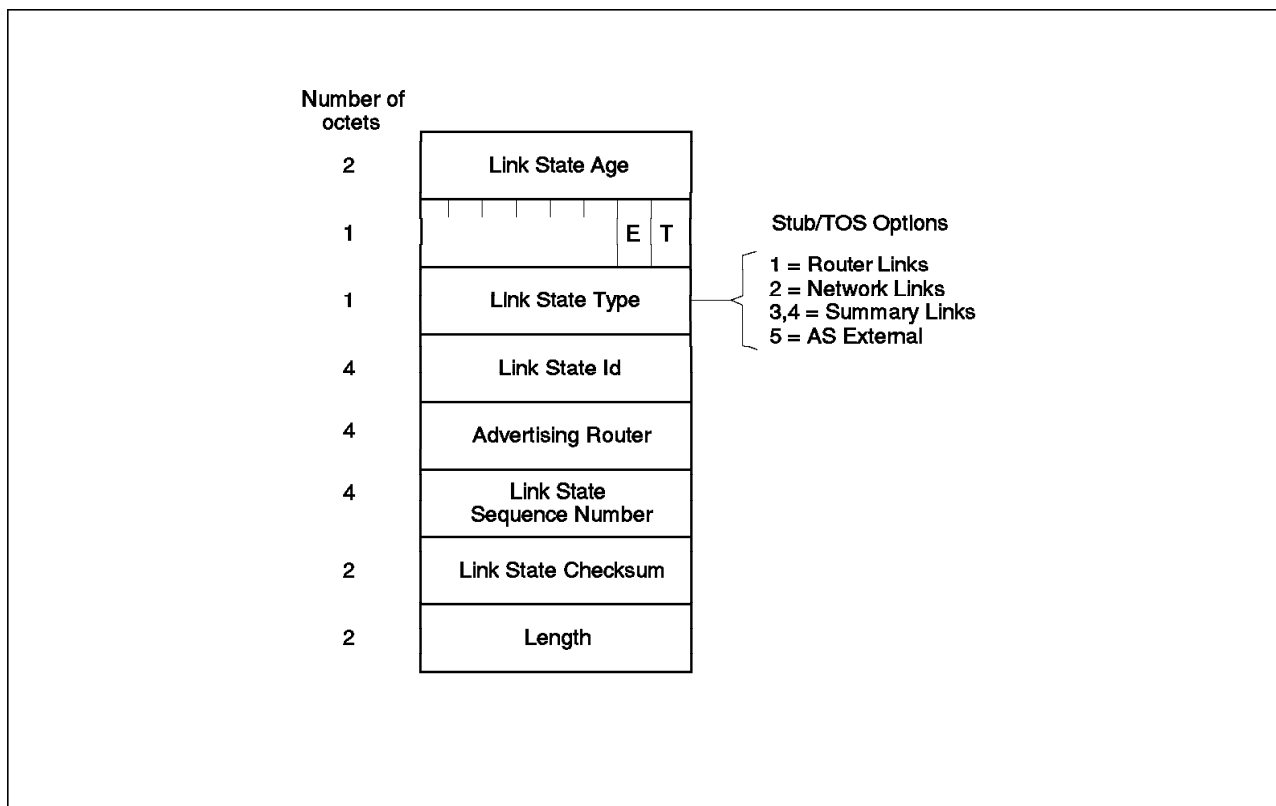


Figure 101. OSPF Link State Header

7.4.2.5 Routing Table Calculation

Each router in an OSPF area builds up a topology database of validated link state advertisements and uses them to calculate the network map for the area. From this map the router is able to determine the best route for each destination and insert it into its routing table.

Each advertisement contains an age field which is incremented while the advertisement is held in the database. An advertisement's age is never incremented past *max age*. When max age is reached it is excluded from routing table calculation, and re-flooded through the area as a newly originated advertisement.

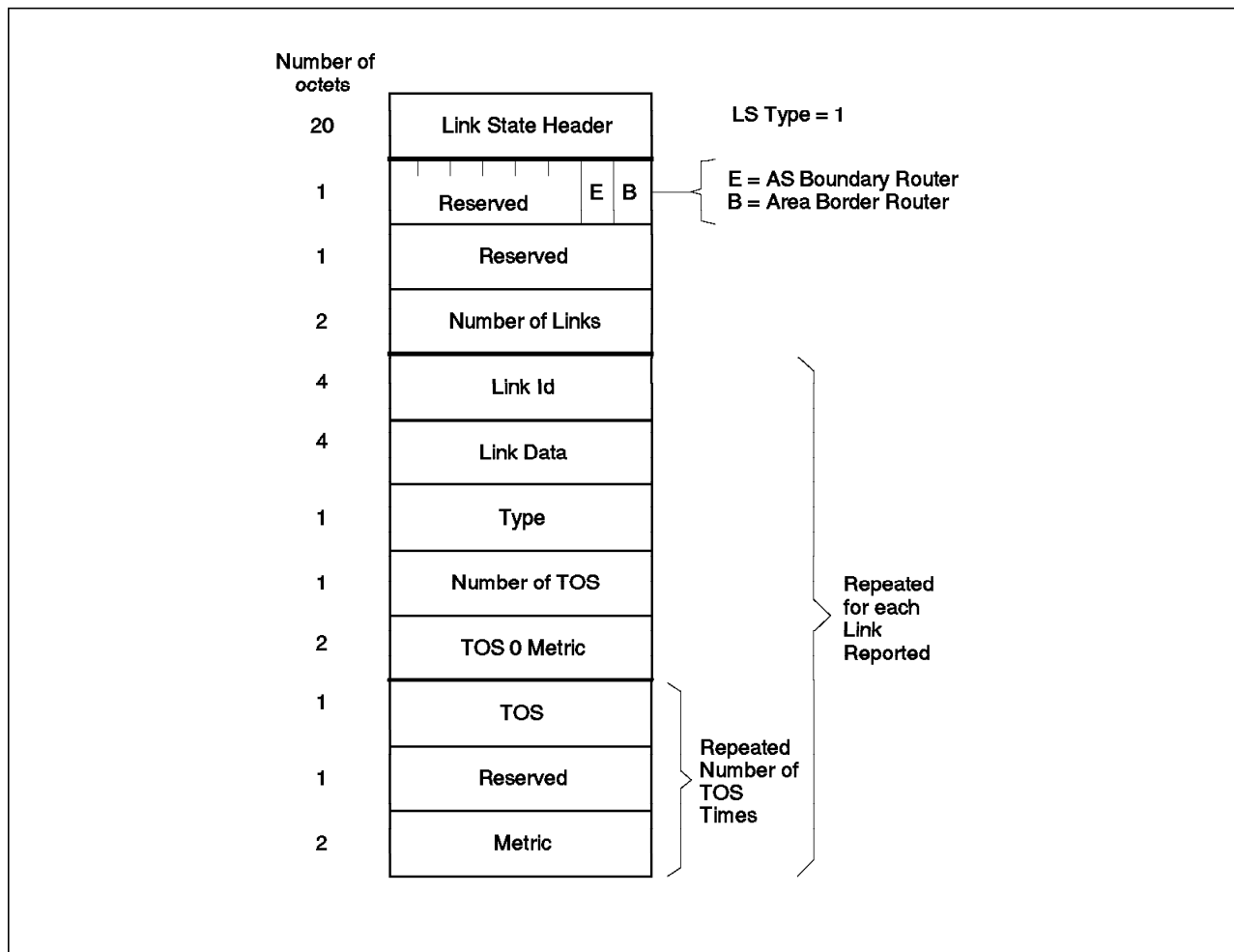


Figure 102. OSPF Router Links Advertisement

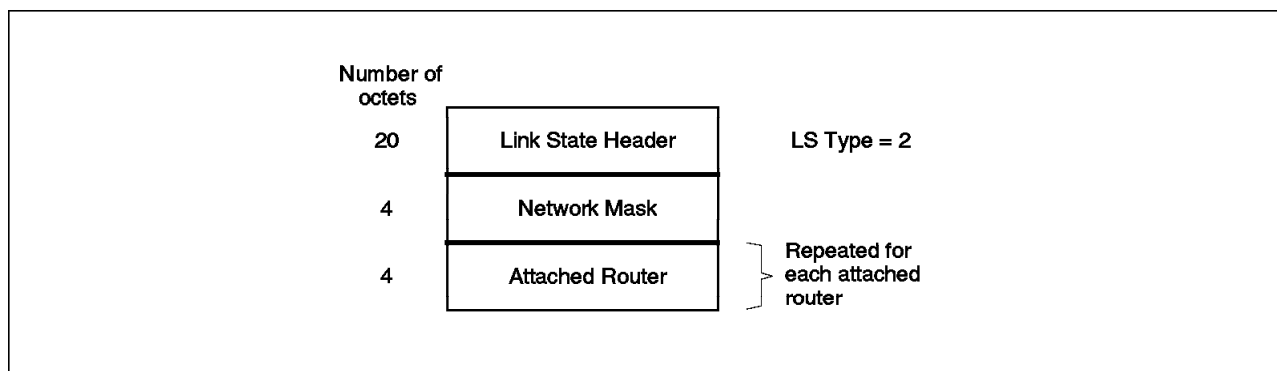


Figure 103. OSPF Network Links Advertisement

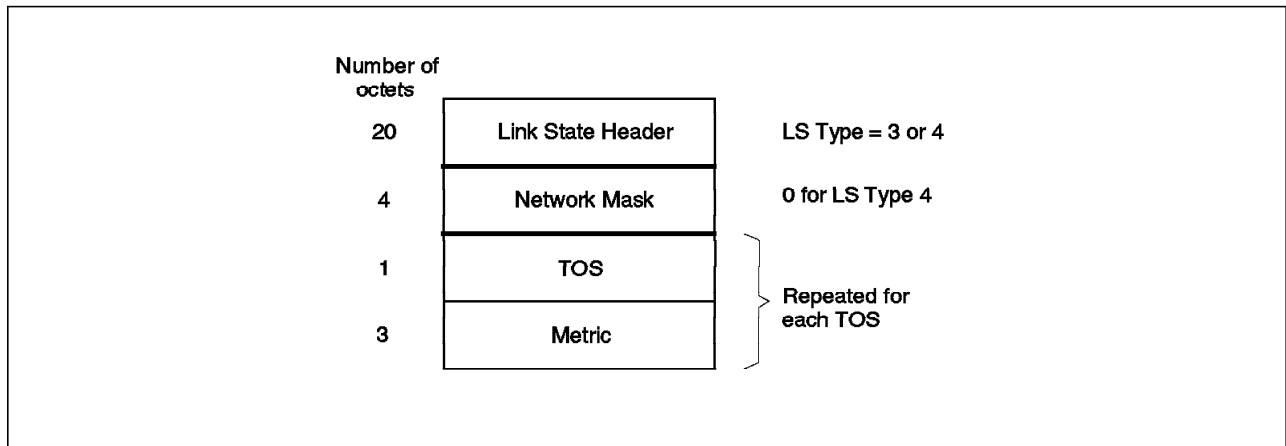


Figure 104. OSPF Summary Links Advertisement

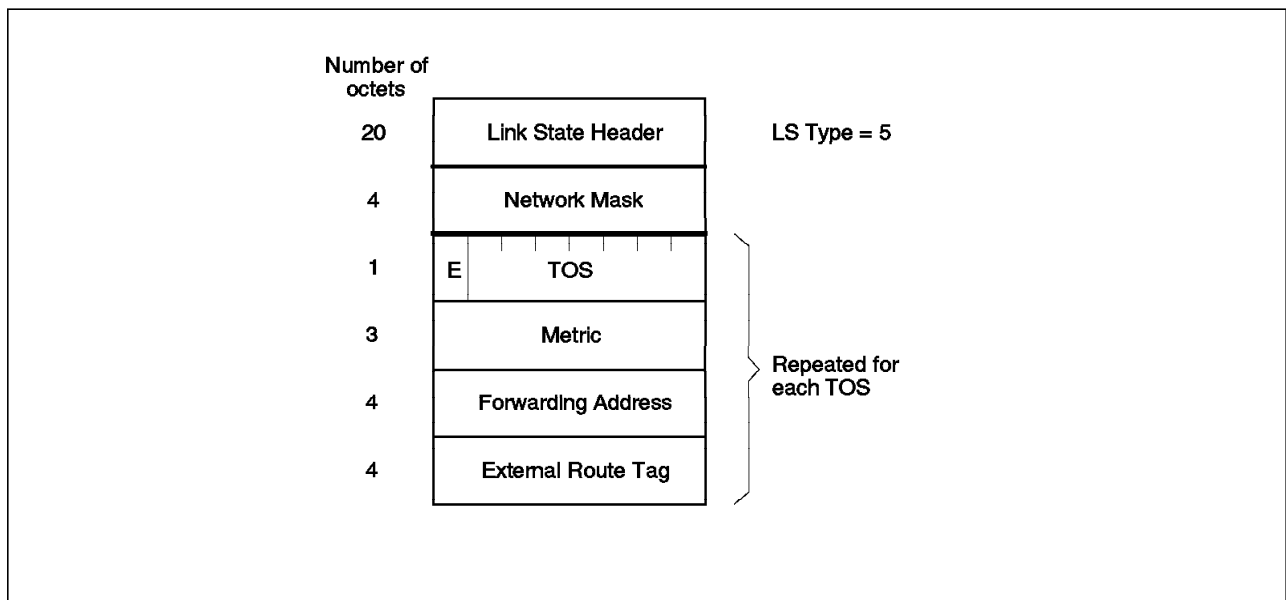


Figure 105. OSPF External Links Advertisement

Routers build up their routing table from the database of link state advertisements in the following sequence:

1. The shortest path tree is calculated from router and network links advertisements allowing best routes within the area to be determined.
2. Inter-area routes are added by examination of summary link advertisements.
3. AS external routes are added by examination of AS external link advertisements.

The topology graph or map constructed from the above process is used to update the routing table. The routing table is recalculated each time a new advertisement is received.

7.5 Border Gateway Protocol (BGP4)

The *Border Gateway Protocol* (BGP) is an exterior gateway protocol used to exchange network reachability information among autonomous systems. An AS is essentially a collection of routers and endnodes that operate under a single administrative organization. Within each AS, routers and endnodes share routing information by using an interior gateway protocol. The interior gateway protocol may be either RIP or OSPF.

BGP was introduced in the Internet in the loop-free exchange of routing information between autonomous systems. Based on Classless Inter-Domain Routing (CIDR), BGP has since evolved to support the aggregation and reduction of routing information.

In essence, CIDR is a strategy designed to address the following problems:

- Exhaustion of Class B address space
- Routing table growth

CIDR eliminates the concept of address classes and provides a method for summarizing n different routes into single routes. This significantly reduces the amount of routing information that BGP routers must store and exchange.

Note: IBM only supports the latest version of BGP, BGP4, which is defined in RFC 1654. All references to BGP in this chapter and on the interface of IBM's routers are BGP4, and do not apply to previous versions of BGP.

7.5.1 Protocol Description

BGP runs over a reliable transport layer connection between neighbor routers. BGP relies on the transport connection for fragmentation, retransmission, acknowledgement and sequencing. It assumes that the transport connection will close in an orderly fashion, delivering all data, in the event of an error notification.

Practical implementations of BGP use TCP as the transport mechanism. Therefore, BGP protocol data units are contained within TCP packets. Connections to the BGP service on a router use TCP port 179.

The BGP protocol comprises four main stages:

- Opening and confirming a BGP connection with a neighbor router
- Maintaining the BGP connection
- Sending reachability information
- Notification of error conditions

7.5.1.1 Opening and Confirming a BGP Connection

BGP communication between two routers commences with the TCP transport protocol connection being established.

Once the connection has been established, each router sends an *open* message to its neighbor.

The BGP open message, like all BGP messages, consists of a standard header plus packet-type specific contents. The standard header consists of a *16-octet*

marker field, which is set to all 1s, the *length* of the total BGP packet, and a *type* field that specifies the packet to be one of four possible types:

1. Open
2. Update
3. Notification
4. Keep alive

The format of the BGP header is shown in Figure 106

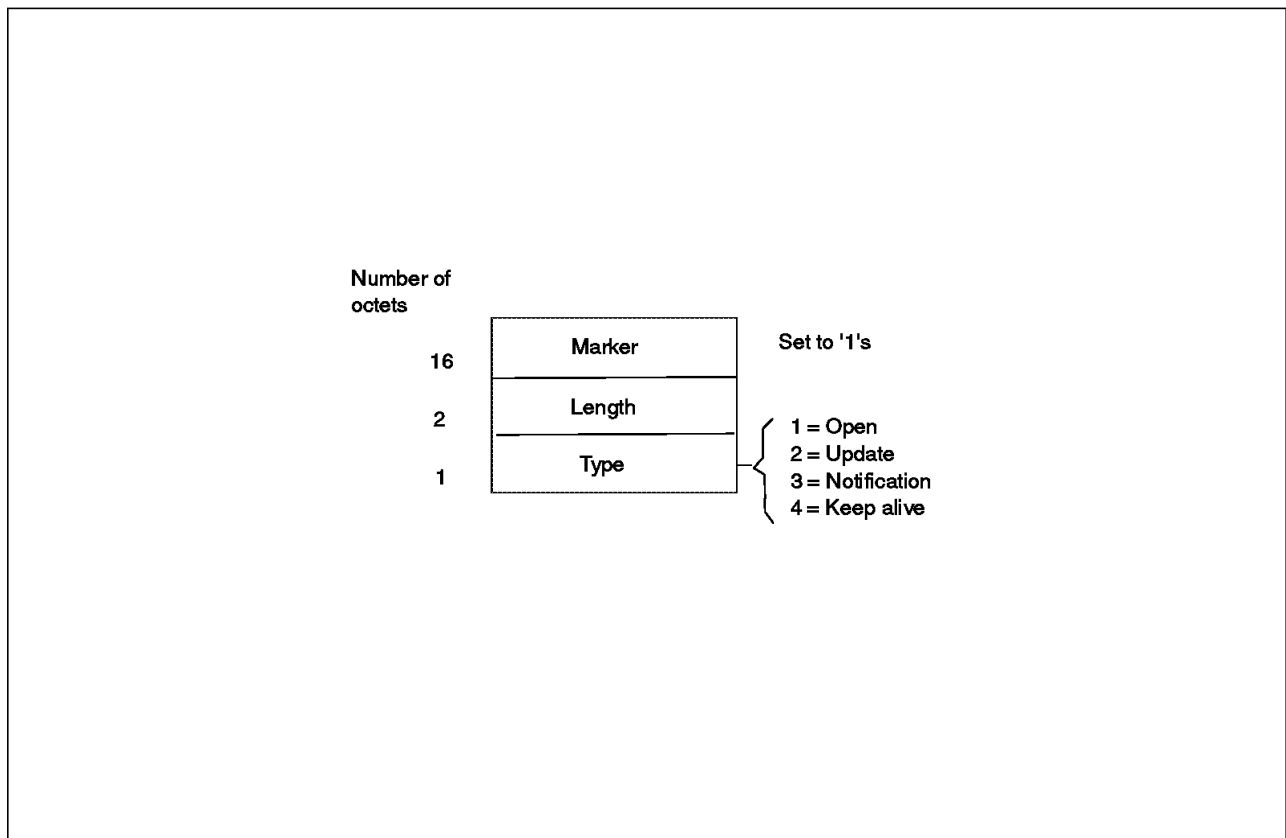


Figure 106. BGP Message Header

The open message defines the originating router's AS number, its BGP *router identifier* and the *hold time* for the connection. If no keep alive, update or notification messages are received for a period of hold time, the originating router assumes an error, sends a notification message, and closes the connection.

The open message also provides an *authentication code* and *authentication data*. The use of these fields is not fully defined in the RFC, and current BGP implementations use authentication code 0 with authentication data of all 0s.

The format of the open message is shown in Figure 107 on page 322

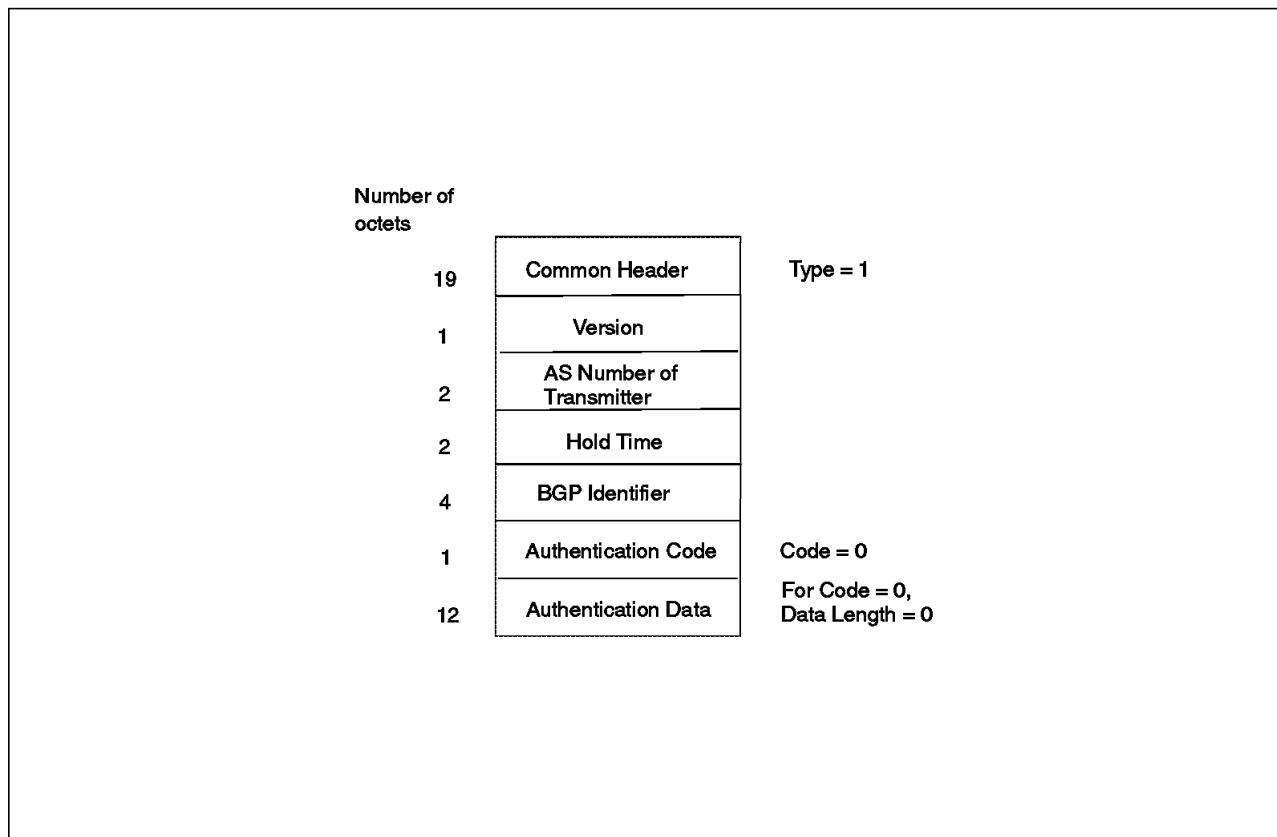


Figure 107. BGP Open Message

An acceptable open message is acknowledged by a *keep alive* message. Once neighbor routers have sent keep alive messages in response to opens, they can proceed to exchange further keep alives, notifications and updates.

7.5.1.2 Maintaining the BGP Connection

BGP messages must be exchanged periodically between neighbors. If no messages have been received for a period defined by hold time in the open message, then an error on the connection is assumed.

BGP uses keep alive messages to maintain the connection between neighbors. Keep alive messages consist of the BGP packet header only, with no data. The RFC recommends that they should be sent at intervals of approximately one third of the hold time.

7.5.1.3 Sending Reachability Information

Reachability information is exchanged between BGP neighbors in update messages.

An update message is used to advertise a single feasible route to a peer, or to withdraw infeasible routes from service. An Update may simultaneously advertise a feasible route and withdraw multiple infeasible routes from service. The format of these is shown in Figure 108 on page 323

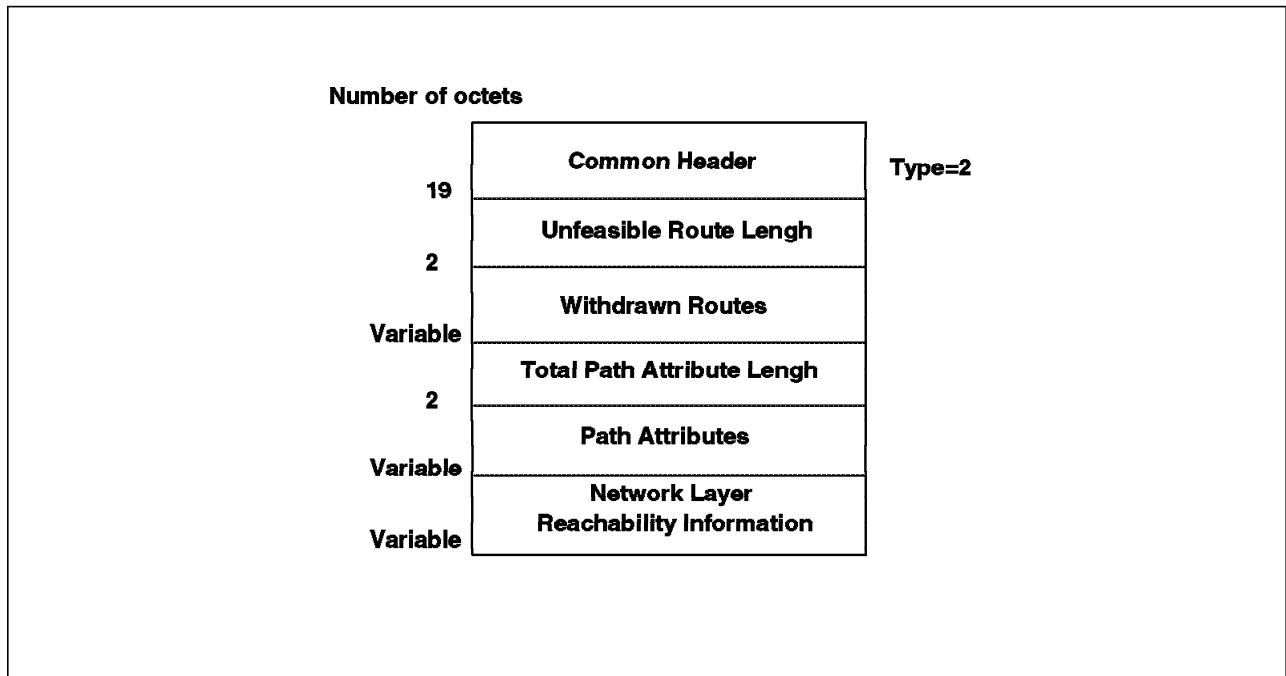


Figure 108. BGP Update Message

An infeasible route length indicates the total length of the withdrawn routes field, in octets. A value of it equals 0 indicates that no routes are being withdrawn from service, and that the Withdrawn Routes field is not present in this update message.

Withdrawn Routes is a variable length field that contains a list of IP address prefixes for the routes that are being withdrawn from service.

Each path attribute consists of a triple set of values: attribute flag, attribute type and attribute value. Three of the attribute flags provide information about the status of the attribute types, and may be optional or well-known, transitive or non-transitive and partial or complete.

Attribute flags must be read in conjunction with their associated attribute types. There are seven attribute types which together define an advertised route:

- Origin, which must be well-known, and defines the origin of the route as an interior gateway protocol, an exterior gateway protocol or other (for example a static route).
- AS Path, which must be well-known, and defines the ASs which must be crossed to reach the network being advertised.
- Next hop, which must be well-known, and defines the next hop to the network being advertised.
- Multi_exit_disc, which is an optional non-transitive attribute used by a BGP speaker's decision process to discriminate among multiple exit points to a neighboring autonomous system.
- Local_pref, which must be well-known, and used by a BGP speaker to inform other BGP speakers in its own autonomous system of the originating speaker's degree of preference for an advertised route.

- Atomic_aggregate, which must be well-known, and used by a BGP speaker to inform other BGP speakers that the local system selected a less specific route without selecting a more specific route which is included in it.
- Aggregator, which must be optional, and indicates the last AS number that formed the aggregate route, followed by the IP address of the BGP speaker that formed the aggregate route.

The format of BGP path attributes is shown in Figure 109.

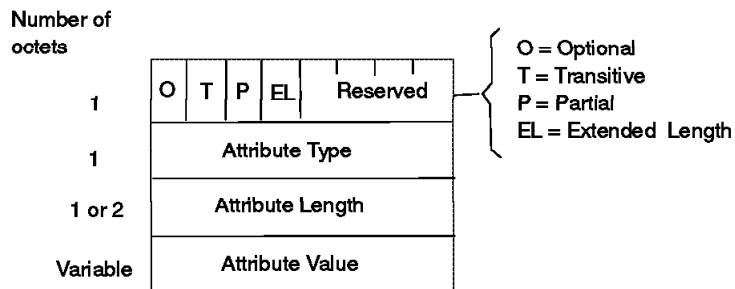


Figure 109. BGP Path Attributes

7.5.1.4 Notifying Errors

Notification messages are sent to a neighbor router when error conditions are detected. The BGP transport connection is closed immediately after a notification message has been sent.

Notification messages consist of an *error code* and an *error subcode*, which further qualifies the main error. The format of notification messages is shown in Figure 110 on page 325

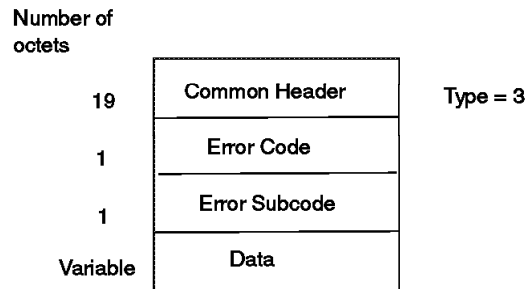


Figure 110. BGP Notification Message

Error codes that are provided by BGP are as follows:

- Message Header Error
- Open Message Error
- Update Message Error
- Hold Timer Expired
- Finite State Machine Error
- Cease

A *data field* is included in the notification message to provide additional diagnostic information.

7.6 ARP Subnet Routing

ARP Subnet Routing is described in RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*. It can be used to create subnets in IP networks with hosts that do not support the usage of subnets or to create subnets without modifying your routing protocol.

7.6.1 The Concept of ARP Subnet Routing

Consider one IP network, as shown in Figure 111, which is divided into subnets, interconnected by routers. In this example, we have two subnets (9.67.46.128 and 9.67.46.112), using a subnet mask of 255.255.255.240. However, none of the hosts knows about the existence of multiple physical networks and the IP subnets. The router uses the subnet mask of 255.255.255.240 and is aware of the different IP subnets within the network.

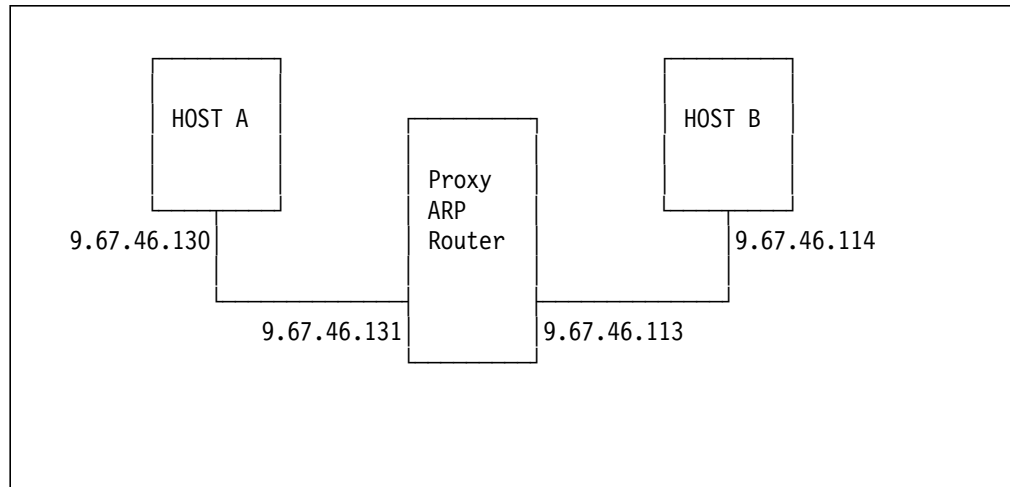


Figure 111. Proxy-ARP Router. The router uses subnet mask 255.255.255.240.

In this example, when Host A in subnet 9.67.46.128 wants to communicate with Host B in subnet 9.67.46.112 it assumes that Host B is on the same physical network and the same IP subnet as itself and sends out an ARP broadcast request. This request is received by the proxy ARP router. This router recognizes that the target protocol address in the broadcast request is an address in another subnet. If the router's routing table specifies that the next hop to that subnet is another physical network, it will reply to the ARP as if it were Host B.

Host A receives the ARP reply, puts it in its cache and will send future IP packets for Host B to the network address of the Proxy-ARP router. The router will forward those packets according to its subnetting mechanism.

7.7 IP Multicasting

IP multicasting allows you to address a set of IP hosts using a specific unique IP address. Such a set is called a *group* and the addresses reserved for those groups are the IP class D addresses. The IP class D address range is 224.0.0.0 through 239.255.255.255. Those addresses have the first four bits of the first octet set to 1110. The remainder is used to specify a multicast group. The address 224.0.0.0 is reserved. The address 224.0.0.1 is assigned to the all hosts group and identifies all hosts using IP multicasting. It is only used on a local network.

Being a member of a group means that you want to receive datagrams sent to this group address. You may send datagrams to a multicast without being a member of a group. An IP multicast address can only be used in the destination address field. You can *join* or *leave* a group. A group existence is dynamic; if there are no members, there is no group. There are, however, so-called *well-known* groups. They are assigned by the Internet authority and correspond

to groups that exist even when there are no members. This is called a permanent group. An example of this is OSPF. OSPF uses the multicast address 224.0.0.5 to send OSPF packets on broadcast networks or on point-to-point connections. The IP multicast software needs to recognize IP multicast addresses if it has applications running which are members of a certain multicast group. It must pass copies of the multicast packets to each application which is a member of that group. A group membership is associated with a network. You may want to share your membership only with hosts on your local network. The IP software which implements this kind of functionality is called Internet Group Management Protocol (IGMP).

7.7.1 IGMP

Internet Group Management Protocol (IGMP) is described in RFC 1112 *Host Extensions for IP Multicasting*. The following is a brief overview of IGMP:

- When a local host wants to join a new multicast group, it sends an IGMP message to the *all hosts group address* with its membership information. This is called an *IGMP Host Membership Report*.
- A local IGMP router receives this membership information.
- This local IGMP router contacts other multicast routers to establish routes and to pass the membership information.
- The local IGMP router polls its local hosts to find out which hosts are still members of the group. This is called an *IGMP Host Membership Query*.
- If there are no local members anymore, the local IGMP gateway stops advertising this group to the other multicast routers.

To prevent local network congestion due to membership advertisements and IGMP router polls, the following is implemented by IGMP:

- The polling rate is set to a maximum of one poll per minute.
- The IGMP router will not poll for each group separately, but will send one query request for all the groups.
- Hosts will not respond to each applicable request, but will use a mechanism by which they listen to responses from other nodes. They will respond only after a random delay, if they have not heard a response within this delay from another host on that network.

The address assignment is not described by this RFC, neither is the routing mechanism between IGMP routers. When you do not use a routing mechanism between IGMP routers, you should define a tunnel between two IGMP routers if you cross an IP network. Using an IP tunnel, IP multicast packets are encapsulated into unicast packets and sent to the IGMP destination router by using normal routing protocols.

A Multicast OSPF (MOSPF), which is an implementation of multicasting, is described in the next section.

7.7.2 Multicast OSPF (MOSPF)

MOSPF (Multicast OSPF) is an enhancement to OSPF. It is described in RFC 1584 *Multicast Extensions of OSPF* and experiences are described in RFC 1585 *MOSPF: Analysis and Experience*.

MOSPF routers use the IGMP protocol to monitor multicast group membership on local LANs through sending of IGMP Host Membership Queries, and reception

of IGMP Host Membership Reports. A MOSPF router then distributes this group location information throughout the routing domain by flooding a new type of OSPF link state advertisement, the group-membership-LSA (type 6). This in turn enables the MOSPF routers to most efficiently forward a multicast datagram to its multiple destinations. A network of routers running MOSPF can forward IP multicast packets directly, sending no more than one copy over a link, and without the need of IP tunnels.

MOSPF is meant to be used internally to a single Autonomous System. When supporting IP multicast over the entire Internet or multiple OSPF areas, MOSPF would have to be used in concert with an inter-AS multicast routing protocol. An example of such protocol is the Distance Vector Multicast Routing Protocol (DVMRP), which is described in the following section.

7.7.3 Distance Vector Multicast Routing Protocol (DVMRP)

DVMRP is a protocol similar to RIP; it passes information about the current multicast group membership and the cost of routes between gateways. MOSPF domains will link to a DVMRP router or domain by using a tunnel. DVMRP uses IGMP messages with a special format to exchange membership information among its attached domains. From this information, the routers will build a routing tree for each possible multicast group. The usage of DVMRP is still experimental; advantages of using it should be fewer configured tunnels and less multicast traffic on the links inside an MOSPF domain.

Chapter 8. The IBM 2210 as an IP Router

The IBM 2210 supports three dynamic routing protocols. All three routing protocols can run simultaneously on IBM 2210.

The following are IP dynamic routing protocols supported by IBM 2210:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol Version 4 (BGP4)

Additionally, the IBM 2210 implements IP multicasting routing protocols MOSPF and DVMRP.

Please refer to Chapter 7, "IP Routing Protocols" on page 295 for a general description of these protocols.

The IBM 2210 supports ARP Subnet Routing (RFC 1027 - also known as Proxy-ARP) and static routing.

This chapter describes the IP routing implementation on the IBM 2210.

8.1 IP Implementation

The IBM 2210 implements the following IP functions:

- IP

This is an unreliable and connectionless delivery mechanism which defines the IP datagram and specifies the delivery of these datagrams across the underlying network.

- ICMP

Internet Control Message Protocol is used to report errors and provide information about unexpected circumstances. It includes support of Echo Request/Reply messages (known as PING), redirect messages (to direct a host to use another hop), and Source-Quench messages (used for congestion control).

- TCP

Transmission Control Protocol is the connection-oriented protocol that allows the reliable stream delivery of data across a network from a TCP module on one machine to a TCP module on another machine.

- Telnet

A simple remote terminal protocol that allows a user at one site to establish a TCP connection to a Telnet server at another site.

- UDP

User Datagram Protocol provides a mechanism that allows application programs to send datagrams to other application programs.

- SNMP

Simple Network Management Protocol is used to monitor IP routers and the network to which they attach.

- TFTP

Trivial File Transfer Protocol is a simple file transfer protocol that runs on top of UDP.

- BootP

The Bootstrap Protocol can be used by diskless machines to learn their IP address and the location of the boot file and boot server.

8.1.1 General IP Parameters

When planning to use the IBM 2210 as an IP router, there are a number of IP parameters that you may configure, regardless of the routing protocol used in your IBM 2210. These parameters are:

- Internal IP address

You may assign an internal IP address to the IBM 2210. The internal address belongs to the router as a whole and not to a particular interface. This address is always reachable as long as one interface on the router is active. This address is also used by the Data Link Switching (DLSw) feature.

- Router ID

You may also assign a router ID to your IBM 2210. This will be the default IP address used in various kinds of IP traffic that originated from the router. For example, it will be used as the IP source address in PING, TFTP or Traceroute packets.

- Routing table size

Each IBM 2210 has a routing table that contains the dynamic routing information known by your router. Each entry in the routing table is 64 bytes, and the routing table size is 768 entries by default.

You may change the number of entries in the IP routing table based on the requirements of your network.

- Router cache size

The IBM 2210 uses a routing cache that contains the recently routed destinations. The router will reference the cache first before using the routing table. The minimum and default size for the router cache table is 64 entries. However, you may change the router cache size based on your requirements.

- IP broadcast format

IBM 2210 allows you to specify the format that will be used by your IBM 2210 when broadcasting packets on a specific interface. In doing so, you must specify the style and the fill-pattern to be used.

The style parameter can be either local-wire or network. When you specify local-wire for the style, the router will use the broadcast address of either 255.255.255.255 or 0.0.0.0. The former is used if you have specified the fill-pattern to be 1, and the latter is used with the fill-pattern of 0.

When you specify network for the style, the router will send the broadcast messages that begin with the network and the subnetwork portion of the IP

address of the interface. The host portion of the broadcast messages will be either all 1s or 0s, depending on the value specified for the fill-pattern parameter.

Note: When receiving messages, the IBM 2210 recognizes all forms of the IP broadcast addresses, regardless of the settings of these parameters.

- Reassembly size

You can configure the size of the buffers that are used for the reassembly of the fragmented IP packets received by the router.

By default, IBM 2210 uses buffers of 12000 bytes.

You can configure a route to a default gateway and the cost of reaching that default gateway. Normally, the default gateway is a router that has more routing information about the network.

- Default subnetwork gateway

In a subnetted network, you can configure a separate default gateway and the cost of reaching it for each subnet network.

All the packets detained for unknown subnets of a known subnetted network are forwarded to the subnetwork's default gateway.

- IP access control

The access control system allows the IBM 2210 to determine which packets are to be forwarded and which packets are to be discarded. For more information, refer to 8.1.11, "Access Controls" on page 337.

8.1.2 Interface Address Assignments

When you assign IP addresses to the router, note the following:

- You must assign at least one IP address to an interface. A hardware interface does not accept or send IP packets unless it has at least one IP address.
- It is possible to assign more than one IP address to an interface.
- You must specify an IP address together with its subnet mask.

Note

Serial lines do not *need* addresses. Such lines are called unnumbered and can be configured without IP addresses, but still enable them for IP traffic using the following command:

IP Config>**Add address 1 0.0.0.1**

The use of unnumbered serial lines has some restrictions which are documented in information APAR II08361.

8.1.3 RIP Implementation in IBM 2210

The following must be considered when configuring RIP for your IBM 2210:

- Only the network portion, as defined by a mask, is entered into the routing table.
- Masks are not sent in RIP broadcasts.

- The maximum number of hops is 15, and a hop count of 16 indicates infinity.
- Destination entries time out after three minutes.
- RIP updates are sent every 30 seconds.
- Variable length subnet masks are not supported.
- RIP is not supported across X.25 circuits.
- Split horizon is always used.
- Poison reverse may be enabled for individual interfaces.
- The 2210 does not accept host-routes in RIP updates.

8.1.3.1 RIP Interoperability with IBM 6611 Network Processor

To use RIP between the IBM 6611 Network Processor and the IBM 2210 take the following into consideration:

1. The broadcast address type used by the IBM 2210

The 6611 only recognizes *local-wire* broadcasts. In our case, testing with V1R3 of MPNP, we found that both fill types are accepted. So broadcasting to 255.255.255.255 or 0.0.0.0 is accepted by the 6611.

2. The RIP version configured for IBM 6611 Network Processor

IBM 6611 Network Processor can be configured to use either RIP Version 1 or RIP Version 2. IBM 2210 only supports RIP Version 1. Therefore, when using RIP between the IBM 2210 and the IBM 6611 Network Processor, the 6611 must be configured to use RIP Version 1.

8.1.4 OSPF Implementation

OSPF implementation sets the OSPF router ID to the address of the first OSPF interface appearing in the router's configuration. However, you may change the router ID using the configuration commands from the ASCII console or the General panel in the IP subdirectory of the Nways MRS Configuration Program.

Note

When you change the router ID of your IBM 2210, the link state advertisements originated by the router before the router ID change may persist in the network for as long as 30 minutes. This may cause an increase in the size of the link state database.

The OSPF implementation in the IBM 2210 provides support for TOS-based routing for TOS 0 only.

IBM 2210 provides support for *simple password*, allowing the authentication of the link state advertisement received from the other routers. To provide authentication, do the following:

1. Specify authentication type 1 when you define the OSPF area.
2. Specify the authentication key to be used when you configure the OSPF parameters for each interface.

You can import routes learned from other protocols (BGP, RIP or static routes) into the OSPF domain when the OSPF router is configured as an AS boundary

router. An OSPF router can also originate a default route into the area. For these purposes enable AS boundary routing.

8.1.4.1 OSPF and Non-Broadcast Networks

If the IBM 2210 is connected to a non-broadcast multi-access (NBMA) network and is eligible to become the *designated router*, provide the router with the information to find its OSPF neighbor(s). You can achieve this by performing the following tasks:

- Define the interface to the NBMA network as non-broadcast.
- Specify the IP address of the OSPF neighbor(s) on the NBMA network.
- Configure your IBM 2210 to become the designated router.

In a star frame relay network with only 2210s, you can use the OSPF point-to-multipoint frame relay enhancement. Refer to Figure 112 for an example of a star or partially meshed network. This type of network is also known as a spoke-and-hub network.

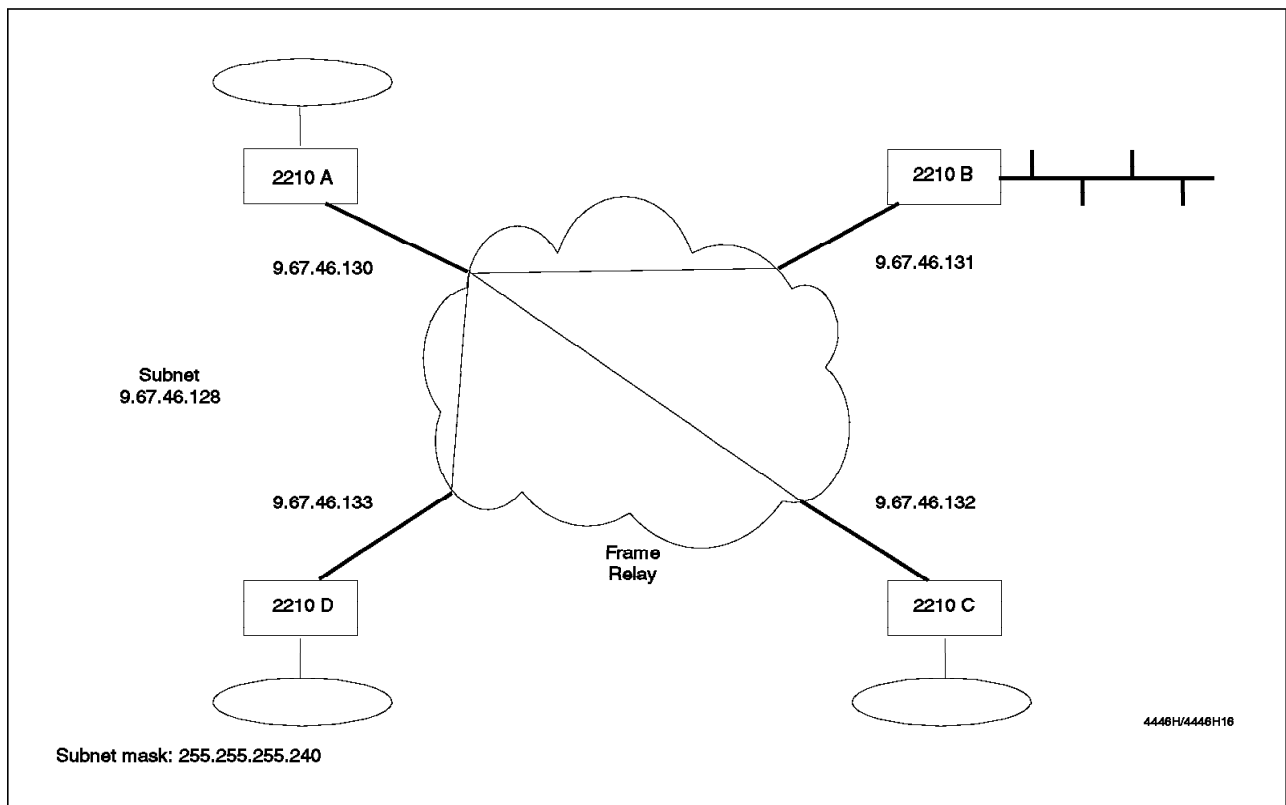


Figure 112. OSPF Point-to-Multipoint Frame Relay

Using the OSPF point-to-multipoint frame relay enhancement provided by IBM 2210, you may now assign a single IP subnet to an entire frame relay cloud and thus a single IP address to each frame relay interface of the router. In this case you only need to specify the OSPF neighbor at one side of each DLCI. In configuring such a network, perform the following tasks:

1. Assign an IP address to the frame relay interface.
2. Enable OSPF on this interface.
3. Define the OSPF neighbor on one side of each DLCI (PVC).

4. To prevent one of the spokes from becoming the designated router, specify a router priority of 0 for the spokes and anything else but 0 for the hub router.

Note

In this type of OSPF configuration environment it is not necessary to use the set non-broadcast command for each interface. By *not* using this command, the router will determine that you intend to use the OSPF point-to-multipoint frame relay enhancement.

8.1.4.2 OSPF Interoperability with IBM 6611 Network Processor

There are no specific OSPF considerations for connecting the IBM 2210 to the IBM 6611 Network Processor when using OSPF.

Concerning frame relay, OSPF and 6611 interoperability, two scenarios were tested, scenario A and B:

- A: A fully meshed frame relay network with two 2210 routers and one 6611.
- B: A partially meshed frame relay network in a star configuration where the 6611 is the hub and the 2210 routers are the spokes.

Scenario A: Refer to 10.6.2, “Scenario 2: DLSw between Two 2210s and 6611 over Frame Relay” on page 484 for a full listing of the configuration steps. Below, the steps concerning frame relay and OSPF are summarized, including the 6611 basic definitions:

- Assign an IP address to the 2210 frame relay interface.
- Enable OSPF and assign the interface to be an OSPF interface.
- Specify the interface as non-broadcast.
- Specify the 6611’s IP address as your OSPF neighbor on that interface and make it eligible to become the designated router.

On the 6611:

- Assign an IP address to the 6611 frame relay interface
- Specify this interface as fully meshed.
- Enable OSPF and assign the interface to be an OSPF interface.

The interface type on the 2210 will specify non-broadcast multi-access (NBMA).

Scenario B: No scenario is included. The differences are summarized in the steps below:

- Assign an IP address to the 2210 frame relay interface.
- Enable OSPF and assign the interface to be an OSPF interface.
- Specify the 6611’s IP address as your OSPF neighbor on that interface and make it eligible to become the designated router.

On the 6611:

- Assign an IP address to the 6611 frame relay interface.
- Specify the DLCIs with their destination IP address as point-to-point links.
- Enable OSPF and assign both interfaces, represented by the IP destination address, as OSPF interfaces.

The interface type on the IBM 2210 will be *P-to-MP* (point-to-multipoint). Using this configuration, the spoke routers can still reach each other via the hub. The 6611 will take care of the routing between the spokes.

8.1.5 MOSPF

Multicasting is already used within OSPF. OSPF packets are sent to a standard multicast IP address of 224.0.0.5.

The 2210 extends this mechanism by implementing MOSPF. When you enable the multicast forwarding capability for each interface, you can specify the following:

- Enable multicast forwarding on the interface.
- Enable the forwarding of multicast packets as unicast or multicast.
- Configure the IGMP polling interval.
- Configure the IGMP local database timeout.

The MOSPF function is used by the IBM 2210 for DLSw and IP tunneling. Both implement client/server groups and peer groups for partner definitions.

DLSw uses a base multicast address of 225.0.1.0 for client and peers and address 225.0.65.0 for servers. The last octet of this address is used to identify the DLSw group number of the client/server group or peer group.

The IP bridge tunnel uses 224.168.0.0 as a base address for client/server groups as well as for peer groups. In this case the last two octets will be used to identify a group.

Within this implementation it is also possible to manually change these addresses and to join or leave a multicast group by specifying its IP address.

8.1.6 DVMRP

Distance-Vector Multicast Routing Protocol (DVMRP) allows you to define IP tunnels between MOSPF domains and a DVMRP domain/router. You can configure an IBM 2210 to use DVMRP and define interface(s) to use it.

8.1.7 BGP4 Implementation

BGP routers selectively collect and advertise reachability information to and from BGP neighbors in their own and other autonomous systems. Reachability information consists of the sequences of AS numbers that form the paths to particular BGP speakers and the list of IP network that can be reached via each advertised path. An AS is an administrative group of networks and routers that share reachability information using one or more Interior Gateway Protocols (IGPs), such as RIP or OSPF.

Routers that run BGP are called BGP speakers. These routers function as servers with respect to their BGP neighbors (clients). Each BGP router opens a passive TCP connection on port 179 and listens for incoming connections from neighbors at this well-known address. The router also opens active TCP connections to enabled BGP neighbors. This TCP connection enables BGP routers to share and update reachability with neighbors in the same or other autonomous systems.

Connections between BGP speakers in the same AS are called internal BGP (IBGP) connections, while connections between BGP speakers in different autonomous systems are external BGP (EBGP) connections.

A single AS may have one or more BGP connections to outside autonomous systems.

Decisions on which reachability information to advertise (send) and which to accept (receive) are made on the basis of explicitly defined policy statements. IBM's BGP4 implementation supports three types of policy statements:

- Originate Policies
- Send Policies
- Receive Policies

BGP routers use four kinds of messages to communicate with their neighbors: open, keep alive, update, and notification messages.

- Open

Open messages are the first messages transmitted when a link to BGP neighbor comes up and establishes a connection.

- Keep alive

Keep-alive messages are used by BGP routers to inform one another that a particular connection is alive and working.

- Update

Update messages contain the interior routing table information. BGP speakers send update messages only when there is a change in their routing tables.

- Notification

Notification messages are sent whenever a BGP speaker detects a condition that forces it to terminate an existing connection. These messages are advertised before the connection is transmitted.

8.1.8 Static Route Implementation

You can define a static route for:

- Default gateway

Packets are routed to the default gateway when the destination cannot be found in the routing table.

- Default subnet gateways

If you are using subnetted networks, you can define a separate default gateway for each subnetted network.

- Static network/subnet/hosts routes

For each destination that is to have a fixed route, you can define a static route.

8.1.9 IP Filters

You can use IP filters to prevent forwarding the packets for a network or subnet. This includes distribution of routing information about these networks.

8.1.10 IP Source Routing

The IP source routing IP options can be used to specify hop-by-hop the route an IP datagram should take through the network. At each intermediate router, the IP destination address in the IP header is modified to the address of the next-hop router. Since the final destination address is not contained in the IP header, IP source routing can be used to bypass access-control filters and compromise the intended security policies.

The IBM 2210 has provided the capability to disable IP source routing to keep outsiders from bypassing access-control filters.

8.1.11 Access Controls

The access control system allows you to be much more specific in filtering IP traffic. You can control access to particular classes of IP addresses and services by controlling source and destination IP addresses, IP protocol numbers and port numbers for the TCP and UDP protocols.

When you enable access control and add an entry to the list, all the IP packets originated, forwarded, or received by the router are checked against the access control list. The following rules apply to this checking mechanism:

- For each packet received, the headers are compared to all the specified fields in each entry in the list.
- If the entry matches the packet and the entry is *inclusive*, the packet is forwarded.
- If the entry matches the packet and the entry is *exclusive*, the packet is discarded.
- If there is no match with the entries in the access control list, the packet is discarded.
- Each entry has an IP address and source and destination IP address.
- Each IP address is logically "AND-ed" with the mask and compared to the address in the entry.
- A mask of 255.255.255.255 matches only the resulting address itself.
- A mask of 0.0.0.0 and the resulting address of 0.0.0.0 is a wildcard and matches any IP address.
- Each entry may have an optional IP protocol number range. A range of 0 to 255 will match to all IP packets (within the address range).
- Each entry may have an optional port number range for UDP or TCP headers.

This implication of the above rules is that if you want to make one exclusion, add inclusion(s) for all the other IP traffic that you want to be forwarded by the router.

8.1.12 BootP Implementation

The IBM 2210 implements the BootP client function and the BootP relay agent, also known as BootP forwarder. The 2210 may use the BootP client function to obtain its boot file (refer to 2.2, "Boot Files and Boot Processes" on page 19). It may also be configured to forward BootP requests to a BootP server.

The 2210 cannot act as a BootP server. You need a host running the bootpd daemon. A BootP server contains a file that lists all the BootP clients for which this server is responsible, their associated IP addresses, and the location and name of their boot files.

The following is a summary of the BootP process:

1. The BootP client copies its MAC address into a BootP packet (based on UDP) and broadcasts it onto the LAN.
2. If the BootP client and server are not on the same network, a local BootP relay agent will receive the request from the client and route it to its defined BootP server(s) (or the next BootP relay agent and route to the BootP server).
3. The BootP server receives the request and tries to match the MAC address with one in its list. If it finds a match, it will send a BootP reply with the client's IP address, subnet mask, and BootP server name. If the BootP client and server are not on the same network, the BootP reply may go through relay agent(s) to reach the client. In this case the relay agent receives the BootP reply, adds an entry to its ARP table, and forwards the reply to the client.
4. The client uses the information that is contained in the reply to initiate a TFTP request to the TFTP server to download the boot image.

You need to assign two parameters when you define the router as a BootP forwarder (relay agent):

- The maximum number of hops you want the BootP request to go through. This is not the number of IP subnetworks, but the number of BootP relay agents needed to get the server from the client (and vice versa).
- The number of seconds you want the client to retry before the BootP request is forwarded. BootP uses a technique of timeout and retransmission. When a client sends a BootP request, it starts a timer. If it does not receive a response before the timer expires, it retransmits the request. This process will be repeated the number of times that you have specified.

8.1.13 Telnet Implementation

To allow you to access the ASCII console interface remotely, the IBM 2210 implements the Telnet function. It allows you to have five Telnet sessions: two servers (inbound to the router) and three clients (outbound from the router).

From a Telnet session, the IBM 2210 does not provide you with any indication of which router you are logged into. You may determine the router by displaying the configuration information of the router. Alternatively, you may use (Ctrl+]) to access the Telnet command mode. You can then issue the status command to display the IP address of the station you are connected to and the current terminal mode.

8.1.14 SNMP Implementation

SNMP (Simple Network Management Protocol) runs on top of UDP and is used for monitoring and managing IP hosts in an IP network. SNMP enables network hosts running vendor-supplied software to read and modify some of the router's operational parameters. In this way, network management can be established for the IP community. The software that processes the SNMP requests from the network management hosts runs on the IBM 2210 and is called an *SNMP agent*.

The following are the various aspects of SNMP that you need to consider when configuring SNMP for your IBM 2210.

8.1.14.1 Authentication

In SNMP, you can define a community. The SNMP community is simply a group of nodes that share network management information. The community is established at configuration time.

The community allows you to define the IP address of the SNMP management station that is allowed to access the information in the SNMP agent's Management Information Base (MIB). It allows you to define a *community name* in accessing the MIB. The community name is used as an authentication scheme that prevents unauthorized users from learning information about an SNMP agent or from modifying its characteristics. By defining an authentication scheme, you can provide security in your network management system.

Note: If no IP address is defined for the SNMP manager in your community table, any IP station that provides the correct community name will be able to access the MIB in the SNMP agent.

8.1.14.2 MIB Support

The operational parameters, or variables, are defined by a MIB (Management Information Base). The standard MIBs supported by IBM 2210 are described in Appendix A of *The Nways MRS Protocol Configuration and Monitoring Reference Volume 1 Version 1 Release 1*.

For each community name, you can specify which MIB, or which part of a MIB, can be accessed by the members of that community. To do so, first add one or more MIB object IDs (the identification of a MIB item) to a view, creating a *subtree*. Then, you assign a view to a community.

8.1.14.3 Traps

SNMP agents can create *trap messages*. These are unsolicited messages that are sent from the router to an SNMP manager in response to a router, network event or condition, such as a router reload or network down. The IBM 2210 provides two types of traps that can be enabled or disabled separately for a specific community name:

- General traps

These traps are defined by the RFCs and allow the router to send the traps asynchronously to the SNMP manager in case of a specific event. There are six general traps defined:

- Link-up
- Link-down
- Cold start

- Warm start
- EGP neighbor loss
- Authentication failure
- Enterprise specific traps

These traps are specific traps that can be generated by event logging system (ELS) messages. You can use the ELS *trap* command to enable sending of messages or groups of messages via an SNMP trap. To enable forwarding by the SNMP agent of your router, enable the trap by typing *enterprise*. The SNMP manager, however, must support these enterprise traps because they are specific to the IBM 2210.

8.1.15 TFTP Implementation

The IBM 2210 implements the TFTP client function and the TFTP server function. The client function allows you to send or receive configurations or boot images to/from a TFTP server. The server function is implemented to provide other routers with a boot image or a configuration file. This implementation allows multiple, simultaneous file transfers between the router's nonvolatile configuration memory (NVCNFG), the Integrated Boot Device (IBD), and remote hosts. Refer to 2.2, "Boot Files and Boot Processes" on page 19 for more information about the boot mechanism.

The TFTP implementation does not allow you to use PUT or COPY to transfer files to another router.

When a router acts as a TFTP server, transfers are transparent to the user. Use the ELS message log to view the transfers in progress. To view all TFTP messages, go to the ELS prompt of the GWCON and issue the following commands:

+ **event**

ELS>**display subsystem tftp all**

You can view the messages either by using the following command to display the messages on the CONFIG console:

* **divert 2 0**

or by using the following command to view the messages on the MONITOR console:

* **talk 2**

8.1.16 ARP-Subnet Routing

The IBM 2210 implements the proxy ARP router function. When the router is configured for ARP subnet routing, it will reply by proxy to the ARP requests for destination that are reachable via the 2210's interfaces. For a description on ARP-subnet routing, refer to 7.6.1, "The Concept of ARP Subnet Routing" on page 326.

8.2 Configuring IP on the IBM 2210

To configure IP on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRS.

8.2.1 IP Configuration Commands

This section summarizes the IP configuration commands available within the CONFIG process of the Nways MRS. To access the commands, issue the following command:

Config>**protocol ip**

Table 55 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference Volume 1 Version 1 Release 1* covers these commands in detail.

Table 55 (Page 1 of 3). IP Configuration Commands	
Command	Function
? (Help)	Lists all the IP configuration commands, or lists the actions associated with specific commands.
Add access-control	Adds an access control entry to the end of the access control list.
Add address	Assigns an IP address to one of the router's hardware network interfaces.
Add bootp-server	Adds a BootP server to the network configuration.
Add filter	Designates an IP network/subnet to be filtered.
Add packet-filter	Define a packet filter record within the router configuration.
Add route	Adds a static network/subnet route to the router's IP configuration.
Add UDP-destination	Adds a UDP destination port number and IP address.
Change address	Modifies one of the router's IP interface addresses.
Change filter	Modifies the subnet mask associated with a filtered network/subnet.
Change route	Modifies either the subnet mask, next hop, or the cost associated with a configured static network/subnet route.
Delete access-control	Deletes one of the access control records.
Delete address	Deletes one of the router's IP interface addresses.
Delete bootp-server	Removes a BootP server from an IP configuration.
Delete default network/subnet-gateway	Deletes either the default gateway or the default subnet gateway for the specified subnetted network.
Delete filter	Deletes one of the router's filtered networks.
Delete packet-filter	Deletes a specified packet-filter from the router configuration.
Delete route	Deletes one of the router's configured static routes.
Delete UDP-destination	Deletes a UDP forwarding destination address that was configured using the add udp-destination command.
Disable arp-net-routing	Turns off ARP network routing.
Disable arp-subnet-routing	Turns off the IP feature called ARP subnet routing or proxy ARP.
Disable bootp-forwarding	Turns off the BootP relay function.
Disable directed-broadcast	Disables forwarding of IP packets whose destination is a nonlocal broadcast address.

Table 55 (Page 2 of 3). IP Configuration Commands

Command	Function
Disable echo-reply	Disables the router's ICMP Echo Reply function.
Disable packet-filter	Disables specified interface-specific access control list (packet filters).
Disable per-packet-multipath	If per-packet-multipath is disabled, the router will choose the first available path to destination.
Disable RFC925-routing	Turns off RFC 925 routing.
Disable source-routing	Prevents the router from forwarding source-routed packets.
Disable UDP-forwarding	Disables UDP forwarding for packets received by the router with the specified UDP destination port number.
Enable ARP-net-routing	Turns on the router's network routing.
Enable ARP-subnet-routing	Turns on the router's ARP subnet or Proxy-ARP functionality.
Enable bootp-forwarding	Turns on BootP packet forwarding.
Enable directed broadcast	Enables forwarding of IP packets whose destination is a nonlocal broadcast address.
Enable echo-reply	Enables the building and sending of an ICMP Echo Reply in response to an ICMP Echo Request.
Enable packet-filter	Enables specified interface-specific access control list (packet filters).
Enable per-packet-multipath	If per-packet-multipath is enabled, and there are multiple equal-cost paths to a destination, the router will choose the path for forwarding each packet in a round-robin fashion.
Enable RFC925-routing	Turns on RFC 925 routing.
Enable source-routing	Allows the router to forward IP packets containing an IP source route option.
Enable UDP-forwarding	Enables UDP forwarding for packets received by the router with the specified UDP destination port number.
List all	Displays the entire IP configuration.
List access-controls	Displays the configured access control settings.
List addresses	Displays the IP interface addresses that have been assigned to the router.
List bootp	Displays whether or not BootP is enabled and the configured BootP servers.
List protocols	Displays the configured state of the IP routing protocols.
List routes	Displays the static network/subnet routes that have been configured.
List sizes	Displays the routing table size, reassembly buffer size, and the route cache size.
List packet-filter	Lists information on packet filters.
List UDP-forwarding	Displays all the configured information for the UDP forwarding function.
Move access-control	Changes the order of the access-control list.
Set access-control	Allows you to configure the router to enable or disable access-control.
Set cache-size	Configures the maximum number of entries for the IP routing cache.
Set default network-gateway	Configures a route to the default gateway.
Set internal-IP-address	Sets the internal IP address that belongs to the router as a whole.
Set reassembly-size	Configures the size of the buffers that are used for the reassembly of fragmented IP packets.
Set TTL	Specifies the time-to-live for packets originated by the router.

Table 55 (Page 3 of 3). IP Configuration Commands	
Command	Function
Set router-id	Sets the default IP address used by the router when generating various kinds of IP traffic.
Set routing table-size	Sets the size of the router's IP routing table.
Exit	Exits the IP configuration environment and returns to the CONFIG.

8.2.2 IP Configuration Steps

To configure your router as an IP router there are several required steps and several optional steps.

The required steps are:

1. Configure the general IP parameters.
2. Assign IP address(es) to the hardware interfaces.
3. Enable one or more dynamic routing protocol(s).
4. Configure the routing protocol(s).

The optional steps are:

- Add static routing information.
- Define IP filter(s).
- Set up access control.
- Set up BootP forwarding definitions.
- Enable ARP subnet routing.
- Enable RFC 925 ARP subnet routing.
- Configure SNMP.
- Configure DVMRP.

The following sections provide you with the information to perform the tasks.

8.2.2.1 Configuring General IP Parameters

Using an ASCII console, IP automatically becomes enabled whenever you assign at least one IP address to any of the router's hardware interfaces.

The following is a summary of the general IP parameters that you may configure for your IBM 2210:

- Internal IP address

You can assign an *internal IP address* to the IBM 2210. The internal address belongs to the router as a whole, and not to a particular interface. This address is always reachable as long as one interface on the router is active. This address is used by the data link switching (DLSw) feature.

When you use RIP, choose the IP address of one of the interfaces as the internal IP address of the IBM 2210. When you use OSPF, choose an address that has a different subnet from any subnets that are used in your network.

In the following example, we have assigned 9.67.46.236 as the internal IP address of our IBM 2210:

IP Config>**set internal-ip-address 9.67.46.236**

- Router ID

You can also assign a router ID to your IBM 2210. This will be the default IP address used in various kinds of IP traffic originated from the router. For example, it will be used as the IP source address in PING, TFTP or Traceroute packets. In addition, OSPF uses the router ID that you have configured for your IBM 2210.

In the following example, we have assigned 9.67.46.236 as the router ID of our IBM 2210.

To assign a router ID to your IBM 2210, use the following command:

IP Config>**set router-id 9.67.46.236**

- Routing table size

You can specify the number of entries in the IP routing table. This table contains the dynamic routing information known by your router.

Each entry in the routing table is 64 bytes, and by default, the routing table size is 768 entries.

In the following example, we have changed the number of routing table entries to 500:

IP Config>**set routing table-size 500**

Note that setting the routing table size too small will cause the dynamic routing information to be discarded. Setting the routing table too large will waste the router memory.

- Router cache size

The router uses a routing cache that contains the recently routed destinations. The router will reference the cache first before using the routing table. The minimum and default size for the router cache table is 64 entries. However, you may change the router cache size by using the following example:

IP Config>**set cache-size 100**

Each entry in the router cache table is 64 bytes.

- Broadcast address

You can specify the format that will be used by your IBM 2210 when broadcasting packets on a specific interface. In doing so, specify the style and the fill-pattern used.

The *style* parameter can be either local-wire or network.

When you specify local-wire for the style, the router will use the broadcast address of either 255.255.255.255 or 0.0.0.0. The former is used if you have specified the fill-pattern to be 1, and the latter is used with the fill-pattern of 0.

When you specify network for the style, the router will send the broadcast messages that begin with the network and the subnetwork portion of the IP address of the interface. The host portion of the broadcast messages will be either all 1s or 0s depending on the value specified for the fill-pattern parameter.

The following example allows the router to use 255.255.255.255 as the destination address of the broadcast messages on interface 9.67.46.236:

```
IP config>set broadcast-address 9.67.46.236  
Use a NETWORK or LOCAL-WIRE style address [NETWORK]? local-wire  
Fill pattern for wildcard part (0 or 1) [0]? 1  
IP config>
```

Note: When receiving messages, the IBM 2210 recognizes all forms of the IP broadcast addresses regardless of the settings of these parameters.

- Reassembly size

You can configure the size of the buffers that are used for the reassembly of the fragmented IP packets received by the router. The following example allows you to set the size of reassembly buffers to 10000 bytes:

```
IP Config>set reassembly-size 10000
```

The default is 12000 bytes.

- Default network gateway

You can configure a route as a default gateway and the cost of reaching that default gateway by using the following example:

```
IP Config>set default network-gateway 9.67.46.238 10
```

In the above example, the router 9.67.46.238 is defined as the default gateway with a cost of 10.

All the packets destined to the networks for which your IBM 2210 does not have a valid routing table entry will be forwarded to the default gateway.

- Default subnetwork gateway

In a subnetted network, you can configure a separate default gateway and the cost of reaching it for each subnet network. In the following example, we have defined 9.67.46.234 to be the default gateway for reaching subnet 9.0.0.0. The cost of reaching this router is 1.

```
IP Config>set default subnet-gateway 9.0.0.0 9.67.46.234 1
```

All the packets destined for unknown subnets of a known subnetted network are forwarded to the subnetwork's default gateway. In the example given above, all the packets for networks 9.0.0.0 to 255.0.0.0 will be sent to router 9.67.46.234.

- IP access control

Refer to 8.2.2.7, "Configuring Access Control" on page 346.

8.2.2.2 Configuring IP Address(es) for Hardware Interfaces

When using the configuration program, use the Interface panel under the IP directory; otherwise use the following commands.

To get the appropriate interface number for the hardware interface for which you wish to assign the IP address, use the following command:

```
Config>List devices
```

To assign an IP address to an interface use the following command:

```
IP Config>Add address
```

The following is an example of how to assign an IP address of 9.67.46.236 with the subnet mask of 255.255.255.240 to interface 0:

```
IP Config>Add address 0 9.67.46.236 255.255.255.240
```

Serial lines do not *need* addresses. Such lines are called unnumbered and can be configured without IP addresses, but still enable them for IP traffic using the following command:

```
IP Config>Add address 1 0.0.0.1
```

8.2.2.3 Configuring Dynamic Routing Protocols

To configure dynamic routing protocols refer to 8.3, "Configuring Dynamic Routing Using RIP" on page 348.

8.2.2.4 Configuring Static Routing Information

Using the configuration program, you can add static routing information for networks or subnetworks by using the Static/Default Subnet route panel on the IP directory. From the ASCII console, you can use the following commands:

```
IP config>add route
```

For example, to add a static route to the network 9.24.104.0 with a subnet mask of 255.255.255.0 via the gateway 9.67.46.238, you can use the following command:

```
IP config>add route 9.24.104.0 255.255.255.0 9.67.46.238 1
```

Note that in the above example, the cost of reaching the gateway is defined as 1.

8.2.2.5 Configuring Filters

You can add filters on the Filter panel of the IP directory when using the Nways MRS Configuration Program. Using the ASCII console, you can use the following command:

```
IP Config>add filter
```

Note: When you add a filter, it will take effect immediately.

For example, to filter the packets destined to subnetwork 9.67.46.32 with the subnet mask of 255.255.255.240, use the following command:

```
IP Config>add filter 9.67.46.32 255.255.255.240
```

8.2.2.6 Configuring IP Source-Routing

You can enable the IP source route option on the General subpanel of the IP panel when using the Nways MRS Configuration Program. Using the ASCII console, you can use the following command:

```
IP config>enable source-routing
```

8.2.2.7 Configuring Access Control

To configure access control, enable access control first. Using the Nways MRS Configuration Program you can enable it on the General panel of the IP directory. Using Nways MRS, use the following command:

```
IP Config>set access control on/off
```


After enabling the access control, add the access control entries to the list. To do so with the Configuration Program, use the Access Control panel on the IP directory. From the ASCII console, use the following command:

IP Config>**add access-control**

When adding entries to the access list, because of the length of the command input, you are advised to get prompted for the command input by entering only the above command by itself.

Deleting entries from the access control list is based on the entry number. To get the entry numbers, use the following command:

IP Config>**list access-controls**

8.2.2.8 Configuring BootP Forwarding

To forward BootP requests do the following:

- Enable BootP/DHCP forwarding and define the maximum number of hops that a BootP request can take. Using configuration program, use the General panel of the BootP/DHCP forwarding subdirectory. Using the ASCII console, use the following command to enable BootP forwarding:

IP Config>**Enable bootp-forwarding**

When you enter the above command with no other parameter, you will be prompted to enter the maximum number of forwarding hops and minimum seconds before forwarding.

- Define one or more BootP servers (that is, where the BootP requests are being forwarded). Using the configuration program, you can define the BootP server via the Addresses panel of the BootP/DHCP forwarding subdirectory. From the ASCII console, enter the following command:

IP Config>**Add bootp-server**

When you enter the above command with no other parameter, you will be prompted to enter the BootP server address.

8.2.2.9 Configuring ARP-Subnet Routing

To enable ARP-subnet routing, you must use the following command from the ASCII console:

IP Config>**Enable arp-subnet-routing**

Note

Configuration of ARP-subnet routing is not supported by Nways MRS Configuration Program.

8.2.2.10 Configuring RFC 925 ARP Subnet Routing

To enable RFC 925 ARP-subnet routing, use the following the ASCII console:

IP Config>**Enable RFC925-routing**

Note

Configuration of RFC 925 ARP-subnet routing is not supported by Nways MRS Configuration Program.

8.2.3 IP Monitoring

Monitoring IP is done from the IP environment at the Gateway Operator Console (GWCON). To access the commands, issue the command:

+ protocol ip

Table 56 shows the available commands. *The Nways MRS Protocol Configuration and Monitoring Reference Volume 1 Version 1 Release 1* covers these commands in detail.

Table 56. IP Monitoring Commands

Command	Function
? (Help)	Lists the IP monitoring commands or lists the actions associated with specific commands.
Access controls	Lists the current IP access control mode, together with the configured access control records.
Cache	Displays a table of all recently routed destinations.
Counters	Lists various IP statistics, including counts of routing errors and packets dropped.
Dump routing tables	Lists the content of the IP routing table.
Interface addresses	Lists the router's IP interface addresses.
Packet-filter	Displays the access-control information defined for the specified packet-filter, or all filters.
Ping	Sends ICMP Echo Requests to another host once per second and watches for a response.
Route	Lists whether a route exists for a specific IP destination, and if so, the routing table entry that corresponds to the route.
Static routes	Lists the static routes that have been configured, including the default gateway.
Traceroute	Displays the complete path (hop-by-hop) to a particular destination.
UDP-forwarding	Displays the UDP port numbers and destination IP addresses that you have added by using the add command or the enable command.
Exit	Exits the IP console environment.

Refer to 8.6, "Scenarios and Configuration Examples" on page 362 for examples.

8.3 Configuring Dynamic Routing Using RIP

To configure RIP on the IBM 2210, you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRS.

An example of how to configure the IBM 2210 by using RIP can be found in 8.6.1, "Scenario 1: Configuring IP RIP over a PPP" on page 362.

8.3.1 RIP Configuration Commands

This section summarizes the RIP configuration commands available within the CONFIG process of the Nways MRS. To access the commands from the ASCII console, issue the following command:

Config>**protocol ip**

Table 57 shows the available commands. *The Nways MRS Protocol Configuration and Monitoring Reference Volume 1 Version 1 Release 1* covers these commands in detail.

Table 57 (Page 1 of 2). RIP Configuration Commands	
Command	Function
? (Help)	Lists all the IP configuration commands, or lists the options associated with specific commands.
Add accept-rip-route	Allows an interface to accept a RIP route when input filtering is enabled for an interface.
Delete accept-rip-route	Removes a route from the list of networks that the RIP protocol always accepts.
Disable receiving rip	Prevents any RIP packets from being received on an interface.
Disable receiving dynamic nets/subnets/host	Ensures that for RIP updates received on the interface, the router accepts only nets/subnets/hosts entered by the add accept-rip-route command.
Disable rip	Turns off the RIP protocol.
Disable sending default/net/subnet/static	Prevents the router from advertising a default route, net-routes, subnet-routes or static routes in RIP updates on an interface.
Enable override default	Enables received RIP information to override the router's default gateway.
Enable override static-routes	Enables received RIP information to override some of the router's statically configured routing information.
Enable receiving rip	Enables receiving RIP updates on an interface.
Enable receiving dynamic host	Modifies the processing of RIP updates that are received on a particular interface.
Enable receiving dynamic nets	Disables input filtering on a network level.
Enable receiving dynamic subnets	Disables input filtering on a subnet level.
Enable rip	Enables the router's RIP protocol processing.
Enable sending default-routes	Enables sending the default route (if one exists) in RIP updates on an interface.
Enable sending net-routes	Enables sending network level routes in RIP updates on an interface.
Enable sending subnet-routes	Enables sending subnet level routes in RIP updates on an interface.
Enable sending static-routes	Enables sending statically configured routes in RIP updates on an interface.
List protocols	Displays the configured state of the IP routing protocols (including RIP).
List rip-routes-accept	Displays the set of routes that the RIP routing protocol always accepts
List tags	Displays the per-interface tags that will be associated with received RIP information.
Set broadcast-address	Specifies the IP broadcast format that the router uses when broadcasting packets on a particular interface (for example, RIP updates).

Table 57 (Page 2 of 2). RIP Configuration Commands	
Command	Function
Set originate-rip-default	Allows RIP to advertise the router as a default.
Set tag	Configures the per-interface tags associated with received RIP information.
Exit	Exits the IP configuration environment and returns to the CONFIG.

When using the Configuration Program, use the panels listed under the RIP subdirectory entry.

8.3.2 RIP Configuration Steps

The following section provides you with the information on how to perform the various tasks required for configuring RIP on the IBM 2210:

1. Enable RIP

You must first enable RIP on the box level to allow the router to send and receive RIP updates on its interfaces. When using the configuration program, you can use the General panel under the RIP route acceptance subdirectory to perform this task. From the ASCII console, issue the following command:

```
IP Config>enable rip
```

Enabling RIP results in sending and receiving of RIP updates to be enabled on all interfaces.

2. RIP Route Acceptance

You may define the nets or subnets for which your router will accept RIP updates. When using the Configuration Program, you can use the RIP Route Acceptance panel under the RIP subdirectory to perform this task. From the ASCII console, use the following command:

```
IP Config>add accept-rip-route
```

Note: The route acceptance is used in combination with RIP flags receive dynamic nets/subnets which are specified for each interface.

3. Originate RIP Default Panel

Allows you to define when the router advertises itself as the default router.

Note: This is used in combination with the RIP flag send default route, which can be specified for each interface. When using the Configuration Program, you can use the Originate RIP Default panel under the RIP subdirectory to perform this task. From the ASCII console, use the following command:

```
IP Config>set originate-rip-default
```

4. Enable/Disable RIP flags on each interface

When using the Configuration Program, the RIP Interface panel under the RIP subdirectory allows you to perform two tasks:

- a. Specify the broadcast format and the tag used in sending out the RIP updates.

The RIP broadcast format allows you to specify the style (network or local-wire) and the fill-pattern (all 0s or all 1s) used in the destination IP address of the RIP updates sent out by the router.

Tags can be used to group routes together for later advertisement via EGP where a tag will be treated as if it were a router's source AS.

b. Define the RIP flags used at each interface

The flags that can be set for each interface are:

- *Send Net Routes*

This parameter allows you to specify if all network-level routes should be included in the RIP updates sent on the selected interface.

- *Send Subnet Routes*

This parameter allows you to specify if all subnet routes should be included in the RIP updates sent on the selected interface.

- *Send Static Routes*

This parameter allows you to specify if statically configured routes and directly connected routes should be included in the RIP updates sent on the selected interface.

- *Send Default Routes*

This parameter allows you to specify if the default route should be included in the RIP updates sent out on the selected interface.

- *Receive RIP*

This parameter allows you to specify if the RIP updates received on this interface should be accepted.

- *Receive Dynamic Nets*

This parameter allows you to specify if the network-level RIP updates received on this interface should be accepted.

- *Receive Dynamic Subnets*

This parameter allows you to specify if the subnetwork-level RIP updates received on this interface should be accepted.

- *Override Default*

This parameter allows you to specify if the received RIP information may be used to override the default gateway.

- *Override Static Routes*

This parameter allows you to specify if the received RIP information may be used to override the router's statically configured routes.

Using the ASCII console, use the following commands to perform the above tasks:

- Use the following command to define the format of the broadcast address used in the RIP updates sent out by your router:

```
IP Config>set broadcast-address
```

- Use the following command to define the tag used for re-advertising the routes from each interface via EGP:

```
IP Config>set tag
```

- Use the following commands to define the RIP flags for each interface:

```

IP Config>enable/disable sending net-routes
IP Config>enable/disable sending all-routes
IP Config>enable/disable sending subnet-routes
IP Config>enable/disable sending static-routes
IP Config>enable/disable sending host-routes
IP Config>enable/disable sending default-routes
IP Config>enable/disable sending poisoned-reverse-routes
IP Config>enable/disable receiving rip
IP Config>enable/disable receiving all
IP Config>enable/disable receiving dynamic nets
IP Config>enable/disable receiving dynamic subnets
IP Config>enable/disable receiving dynamic hosts
IP Config>enable/disable override default
IP Config>enable/disable override static-routes

```

For an example of how to configure an IBM 2210 for RIP, please refer to 8.1.3.1, "RIP Interoperability with IBM 6611 Network Processor" on page 332.

8.3.3 RIP Monitoring

Monitoring RIP is done from the IP environment at the Gateway Operator Console GWCON. To access these commands, issue the following command:

+ protocol ip

Table 58 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference* covers these commands in detail.

Table 58. RIP Monitoring Commands	
Command	Function
? (Help)	Lists the IP monitoring commands or lists the actions associated with specific commands.
Cache	Displays a table of all recently routed destinations.
Counters	Lists various IP statistics, including counts of routing errors and packets dropped.
Dump routing tables	Lists the content of the IP routing table.
Route	Lists whether a route exists for a specific IP destination, and if so, the routing table entry that corresponds to the route.
Traceroute	Displays the complete path (hop-by-hop) to a particular destination.

Refer to 8.6.1, "Scenario 1: Configuring IP RIP over a PPP" on page 362 for an example.

8.4 Configuring Dynamic Routing Using OSPF

To configure OSPF on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRS.

8.4.1 OSPF Configuration Commands

This section summarizes the OSPF configuration commands available within the CONFIG process of the Nways MRS. To access the commands, issue the following command:

Config>**protocol ospf**

Table 59 on page 353 shows the available commands. *The Nways MRS Protocol Configuration and Monitoring Reference* covers these commands in detail.

Table 59. OSPF Configuration Commands	
Command	Function
? (Help)	Lists all the OSPF configuration commands, or lists the options associated with specific commands.
Add	Adds to already existent OSPF information. You can add ranges to areas, and neighbors to non-broadcast networks.
Delete	Deletes OSPF information from SRAM.
Disable	Disables the entire OSPF protocol, AS boundary routing capability, or IP multicast routing.
Enable	Enables the entire OSPF protocol, AS boundary routing capability, or IP multicast routing.
Join	Configures the router to belong to one or more multicast groups.
Leave	Removes the router from membership in multicast groups.
List	Displays the OSPF configuration.
Set	Establishes or changes the configuration information concerning OSPF areas, interfaces, non-broadcast networks, or virtual links. It also allows you to set the way in which OSPF routes are compared to information gained from other routing protocols.
Exit	Exits the OSPF configuration environment and returns to the CONFIG environment.

When using the configuration program use the panels listed under the OSPF subdirectory entry.

8.4.2 OSPF Configuration Steps

Take the following steps to configure OSPF:

1. General Parameters

Enable the IBM 2210 to use OSPF protocol. You must also provide an estimate of the number of external routes and the number of OSPF routers in your OSPF routing domain.

You can perform this step by using the General panel of the OSPF subdirectory of the Configuration program. From the ASCII console, you can use the following command:

```
OSPF Config>enable ospf
```

When using the Configuration Program, you can also enable *per-packet-multicast* on the OSPF General panel.

2. Area Configuration

Define OSPF areas to the IBM 2210 along with the authentication level and address ranges to the areas. If no areas have been defined, a single backbone area is assumed.

When using the Configuration Program, the area and its associated parameters can be defined by using the Area Configuration panel of the OSPF subdirectory. From the ASCII console, you can use the following commands:

```
OSPF Config>add range
```

3. Virtual Links

Define virtual links to interconnect to the backbone area the routers which share a common non-backbone and non-stub area.

When using the Configuration Program, the virtual links can be defined by using the Area Configuration panel of the OSPF subdirectory. From the ASCII console, you can use the following command:

```
OSPF Config>set virtual-link
```

4. IP Multicast Parameters.

You may configure the IBM 2210 to route the IP multicast (class D) datagrams on the OSPF interfaces. To do so, enable your IBM 2210 for multicast routing.

When enabling multicast routing, you need to specify whether you want the router to forward multicast datagrams between OSPF areas as well as whether you want the router to forward multicast datagrams between autonomous systems.

When using the Configuration Program, you can enable the router for multicast routing using the Multicast forwarding panel of the OSPF subdirectory. From the ASCII console, you can use the following command:

```
OSPF Config>enable multicast forwarding
```

When using multicast routing, also specify the multicast capabilities for each OSPF-interface as discussed in the Interfaces section below.

If you have already defined interfaces to OSPF and enabled the multicast routing afterwards, the multicast-forwarding will be enabled automatically on all the OSPF interfaces. If you enable this capability before you define the OSPF interfaces, you will be prompted for it when defining the interface.

5. Interfaces

Define the routers OSPF network interfaces with costs and the OSPF operating parameters and multicast parameters. The following parameters must have the same value for all routers in same network:

- Hello interval
- Dead router interval
- Authentication key (if an authentication of 1 is used)

When using the Configuration Program, you can define the OSPF interface by using the Interface panel of OSPF subdirectory. From the ASCII console, you can use the following command:

```
OSPF Config>set interface
```

Note that the non-broadcast settings must be configured if the router is connected to a non-broadcast multi-access networks such as X.25 or frame relay or when your neighbor router is booting over one of your PPP connections. For additional information about OSPF and non-broadcast networks, refer to 8.1.4.1, "OSPF and Non-Broadcast Networks" on page 333.

When using the Configuration Program, the non-broadcast settings are configured using the Interfaces panel of the OSPF subdirectory. From the ASCII console, you can use the following commands:

```
OSPF Config>set non-broadcast
```

```
OSPF Config>add neighbor
```


6. AS Boundary Routing

If you want the router to import learned routes from the other protocols such as BGP, RIP, static routes, etc., enable AS-boundary routing. Also, if you want the router to originate default routes, enable this option.

Using the Configuration Program, you can enable AS-boundary routing as well as specifying the routes that are to be imported by using the AS Boundary Routing panel of the OSPF subdirectory. This panel also allows you to specify if the router can originate default routes via OSPF interface if the BGP routes are available.

Note: The Configuration Program does provide you with the option to always originate default route.

When you enabling AS boundary routing from the ASCII console, use the following command:

OSPF Config>**enable as boundary routing**

When using this command, you will be prompted to specify if you want to import routes learned from other routing protocols, as well as if you want the router to originate default routes (or default routes if BGP routes are available). The following is the list of the prompts that will be displayed on the ASCII console:

```
Import BGP routes?
Import RIP routes?
Import static routes?
Import direct routes?
Import subnet routes?
Always originate default route?
Originate as type 1 or 2?
Default route cost?
Default forwarding cost?
```

When you specify that the router should originate default routes (or default routes if EGP routes are available) you also need to specify the forwarding address as well as the type (1 or 2) and the path cost. The forwarding address is the IP address that the other OSPF routers will use as their default OSPF router.

Refer to 8.6.3, "Scenario 3: Configuring OSPF with 6611 Interoperability over a PPP" on page 381 for an example on how to configure OSPF.

8.4.3 OSPF Monitoring

Monitoring OSPF is done from the OSPF environment at the Gateway Operator Console GWCON. To access the monitoring commands, issue the following command:

+ **protocol ospf**

Table 60 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference Volume 1 Version 1 Release 1* covers these commands in detail.

Table 60 (Page 1 of 2). OSPF Monitoring Commands	
Command	Function
? (Help)	Lists the OSPF monitoring commands or lists the options associated with specific commands.

Table 60 (Page 2 of 2). OSPF Monitoring Commands

Command	Function
Advertisement	Displays a link state advertisement belonging to the OSPF database.
Area Summary	Displays OSPF area statistics and parameters.
AS external	Lists the AS external advertisements belonging to the OSPF link state database.
Database summary	Displays the advertisements belonging to an OSPF area's link state database.
Dump routing tables	Displays the OSPF routes contained in the routing table.
Interface summary	Displays OSPF interface statistics and parameters.
Join	Configures the router to belong to one or more multicast groups.
Leave	Removes the router from membership in multicast groups.
Mcache	Displays a list of currently active multicast forwarding cache entries.
Mgroups	Displays the group membership of the router's attached interfaces.
Mstats	Displays various multicast routing statistics.
Neighbor summary	Displays OSPF neighbor statistics and parameters.
Ping	Sends ICMP Echo Requests to another host once per second and watches for a response.
Routers	Displays the reachable OSPF area-border routers and AS-boundary routers.
Size	Displays the number of LSAs currently in the link state database, categorized by type.
Traceroute	Displays the complete path (hop-by-hop) to a particular destination.
Statistics	Displays OSPF statistics detailing memory and network usage.
Weight	Dynamically changes the cost of an OSPF interface.
Exit	Exits the OSPF configuration environment and returns to the CONFIG environment.

Note

The OSPF console allows you to make certain dynamic changes in your OSPF environment without the need to restart or reload the router. The following commands take immediate effect on the OSPF environment:

- Join
- Leave
- Weight

For an example refer to 8.6.3, "Scenario 3: Configuring OSPF with 6611 Interoperability over a PPP" on page 381.

8.5 Configuring BGP4

To configure BGP on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRS.

8.5.1 BGP Configuration Commands

This section summarizes the BGP configuration commands available from the CONFIG process of the Nways MRS. To access the commands, issue the following command:

```
Config>protocol bgp
```

Table 61 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference* covers these commands in detail.

Table 61. BGP4 Configuration Commands	
Command	Function
? (Help)	Lists the configuration commands, or lists the actions associated with specific commands.
Add	ADD BGP neighbors.
Change	Modifies information that was originally entered with the add command.
Delete	Deletes BGP configuration information that had been entered with the add command.
Disable	Disables certain BGP features that have been turned on by the enable command.
Enable	Enables BGP speakers or BGP neighbors.
List	Displays BGP configuration items.
move	Changes the order in which policies and aggregates are defined.
Exit	Exits the process.

8.5.2 BGP4 Configuration Steps

To configure BGP4, you can use the BGP4 CONFIG environment of the ASCII console or the panels listed under the BEG4 Subdirectory of the Configuration Program.

The following steps are required to configure BGP4 on the IBM 2210:

1. Enabling BGP

Enabling BGP requires you to specify the BGP router's unique AS number. AS numbers are assigned by Stanford Research Institute Network Information Center. To do so when using the Configuration Program, use the General panel of the BGP4 subdirectory. From the ASCII console, use the following command:

```
BGP Config>enable bgp speaker
```

2. Defining BGP Neighbors

BGP Neighbors are BGP routers with a BGP speaker that establishes a TCP connection. Once neighbors are defined, connections to them are established by default.

BGP neighbors can be internal or external. Internal neighbors exist in the same AS and do not need to have a direct connection to one another. External neighbors exist in different autonomous systems. These must have a direct connection to one another.

To define BGP neighbors, you can use the Configuration Program Neighbors panel of the BGP subdirectory. From the ASCII console, use the following command:

BGp Config>**add neighbor 192.0.190.170**

3. Adding Policies

The policies that you establish determine which routes will be imported and exported by the BGP speaker. You can set up policies for different purposes.

IBM's BGP implementation supports three policy commands:

- *Originate Policy.* This enables you to select the interior gateway protocol(IGP) networks to export.
- *Receive Policy.* This enables you to select the route information to import from BGP peers.
- *Send Policy.* This enables you to select the route information to export to peers. Note that exportable route information can include information collected from neighboring autonomous systems, as well as the routes that originate in the IGP.

To set specific policies for a BGP speaker, when using the Configuration Program, use the Receive/send/originate policies subpanel of BGP4 panel. From the ASCII console, you can use following commands:

bgp Config>**add originate-policy inclusive**

bgp Config>**add originate-policy exclusive**

bgp Config>**add receive-policy inclusive**

bgp Config>**add receive-policy exclusive**

bgp Config>**add no-receive**

bgp Config>**add send-policy inclusive**

bgp Config>**add send-policy exclusive**

8.5.3 BGP4 Monitoring

Monitoring BGP4 is done from the IP environment at the Gateway Operator Console GWCON. To access the monitoring commands, issue the following command:

+ protocol BGP

Table 62 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference Volume 2 Version 1 Release 1* covers these commands in detail.

Table 62 (Page 1 of 2). BGP Monitoring Commands	
Command	Function
? (Help)	Lists the monitoring commands or lists the actions associated with specific commands.
Destinations	Displays all entries in the BGP routing table.
Dump routing tables	Lists the content of the IP routing table.
Neighbors	Displays the current active neighbors.
Paths	Displays all available paths in the database.
Ping	Sends ICMP Echo Requests to another host once per second and watches for a response.
Traceroute	Displays the complete path (hop-by-hop) to a particular destination.

Table 62 (Page 2 of 2). BGP Monitoring Commands	
Command	Function
Exit	Exits the monitoring environment and returns to the GWCON console.

8.5.4 Configuring SNMP

This section describes how to configure the SNMP agent in the IBM 2210.

To configure an SNMP agent on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRS.

There is no SNMP configuration or monitoring scenario included in this book.

8.5.4.1 SNMP Configuration Commands

This section summarizes the SNMP configuration commands available within the CONFIG process of the Nways MRS. To access the commands, issue the following command from the ASCII console:

```
Config>protocol snmp
```

Table 63 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference Volume 1 Version 1 Release 1* covers these commands in detail.

Table 63. SNMP Configuration Commands	
Command	Function
? (Help)	Lists all the SNMP configuration commands, or lists the options associated with specific commands.
Add	Adds a community to the list of SNMP communities, an IP address with mask to a community, or a subtree to a MIB view.
Delete	Removes a community from the list of SNMP communities, an IP address with mask from a community, or a subtree from a MIB view.
Disable	Disables SNMP protocol and standard traps associated with named communities.
Enable	Enables SNMP protocol and standard traps associated with named communities.
List	Displays the current communities with their associated access modes, enabled traps, IP addresses, and views. Also displays all views and their associated MIB subtrees.
Set	Sets a community's access mode or view, and sets the UDP trap port.
Exit	Exits the SNMP configuration environment and returns to the CONFIG.

Using the Configuration Program, you can configure the SNMP agent in the IBM 2210 by using the panels provided under the SNMP subdirectory of the System directory.

8.5.5 SNMP Configuration Steps

The following steps are required to configure SNMP agent in the IBM 2210:

- Enable SNMP

Use the General panel of the SNMP CONFIG subdirectory of the Configuration Program to enable SNMP. This panel also allows you to change the port number to which the traps are sent.

Using the ASCII console, you can issue the following command:

```
SNMP Config>enable snmp
```

```
SNMP Config>set trap_port
```

- Create views with their associated MIB object IDs

Using the Configuration Program, you can use the Subtree panel under the SNMP CONFIG subdirectory to create views and associate them with the MIB object IDs.

Using the ASCII console, you can use the following command:

```
SNMP Config>add sub_tree
```

- Specify community names

Using the Configuration Program, you can use the Communities panel of the SNMP CONFIG subdirectory to assign community names along with their associated IP addresses, access type, and trap flags. Additionally you can assign a view name to a community.

Using the ASCII console, you can use the following commands to:

- Add a community name:

```
SNMP Config>add community
```

- Specify the SNMP manager's IP address:

```
SNMP Config>add address
```

- Assign an access type to a community:

```
SNMP Config>set community access
```

Enable a community to receive traps:

```
SNMP Config>enable trap
```

- Assign one or all views to a community:

```
SNMP Config>set community view
```

8.5.6 Monitoring SNMP

Monitoring SNMP is done from the SNMP environment at the Gateway Operator Console GWCON. To access the commands, issue the following command:

```
+ protocol snmp
```

Table 64 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference Volume 1 Version 1 Release 1* covers these commands in detail.

Note

You cannot view the MIB from the ASCII console.

Table 64 (Page 1 of 2). SNMP Monitoring Commands

Command	Function
? (Help)	Lists the SNMP monitoring commands or lists the options associated with specific commands.
Add	Adds a community to the list of SNMP communities, an IP address with mask to a community, or a subtree to a MIB view.

Table 64 (Page 2 of 2). SNMP Monitoring Commands	
Command	Function
Delete	Removes a community from the list of SNMP communities, an IP address with mask from a community, or a subtree from a MIB view.
Enable/Disable	Enables/disables SNMP protocol and traps associated with named communities.
List	Displays the current configuration of SNMP communities, authentication types, access modes, traps, and network addresses. Also displays the current configuration of views.
Revert	Erases the specified changes and restores the settings to the values in the permanent SNMP configuration.
Save	Takes the specified changes and saves them permanently in the SNMP configuration.
Set	Sets a community's access mode or view.
Statistics	Displays the statistics about the number of variables and the size of the MIB.
Exit	Exits the SNMP monitoring environment and returns to the GWCON environment.

8.5.7 Configuring DVMRP

To configure DVMRP on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of the Nways MRS.

There is no DVMRP configuration or monitoring scenario included in this book.

8.5.7.1 DVMRP Configuration Commands

This section summarizes the DVMRP configuration commands available from the CONFIG process of the Nways MRS. To access these commands issue the following command:

Config>**protocol dvmrp**

Table 65 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference volume 2 Version 1 Release 1* covers these commands in detail.

Table 65. DVMRP Configuration Commands	
Command	Function
? (Help)	Lists all the DVMRP configuration commands, or lists the options associated with specific commands.
DVMRP	Enables or disables DVMRP.
MOSPF	Sets the metric and threshold for the DVMRP interface running over MOSPF. This command also disables the MOSPF VIF.
Phyint	Sets the metric and threshold for LAN interfaces associated with DVMRP.
Tunnel	Adds or deletes tunnels in a MOSPF/DVMRP configuration.
List	Displays the current DVMRP configuration.
Exit	Exits the DVMRP configuration environment and returns to the CONFIG.

When using the Configuration Program, use the DVMRP subdirectory.

8.5.8 Monitoring DVMRP

Monitoring DVMRP is done from the DVMRP environment at the Gateway Operator Console GWCON. To access the commands, issue the following command:

+ protocol dvmrp

Table 66 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference Volume 2 Version 1 Release 1* covers these commands in detail.

Table 66. DVMRP Monitoring Commands	
Command	Function
? (Help)	Lists the DVMRP monitoring commands or lists the options associated with specific commands.
Dump routing tables	Displays the OSPF routes contained in the routing table.
Interface summary	Displays OSPF interface statistics and parameters.
Join	Configures the router to belong to one or more multicast groups.
Leave	Removes the router from membership in multicast groups.
Mcache	Displays a list of currently active multicast forwarding cache entries.
Mgroups	Displays the group membership of the router's attached interfaces.
Mstats	Displays various multicast routing statistics.
Exit	Exits the DVMRP monitoring environment and returns to the GWCON environment.

8.6 Scenarios and Configuration Examples

This section provides scenarios and configuration examples on IP and IP routing protocols.

The samples include a description of the goals of the scenario, a configuration drawing and listings of the configuration using the ASCII console as well as using the MRS Configuration Program.

This section includes the following scenarios:

1. Scenario 1: IP RIP over a PPP
2. Scenario 2: IP RIP over a PPP (ISDN)
3. Scenario 3: OSPF Single Area with 6611 Interoperability over a PPP
4. OSPF Single Area over Frame Relay (see 10.6.2, "Scenario 2: DLSw between Two 2210s and 6611 over Frame Relay" on page 484).

8.6.1 Scenario 1: Configuring IP RIP over a PPP

In this scenario two 2210s are connected via an RS-232 PPP link. One of the 2210s (2210A) has a token-ring LAN interface and the other (2210B) has an Ethernet LAN interface. Attached to the Ethernet LAN is a PS/2 running TCP/IP for OS/2 with the RouteD daemon. Refer to Figure 113 on page 363 for the configuration.

This scenario shows you how to configure RIP on a 2210, how you can set RIP flags and how to define a RIP input filter. In this scenario the RIP updates for subnet 9.67.46.16 will always be accepted at the 2210B router. All other subnets received on the Ethernet interface of 2210B will be discarded.

Refer to Figure 114 on page 364 for the ASCII console commands used to configure 2210B, which also shows you an example of the monitoring functions of RIP. Figure 115 on page 368 shows the configuration of 2210B using the MRS Configuration Program.

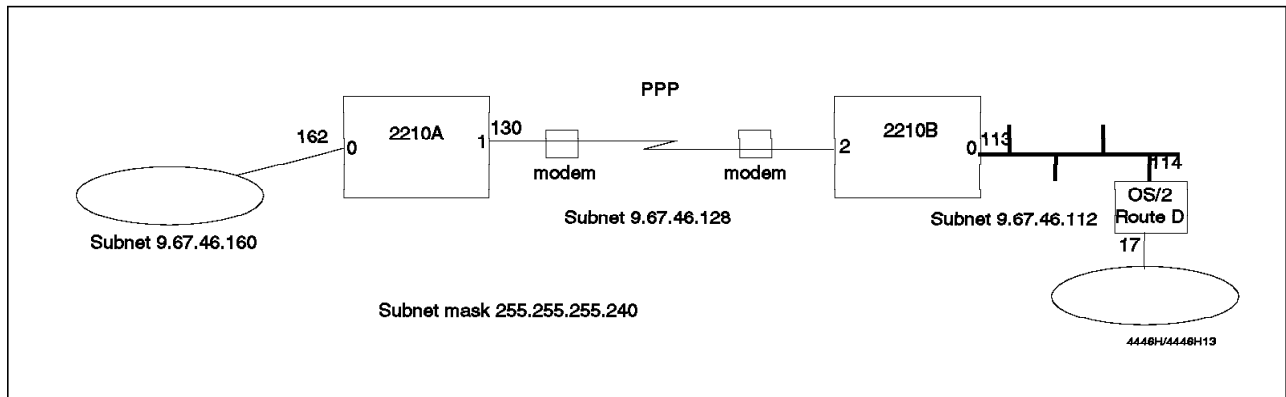


Figure 113. Scenario 1: IP RIP Configuration with IBM 2210s

```

*
*talk 6      1

Config>disable interface 1      2
Config>list device      3
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
      (Disabled)
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>network 0      4
Ethernet interface configuration
ETH config>list      5
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit      6
Config>net 2      7
Point-to-Point user configuration
PPP Config>list hdlc      8

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>set hdlc cable rs-232 dte
PPP Config>exit
Config>protocol ip      9
Internet protocol user configuration
IP config>add address
Which net is this address for [0]? 0
New address [0.0.0.0]? 9.67.46.113
Address mask [255.0.0.0]? 255.255.255.240
IP config>add address
Which net is this address for [0]? 2
New address [0.0.0.0]? 9.67.46.131
Address mask [255.0.0.0]? 255.255.255.240
IP config>list protocol      10
BootP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled
IP config>enable rip      11

:

```

Figure 114 (Part 1 of 4). Scenario 1: Configuring 2210B via an ASCII Console

```

:
IP config>list protocol
BootP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0   9.67.46.113      Send net and subnet routes      12
    intf 1                      IP & RIP are disabled on this interface
    intf 2   9.67.46.131      Send net and subnet routes

Accept RIP updates always for:
[NONE]

IP config>disable receiving dynamic subnets 9.67.46.113 13
IP config>add accept-rip-route 9.67.46.16 14
IP config>list protocol
BootP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0   9.67.46.113      Send net and subnet routes
                                Receive No Dynamic subnet routes
    intf 1                      IP & RIP are disabled on this interface
    intf 2   9.67.46.131      Send net and subnet routes

Accept RIP updates always for:
  9.67.46.16

EGP: disabled
:

```

Figure 114 (Part 2 of 4). Scenario 1: Configuring 2210B via an ASCII Console

```

:
IP config>list addresses
IP addresses for each interface:
  intf 0  9.67.46.113      255.255.255.240  Network broadcast,    fill 0
  intf 1                                IP disabled on this interface
  intf 2  9.67.46.131      255.255.255.240  Network broadcast,    fill 0
IP config>list rip-routes-accept
Accept RIP updates always for:
  9.67.46.16
IP config>ctrl+p
*restart
Are you sure you want to restart the gateway? (Yes or [No]):y

```

Copyright Notices:
 Copyright 1985-1994 Proteon, Inc.
 Copyright 1984-1987, 1989 by J. Noel Chiappa
 Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*t 5

CGW Operator Console

+protocol ip

IP>dump

Type	Dest net	Mask	Cost	Age	Next hop(s)
Sbnt	9.0.0.0	FF000000	1	0	None
RIP %	9.67.46.16	FFFFFFF0	2	30	9.67.46.114
Dir*	9.67.46.112	FFFFFFF0	1	0	Eth/0
Dir*	9.67.46.128	FFFFFFF0	1	0	PPP/1
RIP	9.67.46.160	FFFFFFF0	2	0	9.67.46.130

15

Routing table size: 768 nets (49152 bytes), 5 nets known

IP>interface

Interface	IP Address(es)	Mask(s)
Eth/0	9.67.46.113	255.255.255.240
PPP/1	9.67.46.131	255.255.255.240

:

Figure 114 (Part 3 of 4). Scenario 1: Configuring 2210B via an ASCII Console

```
:
IP>route 9.67.46.19

Destination: 9.67.46.16
Mask: 255.255.255.240
Route type: RIP
Distance: 2
Age: 0
Tag: 0
Next hop(s): 9.67.46.114 (Eth/0)
```

Figure 114 (Part 4 of 4). Scenario 1: Configuring 2210B via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** In this configuration serial interface 1 will not be used.
- 3** List the interface on this router.
- 4** Start customization of the Ethernet interface.
- 5** The defaults can be used for this scenario. Ensure that the other stations on the Ethernet LAN use the same IP-encapsulation as your IBM 2210.
- 6** Exit from the Ethernet configuration.
- 7** Start customization of serial interface 2.
- 8** An RS-232 null modem is used.
- 9** Start customization of the IP environment and assign IP addresses and subnet masks to the interfaces.
- 10** By default none of the routing protocols is enabled.
- 11** Enable RIP on all interfaces.
- 12** The protocol list shows the current RIP flags per interface. To enable RIP this is all you need to do. However, we want to configure filters as shown in the next steps.
- 13** In this scenario, an input filter is defined to disable receiving RIP updates from all the subnets.
- 14** Allows the RIP updates for 9.67.46.16 subnet to always be accepted. The protocol listing shows the settings defined.
- 15** After the restart, go to monitor and notice that 9.67.46.16 is in the route table with a % sign. This indicates that the RIP updates will always be received for this subnetwork.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 126** **2**
 Select CONFIGURE of interface 0
 ENABLE INTERFACE
 Select CONNECTOR TYPE
 Select **AUTO-CONFIG**
 Select IP ENCAPSULATION
 Select ETHERNET

Select CONFIGURE of serial interface 1 **3**
 On the GENERAL subpanel:
DISABLE INTERFACE

Select CONFIGURE of serial interface 2 **4**
 On the GENERAL subpanel
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select RS-232 DTE
 Select subpanel LCP
 RETRY TIMER = 3000
 CONFIG TRIES = 20
 NAK TRIES = 10
 TERMINATE TRIES = 10
 MAXIMUM RECEIVE UNIT = 2048

:

Figure 115 (Part 1 of 3). Scenario 9: Configuring 2210B Using Nways MRS

```

:
    Select subpanel BNCP
        ENABLE MAGIC NUMBER
        DISABLE TINYGRAM COMPRESSION
    Select subpanel IPCP
        DISABLE IP COMPRESSION
        NUMBER OF SLOTS = 16
        DISABLE SEND IP ADDRESS
        DISABLE REQUEST IP ADDRESS

On the 2210 Navigation Window:
Select GENERAL on the IP directory

On the IP GENERAL Window:
    ENABLE IP 5
    DISABLE ACCESS CONTROL
    ENABLE DIRECTED-BROADCAST
    INTERNAL ADDRESS blank
    ROUTING TABLE SIZE = 768
    CACHE SIZE = 64
    ROUTER ID blank

On the 2210 Navigation Window:
Select INTERFACES on the IP directory

On the IP INTERFACES Window:
    Select IP ADDRESSES for interface 0 6
        IP ADDRESS = 9.67.46.113
        SUBNET MASK = 255.255.255.240
        Select ADD
    Select IP ADDRESSES for interface 2
        IP ADDRESS = 9.67.46.131
        SUBNET MASK = 255.255.255.240
        select ADD

On the 2210 Navigation Window:
Select GENERAL on the RIP directory

On the RIP GENERAL Window:
    ENABLE RIP 7

On the 2210 Navigation Window:
Select RIP ROUTE ACCEPTANCE on the RIP directory

On the RIP ROUTE ACCEPTANCE window:
    NETWORK ADDRESS = 9.67.46.26 8
    Select ADD

On the 2210 Navigation Window:
Select INTERFACES on the RIP directory

:

```

Figure 115 (Part 2 of 3). Scenario 9: Configuring 2210B Using Nways MRS

```

:
On the RIP INTERFACES Window: 9
  Select CONFIGURE of interface 0
    On the GENERAL subpanel
      Select BROADCAST ADDRESS STYLE
      Select NETWORK
      Select ADDRESS FILL PATTERN
      Select ZEROES
      INTERFACE TAG (AS NUMBER) = 0
    On the FLAGS subpanel
      ENABLE SEND NET ROUTES
      ENABLE SEND SUBNET ROUTES
      DISABLE SEND STATIC ROUTES
      DISABLE SEND DEFAULT ROUTES
      ENABLE RECEIVE RIP
      ENABLE RECEIVE DYNAMIC NETS
      DISABLE RECEIVE DYNAMIC SUBNETS
      DISABLE OVERRIDE DEFAULT
      DISABLE OVERRIDE STATIC ROUTES

On the 2210 Navigation Window:
  Select CONFIGURE from the menu bar
  Select CREATE ROUTER CONFIGURATION 10

  On the FILE NAME FOR CONFIGURATION DATA, PLEASE? Window:
    enter <config.nme>
    Select OK

```

Figure 115 (Part 3 of 3). Scenario 9: Configuring 2210B Using Nways MRS

Notes:

- 1** Start creating a new configuration.
- 2** Configure Model 126. Use AUTO-CONFIG for the Ethernet interface.
- 3** Disable the interfaces that are not used in this scenario.
- 4** For serial interface 2 the defaults are good.
- 5** Enable IP.
- 6** Assign IP addresses to the corresponding interfaces.
- 7** Enable RIP on all interfaces.
- 8** Allow RIP updates to be received for subnet 9.67.46.16.
- 9** Disable reception of any other subnet on the Ethernet interface.
- 10** Create a configuration file.

8.6.2 Scenario 2: Configuring IP RIP over a PPP (ISDN)

In this scenario two 2210s are connected via an ISDN PPP link. One of the 2210s (2210a) has a token-ring LAN interface and the other (2210b) has an Ethernet LAN interface. Attached to the token-ring interface is a workstation running TCP/IP for OS/2.

The aim of Scenario 2 is to simply be able to PING the Ethernet interface of the 2210b router from the OS/2 workstation connected to the token-ring LAN. Refer to Figure 116 for the configuration. Testing the ISDN configuration of each 2210 will be completed in this process.

Note: For this scenario the ISDN switch used was INS64-compatible, and only required four digits as a dial address for connection to be made. Also, we are considering that we are keeping the ISDN connection always up which is not the case when there is a charge for the time the connection is up. In this situation, we strongly recommend you not to use RIP. Use static routes and dial-on-demand feature that will allow you to connect only when there are useful packages to be sent.

Refer to Figure 117 on page 372 for the ASCII console commands used to configure the 2210a.

Figure 118 on page 379 shows the MRS Configuration program for the 2210a configuration.

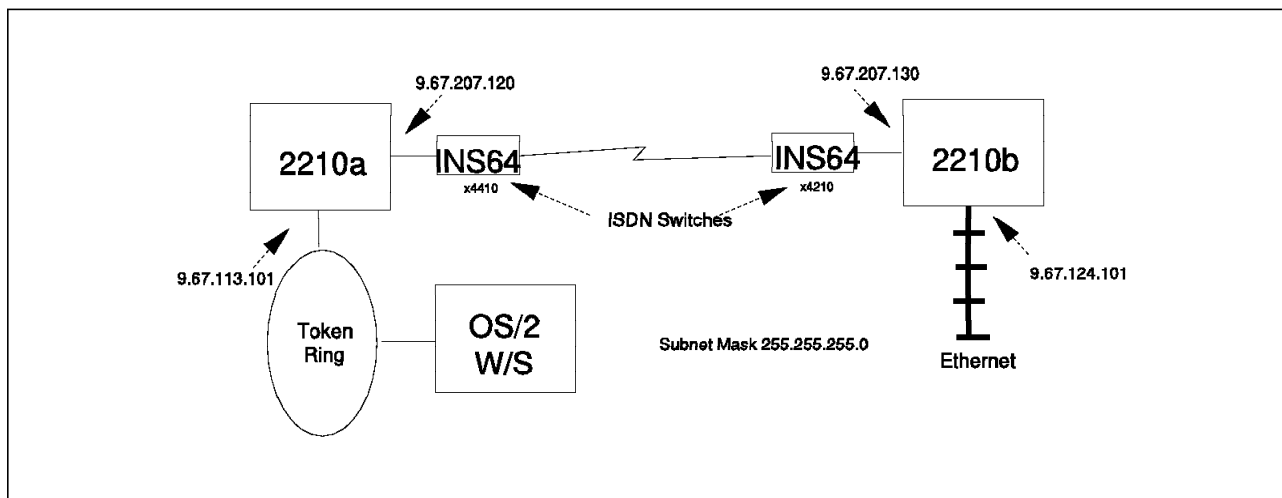


Figure 116. Scenario 2: IP RIP Configuration over ISDN (PPP)

```

*
*talk 6      1

Config>network 0      2
Token-Ring interface configuration

TKR config>speed
Speed (4 or 16) [4]? 16
TKR config>media shielded
TKR config>exit

Config>add isdn-address      3
Assign address name [1-23] chars []? 2210a
Assign network dial address [1-15] digits []? 4410
Assign network subdial address [0-20] digits []?

Config>add isdn-address      4
Assign address name [1-23] chars []? 2210b
Assign network dial address [1-15] digits []? 4210
Assign network subdial address [0-20] digits []?

Config>list devices      5
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
      (Disabled)
Ifc 2 (WAN SDLC): CSR 81640, CSR2 80E00, vector 92
      (Disabled)
Ifc 3 (ISDN): CSR      0, vector 0

Config>network 3      6
ISDN user configuration
ISDN Config>set switch ins64
ISDN Config>set local-address-name
Assign local address name []? 2210a
ISDN Config>set dn0
Enter DNO (Directory-Number-0) []? 4410
ISDN Config>set tei
TEI [AUTO]?

ISDN Config>set framesize
Framesize in bytes (1024/2048/4096) [4096]? 2048

ISDN Config>list all      7

                                ISDN Configuration

Local Network Address Name      = 2210a
Local Network Address           = 4410
Local Network Subaddress        =

```

Figure 117 (Part 1 of 6). Scenario 2: Configuring 2210a via an ASCII Console

```

Maximum frame size in bytes   = 2048
Outbound call address Timeout = 180 Retries = 0
Switch Variant                = NTT INSnet64
TEI                           = Automatic
PS1 detect                    = Enabled
No circuit address accounting information being kept
ISDN Config>exit

Config>add device dial-circuit 8
Adding device as interface 4

Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters

Config>network 4 9
Circuit configuration

Circuit Config>set net 10
Base net for this circuit [0]?3
Circuit Config>set destination 11
Assign destination address name []?2210b
Circuit Config>set calls both 12
Circuit Config>set idle 13
Idle timer (seconds, 0 means always active) [0]?0

Circuit Config>list all 14

Base net:          3
Destination name:  2210b
Inbound dst name:  * ANY *
Outbound calls     allowed
Idle timer         = 0 (fixed circuit)
SelfTest Delay Timer = 150 ms

Circuit Config>encapsulator 15
Point-to-Point user configuration
PPP Config>list all 16

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:
Terminate Tries:              10   Retry Timer:

LCP Options
-----
Max Receive Unit:             2048   Magic Number:

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:
Terminate Tries:              10   Retry Timer:

```

Figure 117 (Part 2 of 6). Scenario 2: Configuring 2210a via an ASCII Console

```
IPCP Options
-----
IPCP Compression:          None
IP Address:                Send, Request
```

```
PPP Config>exit 17
```

```
Circuit Config>exit
Config>
```

```
Config>protocol ip 18
```

```
Internet protocol user configuration
```

```
IP config>add address
```

```
Which net is this address for [0]?
```

```
New address [0.0.0.0]? 9.67.113.101
```

```
Address mask [255.0.0.0]? 255.255.255.0
```

```
IP config>add address
```

```
Which net is this address for [0]? 4
```

```
New address [0.0.0.0]? 9.67.207.120
```

```
Address mask [255.0.0.0]? 255.255.255.0
```

```
IP config>enable rip 19
```

```
IP config>list all 20
```

```
Interface addresses
```

```
IP addresses for each interface:
```

intf 0	9.67.113.101 255.255.255.0	Network broadcast, fil 0
intf 1		IP disabled on this interface
intf 2		IP disabled on this interface
intf 3	9.67.207.120 255.255.255.0	Network broadcast, fil 0
intf 4		IP disabled on this interface

```
Routing
```

```
Protocols
```

Figure 117 (Part 3 of 6). Scenario 2: Configuring 2210a via an ASCII Console

```

BootP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0   9.67.113.101   Send net and subnet routes
    intf 1                               IP & RIP are disabled on this interface
    intf 2                               IP & RIP are disabled on this interface
    intf 3   9.67.207.120   Send net and subnet routes
    intf 4                               IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

EGP: disabled
IP Config>ctrl+p    21
*restart
Are you sure you want to restart the gateway? (Yes or [No]):

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

```

Figure 117 (Part 4 of 6). Scenario 2: Configuring 2210a via an ASCII Console

```

* Talk 5
+net 3
ISDN Console

ISDN>calls
Net Interface Site Name           In   Out   Rfsd  Blckd
  4   PPP/1   2210b                0    1     1     0

Unmapped connection indications:      0

ISDN>circuits
Net Interface MAC/Data-Link      State   Reason   Duration
  4   PPP/1   Point to Point    Up B1    SelfTest  0:05:40

ISDN>parameters
ISDN Port parameters:

Local Address Name:      2210a
Local Network Address:   6210
Local Network Subaddress:
Frame Size:              2048
TEI:                     Automatic
Switch Variant:          NTT INSnet64
Outbound call address Timeout: 180      PS1 detect: Enabled
Retries:                  0

ISDN>statistics
Link: Active   ISDN Firmware: 1.0   Handler State: Running

          D Channel   B1 Channel   B2 Channel

Total Transmits      48          260          0
Total Receives       54          259          0
Transmit Bytes       377        13197          0
Receive Bytes        373        13133          0
Invalid Interrupts    0           0           0

Transmit:      D      B1      B2   Receive:      D      B1

Error          0      0      0   Error          0      0
Overflow       0      0      0   Overflow       0      0
Underrun       0      0      0   Overrun       0      0
Abort          0      0      0   Abort         0      0
CRC Error      0      0      0   CRC Error     0      0

ISDN>exit

```

Figure 117 (Part 5 of 6). Scenario 2: Configuring 2210a via an ASCII Console

```

+interface 3 28
Nt Nt' Interface      CSR Vec  Self-Test  Self-Test  Maintenance
3 3  ISDN/0            0  0    Passed    Failed     Failed
                                1      0
                                0

ISDN Base Net MAC/data-link on ISDN Basic Rate Interface interface
Link:  Active  ISDN Firmware:  1.0  Handler State: Running

                                D Channel  B1 Channel  B2 Channel

Total Transmits                54          297          0
Total Receives                 60          296          0
Transmit Bytes                 413        14881          0
Receive Bytes                  409        14817          0
Invalid Interrupts             0           0           0

Transmit:      D      B1      B2  Receive:      D      B1

Error          0      0      0  Error          0      0
Overflow       0      0      0  Overflow       0      0
Underrun       0      0      0  Overrun        0      0
Abort          0      0      0  Abort          0      0
                                CRC Error    0      0

+interface 4 29
Nt Nt' Interface      CSR Vec  Self-Test  Self-Test  Maintenance
4 3  PPP/1            0  0    Passed    Failed     Failed
                                1      2
                                0

Point to Point MAC/data-link on ISDN Basic Rate Interface interface

+protocol ip 30
IP>dump 31

Type  Dest net      Mask    Cost Age  Next hop(s)

Sbnt  9.0.0.0        FF000000 1    0    None
Dir*  9.67.113.0     FFFFFFF0 1    0    TKR/0
RIP   9.67.124.0     FFFFFFF0 2    20   9.67.207.130
Dir*  9.67.207.0     FFFFFFF0 1    0    PPP/2

Routing table size: 768 nets (49152 bytes), 4 nets known

IP>ctrl+p 32

```

Figure 117 (Part 6 of 6). Scenario 2: Configuring 2210a via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Start customization of the token-ring interface.
- 3** Add an ISDN address name for the 2210a.
- 4** Add an ISDN address name for the 2210b.
- 5** List the interfaces on this router.

- 6** Start customization of the ISDN interface, setting the ISDN switch type, local address name, directory number 0, TEI and framesize.
- 7** Show the ISDN configuration.
- 8** Add a dial circuit.
- 9** Start customization of the dial circuit interface.
- 10** Link the dial circuit to the ISDN interface.
- 11** Configure the destination of the dial circuit.
- 12** Allow for both incoming and outgoing calls.
- 13** Set the line to always be active.
- 14** Show the dial circuit configuration.
- 15** Enter the PPP user configuration.
- 16** List all PPP configuration settings [Defaults].
- 17** Run the exit command twice to get back to the CONFIG prompt.
- 18** Start customization of the IP environment and assign IP addresses and subnet masks to the interfaces.
- 19** Enable RIP on all interfaces.
- 20** Show the IP configuration.
- 21** Exit the CONFIG process and restart the router for changes to take effect.
- 22** Enter the monitor process.
- 23** Enter the ISDN interface.
- 24** View the calls that have been made.
- 25** View the data link circuits status.
- 26** Show the statistics of the ISDN transmits and receives.
- 27** Exit the ISDN interface monitor.
- 28** View entire interface statistics of ISDN.
- 29** View entire data link circuit statistics.
- 30** Enter the IP Protocol Monitor.
- 31** List the routing table and view all routes.
- 32** Exit the monitoring process.

On the 2210 Navigation Window:
Select CONFIGURE from the menu bar
Select NEW CONFIGURATION
Select 2210-125/127 (TR/WAN/WAN/ISDN) **1**

On the 2210 Navigation Window:
Select ISDN ADDRESSES on the DEVICES directory.

On the ISDN ADDRESSES Window: **2**
ISDN ADDRESS NAME **2210a**
NETWORK DIAL ADDRESS **4410**
Select **ADD**

ISDN ADDRESS NAME **2210b**
NETWORK DIAL ADDRESS **4210**
Select **ADD**

On the 2210 Navigation Window:
Select DIAL CIRCUITS on the DEVICES directory.

On the DIAL CIRCUITS Window: **3**
BASE INTERFACE NUMBER **3**
CALLS BOTH
DISBALE ANY INBOUND
CIRCUIT TYPE **FIXED (LEASED)**
IDLE TIMER 0
SELF TEST DELAY TIMER 150
DESTINATION ADDRESS NAME **2210b**
Select **ADD**

On the 2210 Navigation Window:
Select INTERFACES on the DEVICES directory. **4**
MODEL 2210- 125/127
Select CONFIGURE for TOKEN-RING Interface
ENABLE INTERFACE
MAC ADDRESS 000000000000
SPEED **16**
PACKET SIZE 2048
RIF TIMER 120
DISABLE END NODE SOURCE ROUTING

Select CONFIGURE for ISDN Interface **5**
On the GENERAL subpanel:
ENABLE INTERFACE
MAX. FRAME SIZE 2048
PS1 DETECT
LOCAL ADDRESS NAME **2210a**
CALL ADDRESS: TIME OUT 180
RETRIES 2
SWITCH VARIANT **INS64**
TEI AUTO
DIRECTORY NUMBER 0
directory NUMBER 1

:

Figure 118 (Part 1 of 2). Scenario 2: Configuring 2210a via MRS Configuration Program

Select CONFIGURE for DIAL CIRCUIT (PPP) interface: **6**

On the GENERAL subpanel:

ENABLE INTERFACE

On the 2210 Navigation Window:

Select IP on the PROTOCOLS directory.

Select GENERAL from the IP directory.

On the IP GENERAL Window: **7**

ENABLE IP

DISABLE ACCESS CONTROL

ENABLE DIRECTED-BROADCAST

DISABLE PER-PACKET-MULTIPATH

INTERNAL ADDRESS blank

ROUTING TABLE SIZE = 768

CACHE SIZE = 64

ROUTER ID blank

On the 2210 Navigation Window:

Select IP on the PROTOCOLS directory.

Select INTERFACES from the IP directory.

On the IP INTERFACES Window: **8**

Select IP ADDRESSES for interface 0

IP ADDRESS = **9.67.113.101**

SUBNET MASK = 255.255.255.0

Select **ADD**

Select IP ADDRESSES for interface 4

IP ADDRESS = **9.67.207.120**

SUBNET MASK = 255.255.255.0

Select **ADD**

On the 2210 Navigation Window:

Select RIP on the PROTOCOLS directory.

Select GENERAL from the RIP directory.

On the RIP GENERAL Window: **9**

ENABLE RIP

On the 2210 Navigation Window:

Select CONFIGURE from the menu bar

Select SAVE CONFIGURATION AS

On the SAVE AS Window: **10**

DATABASE PATH = D:\RCFG120

DATABASE FILENAME = **2210A.CDB**

CONFIGURATION NAME = **2210a Configuration Data**

Select **OK**

On the 2210 Navigation Window: **11**

Select CONFIGURE from the menu bar

Select CREATE ROUTER CONFIGURATION

Enter filename **CONFIG.CFG**

Select **OK**

Figure 118 (Part 2 of 2). Scenario 2: Configuring 2210a via MRS Configuration Program

Notes:

- 1** Start a new configuration for the 2210 Model 125/127.
- 2** Add all ISDN addresses.
- 3** Add a dial circuit and configure an ISDN interface and destination address.
- 4** Configure the token-ring interface.
- 5** Configure the ISDN interface.
- 6** Ensure that the dial circuit (PPP) interface is enabled.
- 7** Enable IP.
- 8** Assign IP addresses to each interface.
- 9** Enable RIP.
- 10** Save configuration to the database for future reference.
- 11** Create router-compatible configuration file.

8.6.3 Scenario 3: Configuring OSPF with 6611 Interoperability over a PPP

In this scenario two 2210s (2210A and 2210B) are attached to a 6611 over a V35 PPP link, as shown in Figure 119 on page 382.

The 2210B is attached to an Ethernet LAN which includes a workstation running TCP/IP for OS/2 with the Routed daemon. Therefore, 2210B is an AS boundary router. It will originate default routes in the OSPF area. It will also advertise itself into the RIP network as the default router when it has OSPF routes available. It will not propagate the RIP routes into the OSPF area.

Using this configuration, users in subnet 9.67.46.160 will still be able to reach subnet 9.67.46.16.

Figure 120 on page 383 and Figure 121 on page 389 show the configuration of 2210A for this scenario.

Figure 122 on page 393 and Figure 123 on page 400 show the configuration of 2210B for this scenario.

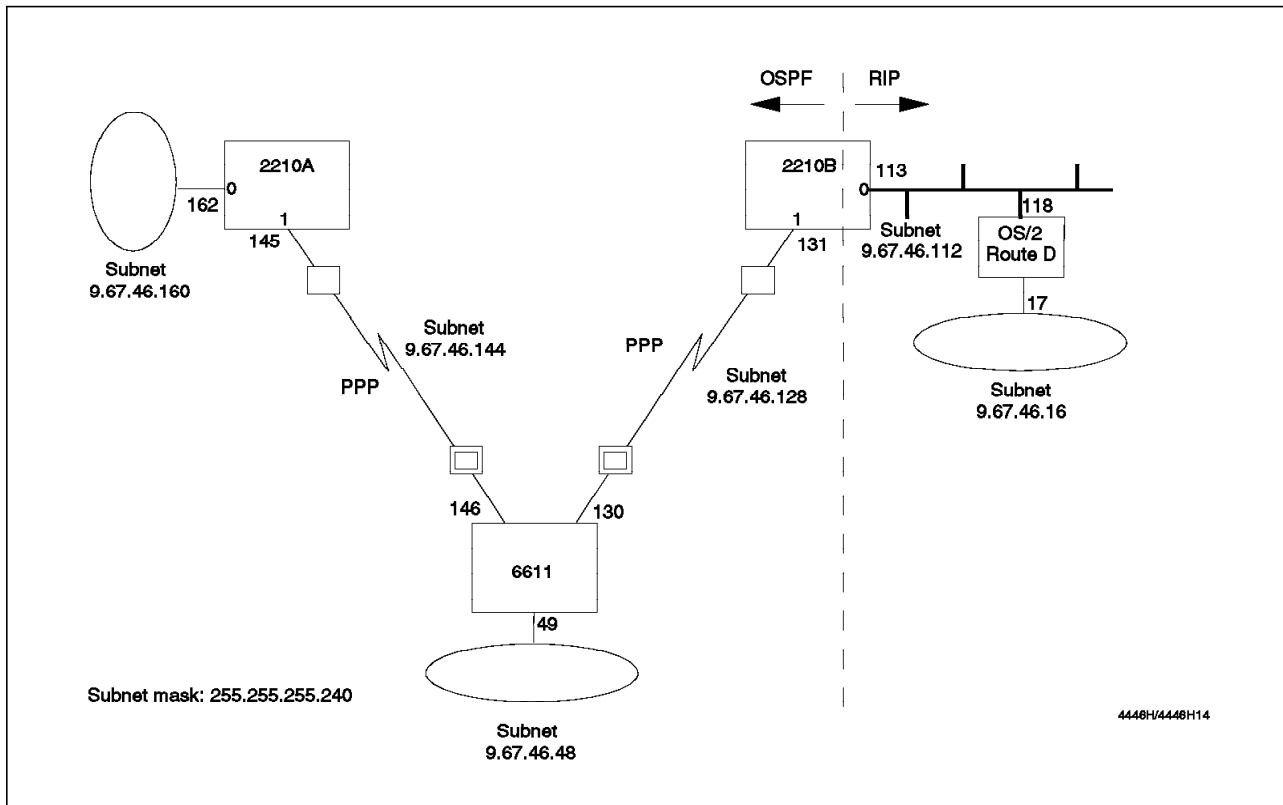


Figure 119. Scenario 3: OSPF Configuration with the IBM 2210 and IBM 6611 Network Processor

```

*talk 6 1

Config>list device 2
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>disable interface 2
Config>network 0 3
Token-Ring interface configuration
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                      4 Mb/sec
Media:                      Shielded

RIF Aging Timer:           120
Source Routing:            Enabled
MAC Address:                000000000000
IPX interface configuration record missing

TKR config>media unshielded 4
TKR config>set physical
MAC address in 00:00:00:00:00:00 form []? 40:00:22:10:a0:01
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                      4 Mb/sec
Media:                      Unshielded

RIF Aging Timer:           120
Source Routing:            Enabled
MAC Address:                40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 5
Point-to-Point user configuration

:

```

Figure 120 (Part 1 of 5). Scenario 3: Configuring 2210A via an ASCII Console

```

:
PPP Config>list hdlc

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>set hdlc cable v35 dte
PPP Config>exit
Config>protocol ip 6
Internet protocol user configuration
IP config>add address
Which net is this address for [0]?
New address [0.0.0.0]? 9.67.46.162
Address mask [255.0.0.0]? 255.255.255.240
IP config>add address
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.145
Address mask [255.0.0.0]? 255.255.255.240
IP config>set internal address
Internal IP address [9.67.46.162]?
IP config>set router-id
Router-ID [9.67.46.162]?
IP config>list addresses
IP addresses for each interface:
  intf 0   9.67.46.162      255.255.255.240  Network broadcast,    fill 0
  intf 1   9.67.46.145      255.255.255.240  Network broadcast,    fill 0
  intf 2                                     IP disabled on this interface
Router-ID: 9.67.46.162
Internal IP address: 9.67.46.162
IP config>exit
Config>protocol ospf 7
Open SPF-Based Routing Protocol configuration console
OSPF Config>enable ospf
Estimated # external routes [0]? 20
Estimated # OSPF routers [0]? 20
OSPF Config>set interface 8
Interface IP address [0.0.0.0]? 9.67.46.162
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?

:

```

Figure 120 (Part 2 of 5). Scenario 3: Configuring 2210A via an ASCII Console

```

:
OSPF Config>set interface
Interface IP address [0.0.0.0]? 9.67.46.145
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
OSPF Config>enable as boundary 9
Import EGP routes? [No]:
Import BGP routes? [No]:
Import RIP routes? [No]:
Import static routes? [No]:
Import direct routes? [No]: yes
Import subnet routes? [No]: yes
Always originate default route? [No]:
Originate default if EGP/BGP routes available? [No]:
OSPF Config>exit
Config>ctrl+p
*restart 10
Are you sure you want to restart the gateway? (Yes or [No]):y

```

```

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

```

```

MOS Operator Control

```

```

*talk 5 11

```

```

CGW Operator Console

```

```

+protocol ospf 12
Open SPF-Based Routing Protocol console

```

```

:

```

Figure 120 (Part 3 of 5). Scenario 3: Configuring 2210A via an ASCII Console

```

:
OSPF>dump 13
Type   Dest net      Mask      Cost Age  Next hop(s)

SPE2   0.0.0.0       00000000  1    5209  9.67.46.146
Sbnt   9.0.0.0       FF000000  1    0     9.67.46.146
SPF    9.67.46.48    FFFFFFFF0  26   26    9.67.46.146
SPE2   9.67.46.112   FFFFFFFF0  1    5209  9.67.46.146
SPE2   9.67.46.128   FFFFFFFF0  1    5209  9.67.46.146
SPF    9.67.46.130   FFFFFFFF  5210 5210  9.67.46.146
SPF    9.67.46.131   FFFFFFFF  5209 5209  9.67.46.146
Dir*   9.67.46.144   FFFFFFFF0  1    0     PPP/0
SPF    9.67.46.145   FFFFFFFF  5209 5209  PPP/0
SPF    9.67.46.146   FFFFFFFF  1     1     9.67.46.146
SPF*   9.67.46.160   FFFFFFFF0  1     1     TKR/0
SPF    9.67.46.162   FFFFFFFF  0     0     SINK/0

Default gateway in use.
Type Cost Age  Next hop
SPE2 1    5209 9.67.46.146

Routing table size: 768 nets (49152 bytes), 12 nets known
OSPF>ping 9.67.46.17 14
PING 9.67.46.17: 56 data bytes
64 bytes from 9.67.46.17: icmp_seq=0. time=50. ms
64 bytes from 9.67.46.17: icmp_seq=1. time=50. ms
64 bytes from 9.67.46.17: icmp_seq=2. time=50. ms
64 bytes from 9.67.46.17: icmp_seq=3. time=50. ms
64 bytes from 9.67.46.17: icmp_seq=4. time=50. ms
64 bytes from 9.67.46.17: icmp_seq=5. time=50. ms
64 bytes from 9.67.46.17: icmp_seq=6. time=66. ms
64 bytes from 9.67.46.17: icmp_seq=7. time=50. ms
64 bytes from 9.67.46.17: icmp_seq=8. time=50. ms

----9.67.46.17 PING Statistics----
9 packets transmitted, 9 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 50/51/66

:

```

Figure 120 (Part 4 of 5). Scenario 3: Configuring 2210A via an ASCII Console


```

:
OSPF>statistics 15

S/W version:          2.1
OSPF Router ID:       9.67.46.162
External comparison:  Type 2
AS boundary capability: Yes
Import external routes: DIR SUB
Orig. default route:  No (0,0.0.0.0)
Default route cost:   (1, Type 2)
Default forward. addr: 0.0.0.0

Attached areas:          1 Estimated # external routes: 20
Estimated # OSPF routers: 20 Estimated heap usage: 11680
OSPF packets rcvd:       21 OSPF packets rcvd w/ errs: 0
Transit nodes allocated: 17 Transit nodes freed: 14
LS adv. allocated:       10 LS adv. freed: 6
Queue headers alloc:     32 Queue headers avail: 32

# Dijkstra runs:         6 Incremental summ. updates: 0
Incremental VL updates:  0 Buffer alloc failures: 0
Multicast pkts sent:     31 Unicast pkts sent: 5
LS adv. aged out:        0 LS adv. flushed: 0
Incremental ext. updates: 2

OSPF>router 16
DType RType Destination      Area      Cost      Next hop(s)
ASBR  SPF   9.67.46.49      0.0.0.0    1         9.67.46.146
ASBR  SPF   9.67.46.131    0.0.0.0   5209      9.67.46.146

```

Figure 120 (Part 5 of 5). Scenario 3: Configuring 2210A via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** In this configuration serial interface 2 will not be used.
- 3** Start customization of the token-ring interface.
- 4** In this case we are on a 4 Mbps ring and are using the UTP port. In addition, a universally administered address (UAA) is used.
- 5** Start customization of serial interface 1. Notice the default setting of *encoding* is NRZ. The interface type is V35.
- 6** Start customization of the IP environment and assign IP addresses and subnets masks to the interfaces.
- 7** To configure OSPF go to the OSPF config console, enable OSPF and fill in the estimated number of external routes and the estimated number of OSPF routers.
- 8** Define the interfaces on which you want to enable OSPF and specify the related parameters.

- 9** Enable AS Boundary Routing to import direct and subnet routes.
- 10** Restart the router to activate this configuration.
- 11** The router restarted. Access the GWCON process to monitor the router.
- 12** Access the OSPF monitor console.
- 13** Show the routing table. (The same result could be obtained with the dump command on the IP monitor console.)
- 14** From 2210A you can reach subnet 9.67.46.16 due to the default route which is originated by 2210B.
- 15** The statistics command gives you more information about the OSPF environment.
- 16** The router command shows you the currently found OSPF routers.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 125** **2**
 Select CONFIGURE of interface 0
 ENABLE INTERFACE
 MAC ADDRESS = **40002210A001**
 Select SPEED
 Select 4
 Select PACKET SIZE
 Select 2052
 Select CABLE TYPE
 Select UTP
 RIF TIMER = 120
 DISABLE END NODE SOURCE ROUTING

Select CONFIGURE of serial interface 1 **3**
 On the GENERAL subpanel
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select **V35 DTE**
 Select subpanel LCP
 RETRY TIMER = 3000
 CONFIG TRIES = 20
 NAK TRIES = 10
 TERMINATE TRIES = 10
 MAXIMUM RECEIVE UNIT = 2048
 Select subpanel BNCP
 ENABLE MAGIC NUMBER
 DISABLE TINYGRAM COMPRESSION
 Select subpanel IPCP
 DISABLE IP COMPRESSION
 NUMBER OF SLOTS = 16
 DISABLE SEND IP ADDRESS
 DISABLE REQUEST IP ADDRESS

:

Figure 121 (Part 1 of 3). Scenario 10: Configuring 2210A Using the Nways MRS Configuration Program

```

:
  Select CONFIGURE of serial interface 2      4
    On the GENERAL subpanel:
      DISABLE INTERFACE

On the 2210 Navigation Window:
Select GENERAL on the IP directory

On the IP GENERAL Window:
  ENABLE IP      5
  DISABLE ACCESS CONTROL
  ENABLE DIRECTED-BROADCAST
  INTERNAL ADDRESS 9.67.46.162
  ROUTING TABLE SIZE = 768
  CACHE SIZE = 64
  ROUTER ID 9.67.46.162

On the 2210 Navigation Window:
Select INTERFACES on the IP directory

On the IP INTERFACES Window:
  Select IP ADDRESSES for interface 0      6
    IP ADDRESS = 9.67.46.162
    SUBNET MASK = 255.255.255.240
    Select ADD
  Select IP ADDRESSES for interface 1
    IP ADDRESS = 9.67.46.145
    SUBNET MASK = 255.255.255.240
    select ADD

On the 2210 Navigation Window:
Select GENERAL on the OSPF directory

On the OSPF GENERAL window:
  ENABLE OSPF      7
  DISABLE PER-PACKET-MULTICAST
  NUMBER OF EXTERNAL ROUTES = 100
  NUMBER OF OSPF ROUTERS = 50

On the 2210 Navigation Window:
Select INTERFACE on the OSPF directory

On the OSPF INTERFACES GENERAL Window:
  Select CONFIGURE of interface 0      8
  On the MULTICAST EXT subpanel
    ENABLE OSPF
    DISABLE MULTICAST
    DISABLE FORW/REC AS UNICAST
    COST = 1
    PRIORITY = 1
    IGMP POLLING INTERVAL = 60
    IGMP TIMEOUT 180
:

```

Figure 121 (Part 2 of 3). Scenario 10: Configuring 2210A Using the Nways MRS Configuration Program

```

:
    Select AREA NUMBER
        Select 0.0.0.0
    AUTHENTICATION KEY = 0
Select subpanel TIMERS
    RETRANS INTERVAL = 5
    HELLO INTERVAL = 10
    TRANSMISSION DELAY = 1
    DEAD ROUTER INTERVAL = 40

Select CONFIGURE of interface 1
On the MULTICAST EXT subpanel
    ENABLE OSPF
    DISABLE MULTICAST
    DISABLE FORW/REC AS UNICAST
    COST = 1
    PRIORITY = 1
    IGMP POLLING INTERVAL = 60
    IGMP TIMEOUT 180
    Select AREA NUMBER
        Select 0.0.0.0
    AUTHENTICATION KEY = 0
Select subpanel TIMERS
    RETRANS INTERVAL = 5
    HELLO INTERVAL = 10
    TRANSMISSION DELAY = 1
    DEAD ROUTER INTERVAL = 40

On the 2210 Navigation Window:
Select AS BOUNDARY ROUTING on the OSPF directory

On the AS BOUNDARY ROUTING window:
    ENABLE AS BOUNDARY 9
    DISABLE IMPORT EGP ROUTES
    DISABLE IMPORT RIP ROUTES
    DISABLE IMPORT STATIC ROUTES
    ENABLE IMPORT DIRECT ROUTES
    ENABLE IMPORT SUBNET ROUTES

On the 2210 Navigation Window:
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION 10

    On the FILE NAME FOR CONFIGURATION DATA, PLEASE? Window:
        enter <config.nme>
        Select OK

```

Figure 121 (Part 3 of 3). Scenario 10: Configuring 2210A Using the Nways MRS Configuration Program

Notes:

- 1** Start creating a new configuration.
- 2** Configure the router as Model 125. In addition, define a local address and a MAC address.

- 3** Configure interface 1 as a V35 PPP interface.
- 4** Disable interface 2 which is not used in this scenario.
- 5** Enable IP.
- 6** Assign IP addresses to the interfaces.
- 7** Enable OSPF.
- 8** Define the interfaces on which you want to enable OSPF, and specify the related parameters.
- 9** Enable AS Boundary Routing to import direct and subnet routes.
- 10** Create the router configuration file.

```

*talk 6 1

Config>list device 2
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>disable interface 2
Config>network 0 3
Ethernet interface configuration
ETH config>list 4
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:       ETHER

ETH config>exit
Config>network 1 5
Point-to-Point user configuration
PPP Config>list hdlc

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: Unknown, assuming DTE (other than X.21)
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>set hdlc cable v35 dte
PPP Config>exit
Config>protocol ip 6
Internet protocol user configuration
IP config>add address
Which net is this address for [0]?
New address [0.0.0.0]? 9.67.46.113
Address mask [255.0.0.0]? 255.255.255.240
IP config>add address
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.131
Address mask [255.0.0.0]? 255.255.255.240
IP config>enable rip 7
IP config>list protocol
BootP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled

:

```

Figure 122 (Part 1 of 6). Scenario 10: Configuring 2210B via an ASCII Console

```

:
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0  9.67.46.113    Send net and subnet routes
    intf 1  9.67.46.131    Send net and subnet routes
    intf 2                                IP & RIP are disabled on this interface
  
```

Accept RIP updates always for:
[NONE]

```

EGP: disabled
IP config>disable sending subnet-routes
Set for which interface address [0.0.0.0]? 9.67.46.131
IP config>disable sending net-routes
Set for which interface address [0.0.0.0]? 9.67.46.131
IP config>disable receiving rip
Set for which interface address [0.0.0.0]? 9.67.46.131
IP config>list protocol
BootP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0  9.67.46.113    Send net and subnet routes
    intf 1  9.67.46.131    Send no routes
                                Received RIP packets are ignored.
    intf 2                                IP & RIP are disabled on this interface
  
```

Accept RIP updates always for:
[NONE]

```

EGP: disabled
IP config>enable sending default-routes
Set for which interface address [0.0.0.0]? 9.67.46.113
IP config>list protocol
BootP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
:

```

Figure 122 (Part 2 of 6). Scenario 10: Configuring 2210B via an ASCII Console


```

:
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0   9.67.46.113   Send net, subnet and default routes
    intf 1   9.67.46.131   Send no routes
                           Received RIP packets are ignored.
    intf 2                               IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

EGP: disabled
IP config>set originate-rip-default 11
Always originate default route? [No]:
Originate default if EGP/BGP routes available? [No]:
Originate default if OSPF routes available? [No]: yes
Originate default of cost [1]?
IP config>exit
Config>protocol ospf 12
Open SPF-Based Routing Protocol configuration console
OSPF Config>enable ospf 13
Estimated # external routes [0]? 20
Estimated # OSPF routers [0]? 20
OSPF Config>set interface 14
Interface IP address [0.0.0.0]? 9.67.46.131
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key []?
Retype Auth. Key []?
OSPF Config>enable as boundary 15
Import EGP routes? [No]:
Import BGP routes? [No]:
Import RIP routes? [No]:
Import static routes? [No]:
Import direct routes? [No]: yes
Import subnet routes? [No]: yes Always originate default route? [No]: yes
Originate as Type 1 or 2 [2]?
Default route cost [1]?
Default forwarding address [0.0.0.0]? 9.67.46.131
:

```

Figure 122 (Part 3 of 6). Scenario 10: Configuring 2210B via an ASCII Console

```

:
OSPF Config>list all 16

--Global configuration--
  OSPF Protocol:      Enabled
  # AS ext. routes:   20
  Estimated # routers: 20
  External comparison: Type 2
  AS boundary capability: Enabled
  Import external routes: DIR SUB
  Orig. default route: Always (0,0.0.0.0)
  Default route cost: (1, Type 2)
  Default forward. addr.: 9.67.46.131
  Multicast forwarding: Disabled

--Area configuration--
Area ID      AuType      Stub? Default-cost Import-summaries?
0.0.0.0      0=None        No      N/A      N/A

--Interface configuration--
IP address    Area      Cost Rtrns TrnsDly Pri Hello Dead
9.67.46.131   0.0.0.0    1     5     1     1    10   40
OSPF Config>ctrl+p
*restart 17
Are you sure you want to restart the gateway? (Yes or [No]):y

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 18

CGW Operator Console

+protocol ospf 19
Open SPF-Based Routing Protocol console

:

```

Figure 122 (Part 4 of 6). Scenario 10: Configuring 2210B via an ASCII Console

```

:
OSPF>dump
Type   Dest net      Mask      Cost Age  Next hop(s)

Sbnt   9.0.0.0        FF000000  1    0    None
RIP    9.67.46.16     FFFFFFFF  2    10   9.67.46.114
SPF    9.67.46.48     FFFFFFFF  26   26   9.67.46.130
Dir*   9.67.46.112    FFFFFFFF  1    0    Eth/0
Dir*   9.67.46.128    FFFFFFFF  1    0    PPP/0
SPF    9.67.46.130    FFFFFFFF  1    1    9.67.46.130
SPF    9.67.46.131    FFFFFFFF  5209 5209 PPP/0
SPE2   9.67.46.144    FFFFFFFF  1    5209 9.67.46.130
SPF    9.67.46.145    FFFFFFFF  5209 5209 9.67.46.130
SPF    9.67.46.146    FFFFFFFF  5210 5210 9.67.46.130
SPF    9.67.46.160    FFFFFFFF  5210 5210 9.67.46.130
SPF    9.67.46.162    FFFFFFFF  5209 5209 9.67.46.130

Routing table size: 768 nets (49152 bytes), 12 nets known
OSPF>statistics

S/W version:          2.1
OSPF Router ID:       9.67.46.131
External comparison:   Type 2
AS boundary capability: Yes
Import external routes: DIR SUB
Orig. default route:   Always (0.0.0.0.0)
Default route cost:    (1, Type 2)
Default forward. addr: 9.67.46.131

Attached areas:          1 Estimated # external routes: 20
Estimated # OSPF routers: 20 Estimated heap usage: 11680
OSPF packets rcvd:       18 OSPF packets rcvd w/ errs: 0
Transit nodes allocated: 15 Transit nodes freed: 12
LS adv. allocated:       18 LS adv. freed: 12
Queue headers alloc:     32 Queue headers avail: 32

# Dijkstra runs:         4 Incremental summ. updates: 0
Incremental VL updates:  0 Buffer alloc failures: 0
Multicast pkts sent:     16 Unicast pkts sent: 5
LS adv. aged out:        0 LS adv. flushed: 0
Incremental ext. updates: 6

OSPF>router
DType RType Destination      Area      Cost      Next hop(s)

ASBR  SPF   9.67.46.49      0.0.0.0    1          9.67.46.130
ASBR  SPF   9.67.46.162     0.0.0.0   5209       9.67.46.130
Fadd  SPF   9.67.46.131     0.0.0.0   5209       9.67.46.130

:

```

Figure 122 (Part 5 of 6). Scenario 10: Configuring 2210B via an ASCII Console

```

:
OSPF>neighbor 23

Neighbor addr      Neighbor ID      State  LSrxl DBsum LSreq Ifc
9.67.46.130        9.67.46.49      128    0     0     0    PPP/0

OSPF>neighbor 9.67.46.130 24

Neighbor IP address: 9.67.46.130
OSPF Router ID:      9.67.46.49
Neighbor State:      128
Physical interface:   PPP/0
DR choice:            0.0.0.0
Backup choice:        0.0.0.0
DR Priority:          0
Nbr options:          E

DB summ qlen:        0  LS rxmt qlen:        0  LS req qlen:        0
Last hello:          9

# LS rxmits:          0  # Direct acks:        0  # Dup LS rcvd:        0
# Old LS rcvd:        0  # Dup acks rcv:        0  # Nbr losses:        0
# Adj. resets:        0

OSPF>database 25
For which area [0.0.0.0]?

Type LS destination  LS originator  Seqno  Age  Xsum
1  9.67.46.49        9.67.46.49    0x8000005E 240  0x1CB0
1  9.67.46.131       9.67.46.131   0x8000002F 236  0x5D13
1  9.67.46.162       9.67.46.162   0x8000001E 1595 0x22B8

# advertisements:    3
Checksum total:      0x9C7B

```

Figure 122 (Part 6 of 6). Scenario 10: Configuring 2210B via an ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** In this configuration serial interface 2 will not be used.
- 3** Start customization of the Ethernet interface.
- 4** The defaults can be used for the Ethernet interface.
- 5** Start customization of serial interface 1. Notice the default setting of *encoding* is NRZ. The interface type is V35.
- 6** Start customization of the IP environment and assign IP addresses and subnets masks to the interfaces.
- 7** Enable RIP.

- 8** Notice that RIP is enabled on all the interfaces including the serial interface which should run OSPF.
- 9** Disable all RIP traffic on the serial interface.
- 10** Enable sending default route on the Ethernet interface.
- 11** Enable the router to advertise itself as the default router in the RIP network.
- 12** To configure OSPF go to the OSPF CONFIG prompt.
- 13** Enable OSPF and specify the estimated number of external routes and the estimated number of OSPF routers.
- 14** Define the interfaces on which you want to enable OSPF and specify the related parameters.
- 15** Enable AS boundary routing to allow the importation of direct and subnet routes and allow this router to originate itself as the default router in the OSPF area.
- 16** The List All command shows the configuration of the OSPF environment.
- 17** Restart the router to activate this configuration.
- 18** The router is restarted. Access the GWCON process to monitor the router.
- 19** Access the OSPF monitor console.
- 20** The routing table (which could also be obtained with the Dump command from the IP monitor) shows the RIP route received from Routed.
- 21** This command shows the statistics generated by the OSPF protocol.
- 22** This command shows you the currently found OSPF routers.
- 23** This command, without a neighbor IP address, displays a one-line summary per neighbor.
- 24** This command, with a neighbor IP address, displays the statistics and parameters about a specific OSPF neighbor.
- 25** This command displays the link state database of the specified area.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 126** **2**
 Select CONFIGURE of interface 0
 ENABLE INTERFACE
 Select CONNECTOR TYPE
 Select **AUTO-CONFIG**
 Select IP ENCAPSULATION
 Select ETHERNET

Select CONFIGURE of serial interface 1 **3**
 On the GENERAL subpanel
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select **V35 DTE**
 Select subpanel LCP
 RETRY TIMER = 3000
 CONFIG TRIES = 20
 NAK TRIES = 10
 TERMINATE TRIES = 10
 MAXIMUM RECEIVE UNIT = 2048
 Select subpanel BNCP
 ENABLE MAGIC NUMBER
 DISABLE TINYGRAM COMPRESSION
 Select subpanel IPCP
 DISABLE IP COMPRESSION
 NUMBER OF SLOTS = 16
 DISABLE SEND IP ADDRESS
 DISABLE REQUEST IP ADDRESS

Select CONFIGURE of serial interface 2 **4**
 On the GENERAL subpanel:
DISABLE INTERFACE

:

Figure 123 (Part 1 of 4). Scenario 3: Configuring 2210B Using the Nways MRS Configuration Program

```

:
On the 2210 Navigation Window:
Select GENERAL on the IP directory

On the IP GENERAL Window:
  ENABLE IP 5
  DISABLE ACCESS CONTROL
  ENABLE DIRECTED-BROADCAST
  INTERNAL ADDRESS blank
  ROUTING TABLE SIZE = 768
  CACHE SIZE = 64
  ROUTER ID blank

On the 2210 Navigation Window:
Select INTERFACES on the IP directory

On the IP INTERFACES Window:
  Select IP ADDRESSES for interface 0 6
    IP ADDRESS = 9.67.46.113
    SUBNET MASK = 255.255.255.240
    Select ADD
  Select IP ADDRESSES for interface 1
    IP ADDRESS = 9.67.46.131
    SUBNET MASK = 255.255.255.240
    select ADD

On the 2210 Navigation Window:
Select GENERAL on the RIP directory

On the RIP GENERAL Window:
  ENABLE RIP 7

On the 2210 Navigation Window:
Select ORIGINATE RIP DEFAULT on the RIP directory

On the RIP ORIGINATE DEFAULT Window:
  DISABLE ALWAYS ORIGINATE DEFAULT ROUTE
  DISABLE ORIGINATE DEFAULT IF EGP ROUTES AVAILABLE
  ENABLE ORIGINATE DEFAULT IF OSPF ROUTES AVAILABLE 8
  ORIGINATE DEFAULT COST(1-16) = 1

On the 2210 Navigation Window:
Select INTERFACES on the RIP directory

On the RIP INTERFACES Window:
  Select CONFIGURE of interface 0
    On the GENERAL subpanel
      Select BROADCAST ADDRESS STYLE
      Select NETWORK
      Select ADDRESS FILL PATTERN
      Select ZEROES
      INTERFACE TAG (AS NUMBER) = 0

:

```

Figure 123 (Part 2 of 4). Scenario 3: Configuring 2210B Using the Nways MRS Configuration Program

```

:
  On the FLAGS subpanel
    ENABLE SEND NET ROUTES
    ENABLE SEND SUBNET ROUTES
    DISABLE SEND STATIC ROUTES
    ENABLE SEND DEFAULT ROUTES 9
    ENABLE RECEIVE RIP
    ENABLE RECEIVE DYNAMIC NETS
    ENABLE RECEIVE DYNAMIC SUBNETS
    DISABLE OVERRIDE DEFAULT
    DISABLE OVERRIDE STATIC ROUTES

  Select CONFIGURE of interface 1
  On the GENERAL subpanel
    Select BROADCAST ADDRESS STYLE
    Select NETWORK
    Select ADDRESS FILL PATTERN
    Select ZEROES
    INTERFACE TAG (AS NUMBER) = 0
  On the FLAGS subpanel
    DISABLE SEND NET ROUTES 10
    DISABLE SEND SUBNET ROUTES
    DISABLE SEND STATIC ROUTES
    DISABLE SEND DEFAULT ROUTES
    DISABLE RECEIVE RIP
    ENABLE RECEIVE DYNAMIC NETS
    ENABLE RECEIVE DYNAMIC SUBNETS
    DISABLE OVERRIDE DEFAULT
    DISABLE OVERRIDE STATIC ROUTES

  On the 2210 Navigation Window:
  Select GENERAL on the OSPF directory

  On the OSPF GENERAL window:
    ENABLE OSPF 11
    DISABLE PER-PACKET-MULTICAST
    NUMBER OF EXTERNAL ROUTES = 100
    NUMBER OF OSPF ROUTERS = 50

  On the 2210 Navigation Window:
  Select INTERFACE on the OSPF directory

  On the OSPF INTERFACES GENERAL Window:
    Select CONFIGURE of interface 1
    On the MULTICAST EXT subpanel
      ENABLE OSPF 12
      DISABLE MULTICAST
      DISABLE FORW/REC AS UNICAST
      COST = 1
      PRIORITY = 1
      IGMP POLLING INTERVAL = 60
      IGMP TIMEOUT 180
:

```

Figure 123 (Part 3 of 4). Scenario 3: Configuring 2210B Using the Nways MRS Configuration Program


```

:
  Select AREA NUMBER
    Select 0.0.0.0
  AUTHENTICATION KEY = 0
Select subpanel TIMERS
  RETRANS INTERVAL = 5
  HELLO INTERVAL = 10
  TRANSMISSION DELAY = 1
  DEAD ROUTER INTERVAL = 40

On the 2210 Navigation Window:
Select AS BOUNDARY ROUTING on the OSPF directory

On the AS BOUNDARY ROUTING window: 13
  ENABLE AS BOUNDARY
  DISABLE IMPORT EGP ROUTES
  DISABLE IMPORT RIP ROUTES
  DISABLE IMPORT STATIC ROUTES
  ENABLE IMPORT DIRECT ROUTES
  ENABLE IMPORT SUBNET ROUTES

On the 2210 Navigation Window:
  Select CONFIGURE from the menu bar
    Select CREATE ROUTER CONFIGURATION 14

    On the FILE NAME FOR CONFIGURATION DATA, PLEASE? Window:
      enter <config.nme>
      Select OK

```

Figure 123 (Part 4 of 4). Scenario 3: Configuring 2210B Using the Nways MRS Configuration Program

Notes:

- 1** Start creating a new configuration.
- 2** Specify Model 126. Use AUTO-CONFIG for the Ethernet interface.
- 3** Interface 1 is a V35 PPP interface.
- 4** Disable interface 2 which is not used.
- 5** Enable IP.
- 6** Assign IP addresses to the interfaces.
- 7** Enable RIP on all interfaces.
- 8** Only originate defaults into the RIP area if there are OSPF routes available.
- 9** Enable to send the default routes on the Ethernet interface.
- 10** Disable RIP on interface 1.
- 11** Enable OSPF.

- 12** Enable interface 1 for OSPF and specify the OSPF parameters.
- 13** Enable AS Boundary and import direct and subnet routes.
- 14** Create a router configuration file.

Chapter 9. IPX Routing and Configuration

This chapter provides an overview of IPX routing, configuring IPX routing on the IBM 2210, plus some configuration scenarios with the IBM 2210.

9.1 RIP Overview

IPX uses the Routing Information Protocol (RIP) to exchange routing information on a NetWare internetwork. NetWare routers use RIP to create and maintain a routing table. The routing table contains information on the networks reachable through that router.

Note: The RIP protocol used by NetWare is different from that used by IP.

The routing table will contain the following information for each network:

- Network number

The network number is the number of the IPX network to which the table entry relates.

- Number of hops to the network

The number of hops indicates the number of routers that must be crossed to reach the network.

- Number of ticks to the network

The number of ticks is an estimate of the time required to reach the network (where one tick is approximately 1/18th of a second).

- Interface through which the network is reached

The interface indicates through which of the router's interfaces this network is reachable.

- Address of the next hop router

The address of the next hop indicates the address of the router which is the next hop to the indicated network.

Note: If the network is directly connected to this router, this field will be blank.

- Aging timer

The aging timer is used to ensure that the information kept is current.

To build and maintain the routing tables, RIP packets are exchanged between the routers.

When a router is first initialized, it will place the network numbers of its directly connected networks into its routing table. It will then broadcast a RIP packet on each of its directly connected networks to inform routers on those networks of the networks it is making available.

The router will then broadcast a RIP request on each directly connected network, requesting information about all other networks available. All routers on those directly connected networks respond with information from their routing tables. The router then adds this information to its routing table and broadcasts a new

RIP packet to the directly connected networks, containing the newly learned information.

Note

Each router uses a split-horizon algorithm which prevents it from sending information about routes it learned back to the network from which it learned those routes.

The algorithm ensures that when a router broadcasts to a locally connected network, it doesn't include any information about other networks that it received from that locally connected network.

The algorithm also ensures that a router does not include information about the network from which it is broadcasting.

The router will now periodically broadcast RIP packets containing all the information in its routing table to its directly connected networks. A configurable parameter, called the *RIP update interval*, determines the interval between these broadcasts.

The router will also broadcast a RIP packet when it detects a network change, such as one of its directly connected networks going down. In this instance, the packet informs the other routers that all networks accessible through the failed network are now unreachable. It does this by setting the hop count for those networks to 16. (A network is considered unreachable if the number of hops is 16.)

When a router receives a RIP packet indicating a network change, it will update its routing table and inform other routers on its directly connected networks of the changes.

A RIP packet will also be sent, informing other routers that a network is unreachable, when the aging timer for the network expires. The timer expires if the router hasn't received any information for that network in a specified time. This mechanism allows the routers to handle the sudden loss of another router.

By using these RIP requests and responses, all routers on the internetwork are able to stay in synchronization.

9.1.1 RIP Packet Format

The RIP packet format is shown in Figure 124 on page 407. The packet is contained within the data portion of an IPX packet. RIP packets are defined within the IPX header as Packet Type 1 and Socket Number X'453'.

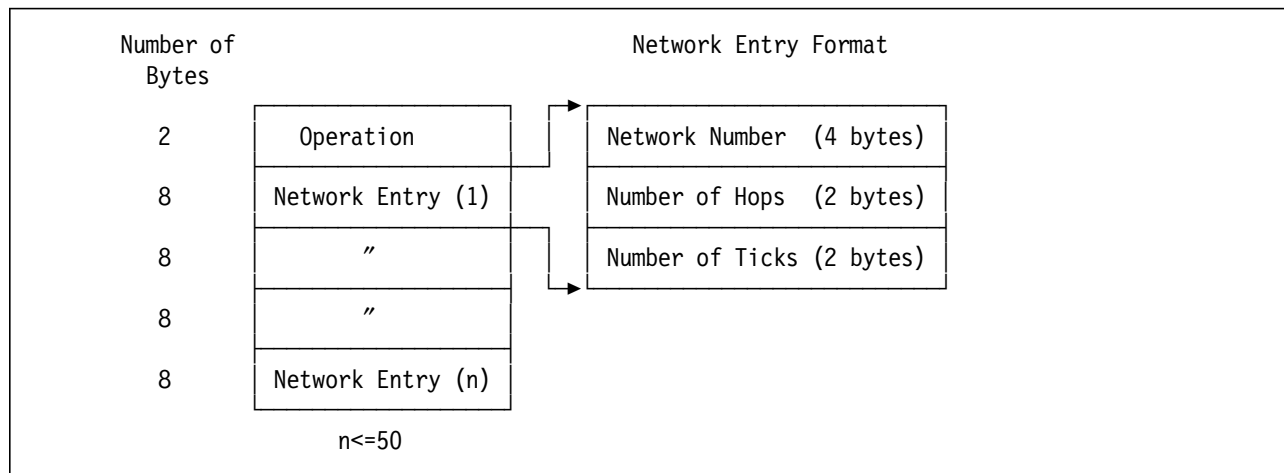


Figure 124. RIP Packet Format

9.1.1.1 Operation

This field indicates whether the packet is a request or a response. If it is a request, the field contains 1, and if it is a response, the field contains 2. A request can be for a specific network or a general request, such as when the router first starts and needs to learn the existing networks. For a general request, the network number field will contain X'FFFFFFF'.

A response is used to reply to a request and also to send informational packets, such as those sent periodically.

9.1.1.2 Network Entry

There can be up to 50 network entries in a RIP packet and each network entry contains the network number, number of hops, and number of ticks. If there is information for more than 50 networks to be broadcast, multiple RIP packets are used.

9.1.2 Route Selection

On large internetworks, there may be multiple routes to a single network. It is the responsibility of the router to select the best route to that network. The following is the criteria used for the best route selection is:

1. Select the route that requires the lowest number of ticks.
2. If multiple routes exist with the number of ticks equal, select the route that also has the lowest number of hops.
3. If multiple routes exist with both ticks and hops equal, the router is free to select any of these routes as the best route.

The routing table might contain a list of routes to each network in case the best route goes down. Alternatively, it might contain alternate routes only if those routes require the same amount of ticks as the best route. Another option would be for the routing table to contain only the best route.

Note

The router is free to choose if it will store only the best route, all routes, or some alternate routes.

When sending RIP responses, however, routers should only include the best route information.

9.2 SAP Overview

IPX uses the Service Advertising Protocol (SAP) to exchange information about available services on a NetWare network. Service-providing nodes, such as file servers and print servers, use SAP to advertise their services and addresses. Routers use SAP to create and maintain a database of services available on the internetwork. This allows clients to determine what services are available, and to obtain the addresses of the servers where they can access those services. This is important, as clients cannot access a file server unless they know the server's address.

The database maintained by the router is commonly called the Server Information Table. It contains the following information for each server:

- **Server name**
The server name is the name assigned to the server.
- **Server address**
The server address is a combination of the network address, the node address and the socket address for the server.
- **Server type**
The server type indicates the type of server this entry represents.
- **Hops to server**
The hops to server indicates the number of routers that must be crossed to reach the server.
- **Interface through which the information was received**
The interface indicates through which of the router's interfaces this SAP information was received.
- **Aging timer**
The aging timer is used to ensure that the information kept is current.

To build and maintain the server information tables, SAP packets are exchanged between routers and servers.

When a router is first initialized, it broadcasts a general SAP request on all of its directly connected networks, requesting information about all available servers on the internetwork. SAP agents on those directly connected networks will respond with information about the servers available, and the router will place that information in its server information table. The router then sends a SAP packet to its directly connected networks, containing the newly learned information.

The router will now periodically broadcast SAP packets containing all the information in its server information table to its directly connected networks. A configurable parameter, called the *SAP update interval*, determines the interval between these broadcasts.

The router will also broadcast a SAP packet when it detects a network change, such as one of its directly connected networks going down. In this instance, the packet informs the other routers that all servers accessible through the failed network are now unreachable. It does this by setting the hop count for those servers to 16.

When a router receives a SAP packet indicating a network change, it will update its server information table and inform other routers on its directly connected networks of the changes.

A SAP packet will also be sent, informing other routers that a server is unreachable, when the aging timer for the server expires. The timer expires if the router hasn't received any information for that server in a specified time. This mechanism allows the routers to handle the sudden loss of another router or server.

By using these SAP requests and responses, all routers and servers on the internetwork are able to stay in synchronization.

9.2.1 SAP Packet Format

The SAP packet format is shown in Figure 125. The packet is contained within the data portion of an IPX packet. SAP packets are defined within the IPX header as Packet Type 4 and Socket Number X'452'.

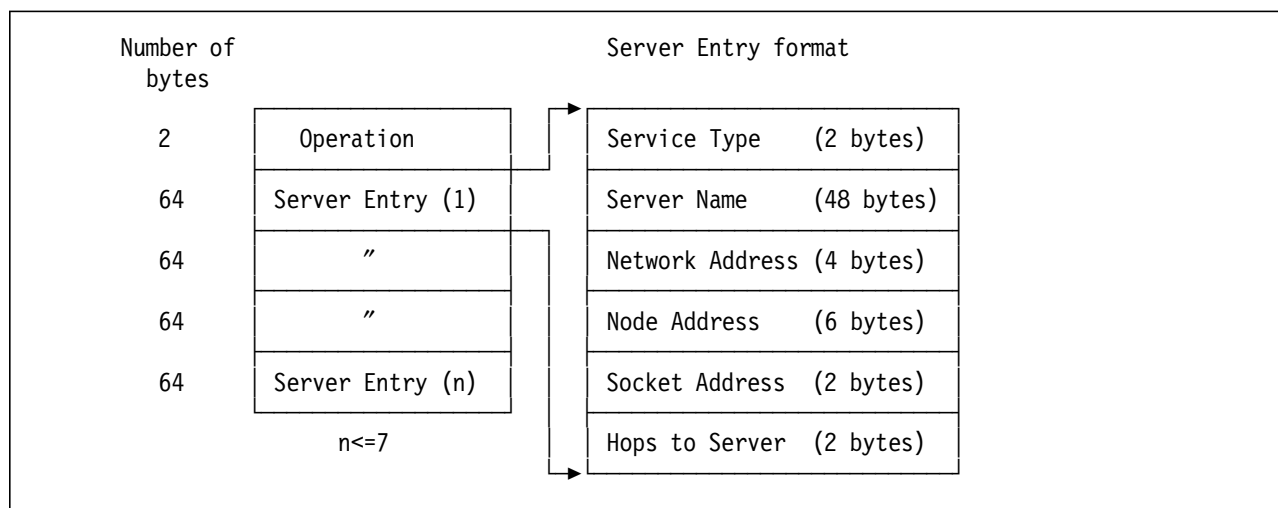


Figure 125. SAP Packet Format

Operation: This field indicates the type of operation being performed by this SAP packet and can be one of the following values:

- Request
- Response
- Get Nearest Server Request
- Get Nearest Server Response

The Get Nearest Server Request and Get Nearest Server Response are discussed in 9.2.2, “Get Nearest Server Request Handling” on page 410.

For all SAP requests, the Operations field is followed by a single Service Type field of two bytes, and nothing else.

All other fields shown are for response packets only.

Service Type: This field identifies the type of service being provided by the server. Some of the well-known server types are:

- X'0003' Print Queue
- X'0004' File Server
- X'0007' Print Server
- X'0009' Archive Server

Server Name: This field contains a 48-byte name that is assigned to a server. Typically, server names are not 48 characters long, but SAP response packets always include the full 48 bytes. The bytes after the end of the actual server name (which is marked by the ASCII null character) are undefined and may contain anything.

Network Address: This field contains the server's network address.

Node Address: This field contains the server's node address.

Socket Address: This field contains the socket number on which the server will receive service requests.

Hops to Server: This field indicates the number of routers that must be crossed to reach the server.

9.2.2 Get Nearest Server Request Handling

When a router receives a Get Nearest Server request, it should first check to see if any servers of the type requested reside on the same network as the requesting station. If that is the case, then the router should not respond to the Get Nearest Server request as the server will do so itself. If no server exists locally to the requester, then the router should respond with the nearest server of the type requested. The criteria used to determine the nearest server are:

1. Select the server which has the best route as determined by the routing table.
2. If multiple servers exist with equally good routes, select the server that also has the least number of hops as determined from the server information table.

9.3 IPXWAN Overview

The IPXWAN protocol was initially described in RFC 1362. RFC 1362 was superseded by RFC 1551, which has now been superseded by RFC 1634. The following overview pertains to IPXWAN as it is described in RFC 1362.

IPXWAN is a protocol used to exchange necessary information between routers prior to exchanging standard IPX routing information over serial links. It can be used over PPP, X.25, and frame relay.

Every IPXWAN router has a primary network number. This is an IPX network number that uniquely identifies the router within the internetwork.

Every IPXWAN router also has a router name. This is a symbolic name for the router, and is between 1 and 47 characters in length. It is useful for network management, as it identifies the router more easily.

An IPXWAN link has the concept of a *link master* and a *link slave*. The roles of master and slave are decided upon when the IPXWAN connection is established.

To initiate the IPXWAN connection, both routers start to send timer request packets. This is started as soon as the link has been established. They will continue to send timer request packets at 20-second intervals until a response is received or a timeout occurs. The timeout is a configurable value and should allow sufficient time for the call setup. If a timeout does occur, the router should issue a disconnect, and retry the link at a later time. The delay between issuing the disconnect and retrying is also configurable.

When a router receives the timer request, the router with the lowest primary network number must reply with a timer response. (The timer request packet contains the primary network number of the sender.) By sending the response, this router will become the slave.

The master becomes responsible for defining the IPX network number that is to be used for the serial link between the routers, and for calculating the RIP transport time that is to be advertised in RIP packets.

The master now sends an information request packet containing the network number, the transport time and its router name to the slave. The slave replies with an information response packet containing the same information, replacing the primary network number and router name with its own.

Once the information request has been received by the slave, and the information response has been received by the master, normal IPX RIP and SAP packets can be exchanged.

9.3.1 IPXWAN Packet Format

The IPXWAN packet format is shown in Figure 126 on page 412. The packet is contained within the data portion of an IPX packet. IPXWAN packets are defined within the IPX header as Packet Type 4 and Socket Number X'9004'.

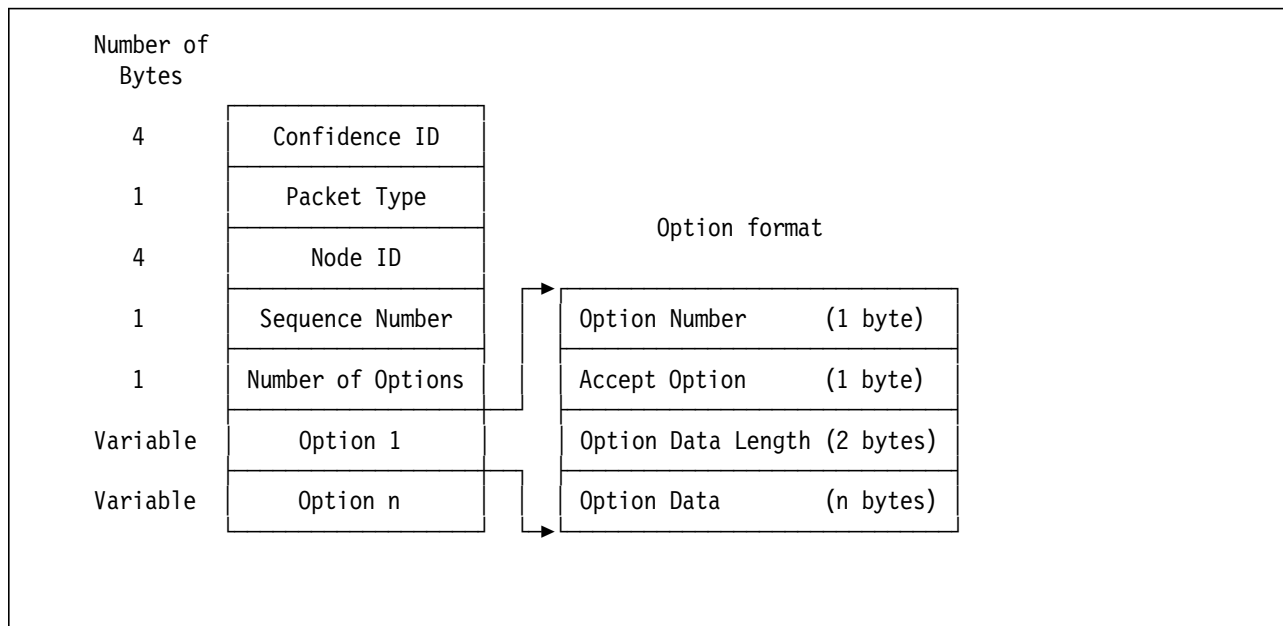


Figure 126. IPXWAN Packet Format

Confidence ID: This is a four-byte field and should be set to X'5741534D'. Any packet received on socket number X'9004' which doesn't have this value in the Confidence ID field should be discarded.

Packet Type: This one-byte field can be set to one of four values and identifies the command or response contained in the packet. The values and associated commands and responses are:

- X'00' Timer Request
- X'01' Timer Response
- X'02' Information Request
- X'03' Information Response

Node ID: This four-byte field is set to the primary network number of the router sending the packet.

Sequence Number: This is a one-byte field and is used to match responses to requests.

Number of Options: This field indicates the number of option fields to follow.

Option Number: This field identifies the option being requested, and is dependent on the packet type. For a timer request and response, two option numbers are used and they are both always sent in timer requests and responses. For an information request and response, only one option number is used.

Accept Option: This field identifies whether the associated option number is supported by the sending router. It can be set to one of three values:

- X'00' No
- X'01' Yes
- X'03' Not applicable

Option Data Length: This field indicates the number of option data bytes following.

Option Data: This field contains data specific to its associated option number.

9.3.1.1 Timer Request and Response Options

The timer request and response packets contain two option numbers:

- X'00' Define routing type
- X'FF' Pad

The define routing type option has a data length field of 1. The field is set to X'00' which means IPX RIP/SAP routing. The PAD option has a data length field of X'020E'. The field is a repeated sequence of X'00' to X'FF'.

9.3.1.2 Information Request and Response Options

The information request and response packets contain just one option number:

- X'01 IPX RIP/SAP information exchange

The data length field for this option is X'0036'. The data field contains:

- The link delay field (two bytes)
- The common network number field (four bytes)
- The router name of the sending router (48 bytes)

9.4 IPX Configuration on the IBM 2210

The IBM 2210 supports IPX over PPP, X.25 and frame relay. Additionally, it supports the IPXWAN protocol over PPP, and is compliant with RFC 1362.

The IBM 2210, supports up to 64 alternate routes per destination network in its routing table, and the RIP and SAP update intervals are both configurable between 1 minute and 1440 minutes.

To configure IPX on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of Nways MRS.

9.4.1 IPX Configuration Commands

This section summarizes the IPX configuration commands available within the CONFIG process of Nways MRS. To access the commands, you need to issue the following command:

```
Config>protocol ipx
```

Table 67 shows the commands available. *The Nways MRS Protocol Configuration and Monitoring Reference* covers these commands in detail.

Table 67 (Page 1 of 2). IPX Configuration Commands	
Command	Function
? (Help)	Lists all the IPX configuration commands, or lists the options associated with specific commands.
Add	Adds global IPX (access controls), and global SAP filters.
Delete	Deletes global IPX (access controls), and global SAP filters.

Table 67 (Page 2 of 2). IPX Configuration Commands

Command	Function
Disable	Disables IPX globally or on specific interfaces, keep-alive filtering, reply to SAP get-nearest-server request, RIP-SAP broadcast pacing and IPXWAN on specific interfaces.
Enable	Enables IPX globally or on specific interfaces, keep-alive filtering, reply to SAP get-nearest-server request, RIP-SAP broadcast pacing and IPXWAN on specific interfaces.
Frame	Specifies the data link format for Ethernet and token-ring interfaces.
List	Displays the current IPX configuration.
Move	Changes the line numbers set when adding access control.
Set	Sets the host number, IPXWAN router name and node ID, IPXWAN connection timeout and retry timer, IPX network number, maximum RIP and SAP table sizes, local and remote cache size, global IPX filter (access controls) and global SAP filter states, cache sizes, RIP/SAP update intervals, keep-alive filtering table size, and split-horizon usage.
Exit	Exits the IPX configuration environment and returns to the CONFIG environment.

9.4.2 IPX Configuration Overview

Configuration of IPX on the IBM 2210 is quite straightforward.

- You need to enable IPX globally and on the required interfaces.
- If you are routing IPX over PPP, you may need to enable IPXWAN.
- You may need to set the frame type that is being used for the token-ring or Ethernet.
- You need to set the network number for each interface, and the host number.
- If you are using IPXWAN, you need to set the node ID and router name.
- If you are routing IPX over X.25, you need to add the IPX protocol to the X.25 interface.
- If you are routing IPX over X.25, you also need to map the destination X.25 address to the destination IPX host number.
- If you are routing IPX over frame relay, you need to map the destination IPX host number to a DLCI.

9.4.2.1 Enabling IPX

To enable IPX globally and on the interfaces:

- Enter IPX Config>**enable ipx** and
IPX Config>**enable interface n** (where n = the interfaces you want to route IPX over), or
- Select **Enable IPX** on the Protocols/IPX/General panel, and select **IPX Enabled** for each interface on the Protocols/IPX/Interfaces panel of the Nways MRS Configuration Program.

9.4.2.2 Enabling IPXWAN

If you need to enable IPXWAN:

- Enter IPX Config>**enable ipxwan n** (where n = the PPP interface you are enabling IPX for), or
- Select **Configure** and then **IPXWAN Enabled** for the required interface on the Protocols/IPX/Interfaces panel of the Nways MRS Configuration Program.

9.4.2.3 Setting the Frame Type

The default frame type for token-ring is token-ring MSB, and for Ethernet it is ethernet_8023. If you need to change either of these:

- Enter IPX Config>**frame**, or
- Select **Configure** and then the frame type for the interface on the Protocols/IPX/Interfaces panel of the Nways MRS Configuration Program.

9.4.2.4 Setting the Network Number and Host Number

The network number needs to be set for all interfaces that are routing IPX. To set the network number:

- Enter IPX Config>**set net-number n net#**
(where n = the interface number, and net# = the IPX network number), or
- Select **Configure** and then **IPX Network Number** for each interface, on the Protocols/IPX/Interfaces panel of the Nways MRS Configuration Program.

Note: The IPX network number for the serial interface can be set to 0, but this will prevent IPX NetBIOS emulation packets from being passed across the serial link.

Each IBM 2210 routing IPX over a serial line needs to have a unique host number, because the serial interfaces do not have their own node address.

To set the host number:

- Enter IPX Config>**set host-number host#**
(where host# is a 12-digit host number), or
- Complete the Host Number field on the Protocols/IPX/General panel of the Nways MRS Configuration Program.

9.4.2.5 Setting the Node ID and Router Name

To set the node ID and router name for IPXWAN:

- Enter IPX Config>**set nodeid** and
- IPX Config>**set name**, or
- Complete the fields on the Protocols/IPXWAN Globals panel of the Nways MRS Configuration Program.

9.4.2.6 Adding IPX to the X.25 Interface

To add the IPX protocol to the X.25 interface:

- Enter X25 Config>**add protocol**, or
- Complete the fields on the Devices/General/X.25 Per Protocol Configuration panel of the Nways MRS Configuration Program.

9.4.2.7 Mapping the X.25 Address to the IPX Host Number

To map the destination X.25 address to the destination IPX host number:

- Enter X25 Config>**add address**, or
- Select **Configure** for the X.25 interface, then select **Mappings** and then complete the fields on the Devices/Interfaces panel of the Nways MRS Configuration Program.

Note: The X25 Config> prompt is accessed by entering:

Config>**network n**, where n = the number of the X.25 interface.

9.4.2.8 Mapping the IPX Host Number to a Frame Relay PVC

To map the destination IPX host number to a PVC for frame relay:

- Enter FR Config>**add protocol-address**, or
- Select **Configure** for the frame relay interface, then select **Protocols** and then complete the fields on the Devices/Interfaces panel of the Nways MRS Configuration Program.

Note: The FR Config> prompt is accessed by entering:

Config>**network n**, where n = the number of the frame relay interface.

9.4.3 Further IPX Configuration Considerations

You do not need access controls and SAP filters to have IPX routing, but they may be required if you wish to restrict access to IPX servers on the network, or if you wish to limit the size of the server information table.

Access controls are used to drop or forward packets based on their source and destination network addresses, node addresses and socket numbers.

Note

Access controls apply to all IPX packets, so if you add access controls, but don't add access controls to allow RIP and SAP packets through, IPX will not function on the router.

Access controls can be added by entering:

IPX Config>**add access-control**

or by completing the fields on the Protocols/IPX/Access Controls panel of the Nways MRS Configuration Program.

Access controls will now also need to be enabled, which you do by entering:

IPX Config>**set access-control on**

or by selecting **Enable Access Controls** on the Protocols/IPX/General panel of the Nways MRS Configuration Program.

SAP filters allow the IBM 2210 to ignore certain entries in SAP advertisements, and so deny access to some servers.

To add a SAP filter, you need to enter the following:

IPX Config>**add filter**

or complete the fields on the Protocols/IPX/SAP Filters panel of the Nways MRS Configuration Program.

SAP filters will now also need to be enabled, which you do by entering:

IPX Config>**set filter on**

or by selecting **Enable Access Controls** on the Protocols/IPX/General panel of the Nways MRS Configuration Program.

Another point to consider is if you have a large IPX internetwork. The IBM 2210, by default, will hold 32 entries in its routing table, and 32 entries in its server information table.

If you have a large IPX internetwork, you may need to increase the size of these tables.

You can increase the size of the routing table by entering the following:

IPX Config>**set maximum networks**

or by completing the Routing Table Size field on the Protocols/IPX/General panel of the Nways MRS Configuration Program.

You can increase the size of the server information table by entering IPX Config>**set maximum services**

or by completing the SAP Table Size field on the Protocols/IPX/General panel of the Nways MRS Configuration Program.

One further point to consider is the SAP and RIP update interval time. By default, both timers are set to one minute, but can be set to anything from one minute to 1440 minutes. You may wish to increase the RIP and SAP interval time on your serial links to reduce traffic across them, but remember that the broadcasts should be more frequent than the lowest aging timer in any other router. This is to prevent unnecessary broadcasts with the message: network unreachable.

9.5 Enhancements to IPX with MRS V1R1

With MRS V1R1, both global and interface filters can be defined. The global filters in this level of code are the same as the MRNS V1R1 access controls. The global-filters and interface-filters are mutually exclusive.

The four interface filters provide extensive control of network access. The router filter is used to group individual IPX networks into several distinct IPX internets by controlling which routers are allowed to exchange routing information. It cannot be used for output filtering.

The RIP filter is used to control the extent to which information about selected networks is disseminated. As an input filter, it can prevent all networks from learning about selected networks (at least through this router). As an output filter, it can prevent some networks from learning about selected networks (at least through this router).

The SAP filter is used to control the extent to which information about services is disseminated. As an input filter it will prevent all networks from learning about selected servers (at least through this router). As an output filter, it will prevent some networks from learning about selected servers (at least through this router).

The IPX filters control the extent to which selected servers and workstations are allowed to communicate with other selected servers and workstations. As an input filter, if a match indicates that the packet should be discarded, it prevents the packet from being transmitted on all interfaces. As an output filter, the decision whether to forward is made based on the output interface. So the packet may be forwarded on some interfaces but not on others.

keep-alive filtering was introduced for the dial-on-demand environment to prevent the line from being bought up by keep-alive requests/replies and serialization packets. If keep-alive filtering is enabled, the router forwards the reply and copies it to its keep-alive table. When the router local to the server receives the next request, it replies to the server. The router local to the client will send keep-alive requests to the client.

Enabling this function also prevents the line from being bought up for serialization packets. These packets are used by Novell to check to see that only one occurrence of a license is present within the network.

9.6 IPX Configuration Scenarios

This section provides some scenarios and configurations for IPX routing, using the IBM 2210. Included is one scenario using the IBM 6611 Network Processor along with the IBM 2210 to demonstrate their interoperability.

For each scenario, the configuration process using the Nways MRS user interface is shown, along with the equivalent process using the Nways MRS Configuration Program.

The two IBM 2210s used were running Nways MRS Version 1 Release 1, and the one IBM 6611 Network Processor used was running IBM 6611 MPNP Version 1 Release 3.

9.6.1 Scenario 12: Routing IPX over X.25

In this scenario, we have one IBM 2210 Model 12T, and one IBM 2210 Model 12E.

An IPX file server running NetWare Version 3.11 was on the Ethernet attached to the IBM 2210 Model 12E.

An IPX client station was on the token-ring attached to the IBM 2210 Model 12T.

The two IBM 2210s were connected via an X.25 network.

Note: The suitability of this configuration is dependent upon the speed of the links into the X.25 network, and the speed of the network itself.

Figure 127 on page 419 is a picture of this scenario.

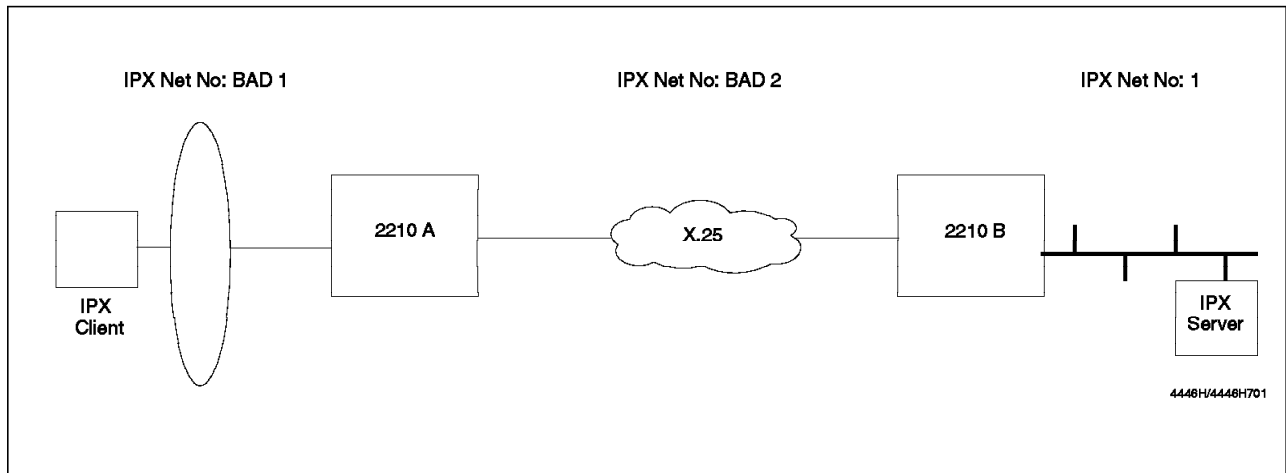


Figure 127. Scenario 1: IPX Routing over an X.25 Network

Figure 128 on page 420 shows the configuration process for 2210A using the Nways MRS CONFIG process.

Figure 129 on page 426 shows the configuration process for 2210B using the Nways MRS CONFIG process.

Figure 130 on page 430 shows the configuration process for 2210A using the Nways MRS Configuration Program.

Figure 131 on page 435 shows the configuration process for 2210B using the Nways MRS Configuration Program.

```

*talk 6 1

Config>network 0 2
Token-Ring interface configuration
TKR config>media unshielded 3
TKR config>set physical-address 40:00:22:10:A0:00
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                     4 Mb/sec
Media:                     Unshielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:               40002210A000
IPX interface configuration record missing

TKR config>exit
Config>set data-link x25 1 4
Config>network 1 5
X.25 User Configuration
X.25 Config>set cable rs-232 dte
X.25 Config>set address 201002600 6
X.25 Config>set calls-out 1 7
X.25 Config>set default-window-size 7
X.25 Config>set svc low-two-way 1
X.25 Config>set svc high-two-way 1
X.25 Config>national-personality set packet-size max 512
X.25 Config>national-personality disable accept-reverse-charges
X.25 Config>national-personality disable request-reverse-charges
X.25 Config>national-personality disable throughput-class-negotiation
X.25 Config>national-personality disable flow-control-negotiation
X.25 Config>add address 8
Protocol [IP]? ipx
CUD Field Usage (Standard or Proprietary) [STANDARD]? standard
IPX Host number (in hex) []? 40002210B002
X.25 Address []? 201002700
X.25 Config>add protocol 9
Protocol [IP]? ipx
Window Size [2]? 7
Default Packet Size [128]? 512
Maximum Packet Size [256]? 512
Circuit Idle Time [30]? 30
Max VCs [4]? 1

```

Figure 128 (Part 1 of 5). Scenario 1: 2210A Configuration Using Nways MRS CONFIG Process

X.25 Config>**list all**

10

X.25 Configuration Summary

Node Address: 201002600
Max Calls Out: 4 Inter-Frame Delay: 1
Speed: 9600 Clocking: External
Cable: RS-232 DTE
Default Window: 7 SVC idle: 30 seconds
National Personality: GTE Telenet (DTE)
PVC low: 0 high: 0
Inbound low: 0 high: 0
Two-Way low: 1 high: 1
Outbound low: 0 high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400

X.25 National Personality Configuration

Follow CCITT: on OSI 1984: on OSI 1988: off
Clear w/diag: on Reset w/diag: on Restart w/diag: on
Request Reverse Charges: off Accept Reverse Charges: off
Allow Packet Restarts: on Suppress Calling Addresses: off
Suppress Cause Fields: on Suppress Frame Idle RRs: off
Frame Extended seq mode: off Packet Extended seq mode: off
Use Multi-link Addresses: off Disable Interface Resets: off
Incoming Calls Barred: off Outgoing Calls Barred: off
Throughput Negotiation: off Flow Control Negotiation: off
DDN Address Translation: off
Call Request Timer: 20 decaseconds
Clear Request Timer: 18 decaseconds (1 retries)
Reset Request Timer: 18 decaseconds (1 retries)
Restart Request Timer: 18 decaseconds (1 retries)
T1 Timer: 4 seconds N2 timeouts: 20
T2 Timer: 2 seconds DP Timer: 500 milliseconds
Standard Version: 1984 Network Type: CCITT
Disconnect Procedure: passive
Window Size Frame: 7 Packet: 2
Packet Size Default: 128 Maximum: 512

X.25 protocol configuration

Prot Number	Window Size	Packet-size Default Maximum	Idle Time	Max VCs
7	7	512 512	30	1

X.25 PVC configuration

No PVCs defined

X.25 address translation configuration

IF # Prot # Protocol -> X.25 address
1 7 40002210B002 -> 201002700 CUD Field = STANDARD

X.25 Config>**exit**

Figure 128 (Part 2 of 5). Scenario 1: 2210A Configuration Using Nways MRS CONFIG Process

```

Config>protocol ipx 11
IPX protocol user configuration
IPX config>enable ipx 12
IPX config>enable interface 0
IPX config>enable interface 1
IPX config>set host-number 40002210A002 13
IPX config>set net-number 0 bad1 14
IPX config>set net-number 1 bad2
IPX config>list all 15

IPX globally                enabled
Host number (serial line)    40002210A002
Router Name (IPXWAN)         RouterA
NodeID (IPXWAN)              2210A
Maximum networks             32
Maximum total alt. route entries 128
Maximum alt. routes per dest. network 3
Maximum services             32
Maximum Network Cache entries 64
Maximum Local Cache entries  64

List of configured interfaces:
      Frame
Ifc  IPX net #  Encapsulation      SAP nearest server reply  IPXWAN
0    BAD1      TOKEN-RING          MSB  Enabled              N/A
1    BAD2      N/A                      Enabled                  N/A

RIP/SAP Timer Intervals
Net  IPX net #      SAP Interval(Minutes)  RIP Interval(Minutes)
  0    BAD1          1                      1
  1    BAD2          1                      1

IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.
IPX config>exit
Config>CTRL+P
*restart 16
Are you sure you want to restart the gateway? (Yes or -No]): y

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control
*talk 5 17

```

Figure 128 (Part 3 of 5). Scenario 1: 2210A Configuration Using Nways MRS CONFIG Process

```

+network 1      18
X.25 Console
X.25>list svcs  19

LCN/   Destination   Originate   Protocol   Totals
State Address         Call        Encapsulated Xmts  Rcv  Resets
1      D 201002700    NO          IPX         75    76    0

    D - Data Transfer  P - Call Progressing
    C - Call Clearing
X.25>statistics all 20

X.25 Physical Layer Counters:
Rx Bytes          43523   Tx Bytes          6883

Adapter cable:      RS-232 DTE  RISC Microcode Revision: 1

V.24 circuit: 105 106 107 108 109 125 141
Nicknames:      RTS CTS DSR DTR DCD RI  LL
RS-232:         CA CB  CC CD  CF CE
State:          ON  ON  ON  ON  ON  ON  OFF

Line speed:        unknown
Last port reset:   2 minutes, 29 seconds ago

Input frame errors:
CRC error          0 alignment (byte length) 6
missed frame       0 too long (> 1507 bytes) 0
aborted frame      10 DMA/FIFO overrun 0
L & F bits not set 0
Output frame counters:
DMA/FIFO underrun errors 0 Output aborts sent 3

Frame Layer Counters:
Received          Transmitted
Information Frames 401          490
RR Command         3           10
RR Response        24           4
RNR Command        0           0
RNR Response       0           0
REJ Command        0           0
REJ Response       0           2
SABM               0           1
SABME              0           0
UA                 1           0
DISC               0           0
DM                 0           0
FRMR               0           0

```

Figure 128 (Part 4 of 5). Scenario 1: 2210A Configuration Using Nways MRS CONFIG Process

T1 Timeouts	0	T2 Timeouts	1	N2 Timeouts	0
Bad Address	0	Unsolicited F-Bit	0	Invalid Ctl	0

Frame Layer Miscellaneous:

Queued Output Frames =	3	Protocol Layer State =	Data Transfer
Send Sequence N(S) =	6	Receive Sequence N(R) =	0

Packet Counters:

	Received	Transmitted
--	----------	-------------

Call Request	2	0
Call Accepted	0	2
Clear Request	1	0
Clear Confirm	0	1
Interrupt Request	0	0
Interrupt Confirm	0	0
RR Packet	2	407
RNR Packet	0	0
REJ Packet	0	0
Reset Request	0	0
Reset Confirm	0	0
Restart Request	1	1
Restart Confirm	0	0
Diagnostic	0	0
Data Packet	411	97
Data Bytes	44355	4752
Buffers Queued	0	0
Invalid Packets Received =	0	
Switched Circuits Opened =	1	

X.25>exit

+protocol ipx **21**

IPX>dump **22**

Type	Dest net	Hops	Delay	Age(M:S)	via Router
Dir	BAD2	0	1	0: 0	BAD2/40002210A002
Dir	BAD1	0	1	0: 0	BAD1/40002210A001
RIP	1	1	2	0:55	BAD2/40002210B002
RIP	32211	2	3	0:55	BAD2/40002210B002

4 route entries used out of 128

4 net entries used out of 32

IPX>slist **23**

State	Typ	Service Name	Hops	Age	Net / Host / Sock
SAP	05B3	BANK311	3	0: 5	32211/000000000001/0000
SAP	0107	BANK311	3	0: 5	32211/000000000001/8104
SAP	0004	BANK311	2	0: 5	32211/000000000001/0451

3 entries used out of 32

Figure 128 (Part 5 of 5). Scenario 1: 2210A Configuration Using Nways MRS CONFIG Process

Notes:

- 1** Talk to the CONFIG process.
- 2** Start customization of the token-ring interface.
- 3** In this scenario, we are using UTP on a 4 MBps ring, and we wish to use a locally administered address.

- 4** Set interface 1 to X.25.
- 5** Start customization of the X.25 interface.
- 6** Set the X.25 address of this router.
- 7** Set X.25 network specific parameters. In this scenario, we only have one SVC, and cannot use reverse charging, throughput class negotiation, or flow control negotiation.
- 8** Add an X.25 address to IPX host number mapping, for the destination router.
- 9** Add the IPX protocol to the X.25 interface.
- 10** List the X.25 configuration to ensure that everything is correct.
- 11** Start the IPX customization.
- 12** Enable IPX globally and on the interfaces.
- 13** Set the IPX host number for the serial interfaces.
- 14** Set the IPX network numbers for each interface.
- 15** List the IPX configuration to ensure that everything is correct.
- 16** Restart the router.
- 17** Talk to the GWCON process.
- 18** Enter the X.25 monitoring console.
- 19** List the active SVCs.
- 20** List all the X.25 statistics.
- 21** Enter the IPX monitoring console.
- 22** List the RIP routing table.
- 23** List the SAP server information table.

```

*talk 6 1

Config>network 0 2
Ethernet interface configuration
ETH config>list
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:       ETHER

ETH config>exit
Config>set data-link x25 1 3
Config>network 1 4
X.25 User Configuration
X.25 Config>set cable rs-232 dte
X.25 Config>set address 201002700 5
X.25 Config>set calls-out 1 6
X.25 Config>set default-window-size 7
X.25 Config>set svc low-two-way 1
X.25 Config>set svc high-two-way 1
X.25 Config>national-personality set packet-size max 512
X.25 Config>national-personality disable accept-reverse-charges
X.25 Config>national-personality disable request-reverse-charges
X.25 Config>national-personality disable throughput-class-negotiation
X.25 Config>national-personality disable flow-control-negotiation
X.25 Config>add address 7
Protocol [IP]? ipx
CUD Field Usage (Standard or Proprietary) [STANDARD]? standard
IPX Host number (in hex) []? 40002210A002
X.25 Address []? 201002600
X.25 Config>add protocol 8
Protocol [IP]? ipx
Window Size [2]? 7
Default Packet Size [128]? 512
Maximum Packet Size [256]? 512
Circuit Idle Time [30]? 30
Max VCs [4]? 1

```

Figure 129 (Part 1 of 3). Scenario 1: 2210B Configuration Using Nways MRS CONFIG Process

X.25 Config>**list all** **9**

X.25 Configuration Summary

Node Address: 201002700
Max Calls Out: 1 Inter-Frame Delay: 1
Speed: 9600 Clocking: External
Cable: RS-232 DTE
Default Window: 7 SVC idle: 30 seconds
National Personality: GTE Telenet (DTE)
PVC low: 0 high: 0
Inbound low: 0 high: 0
Two-Way low: 1 high: 1
Outbound low: 0 high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400

X.25 National Personality Configuration

Follow CCITT: on OSI 1984: on OSI 1988: off
Clear w/diag: on Reset w/diag: on Restart w/diag: on
Request Reverse Charges: off Accept Reverse Charges: off
Allow Packet Restarts: on Suppress Calling Addresses: off
Suppress Cause Fields: on Suppress Frame Idle RRs: off
Frame Extended seq mode: off Packet Extended seq mode: off
Use Multi-link Addresses: off Disable Interface Resets: off
Incoming Calls Barred: off Outgoing Calls Barred: off
Throughput Negotiation: off Flow Control Negotiation: off
DDN Address Translation: off
Call Request Timer: 20 decaseconds
Clear Request Timer: 18 decaseconds (1 retries)
Reset Request Timer: 18 decaseconds (1 retries)
Restart Request Timer: 18 decaseconds (1 retries)
T1 Timer: 4 seconds N2 timeouts: 20
T2 Timer: 2 seconds DP Timer: 500 milliseconds
Standard Version: 1984 Network Type: CCITT
Disconnect Procedure: passive
Window Size Frame: 7 Packet: 2
Packet Size Default: 128 Maximum: 512

X.25 protocol configuration

Prot Number	Window Size	Packet-size Default	Packet-size Maximum	Idle Time	Max VCs
7	7	512	512	30	1

X.25 PVC configuration

No PVCs defined

X.25 address translation configuration

IF # Prot # Protocol -> X.25 address
1 7 40002210A002 -> 201002600 CUD Field = STANDARD

X.25 Config>**exit**

Figure 129 (Part 2 of 3). Scenario 1: 2210B Configuration Using Nways MRS CONFIG Process

```

Config>protocol ipx 10
IPX protocol user configuration
IPX config>enable ipx 11
IPX config>enable interface 0
IPX config>enable interface 1
IPX config>set host-number 40002210B002 12
IPX config>set net-number 0 1 13
IPX config>set net-number 1 bad2
IPX config>list all 14

IPX globally                enabled
Host number (serial line)    40002210B002
Router Name (IPXWAN)         RouterB
NodeID (IPXWAN)              2210B
Maximum networks             32
Maximum total alt. route entries 128
Maximum alt. routes per dest. network 3
Maximum services             32
Maximum Network Cache entries 64
Maximum Local Cache entries  64

List of configured interfaces:
      Frame
Ifc  IPX net #  Encapsulation      SAP nearest server reply  IPXWAN
0    1          ETHERNET_802.3      Enabled                  N/A
1    BAD2       N/A                 Enabled                  N/A

RIP/SAP Timer Intervals
Net  IPX net #      SAP Interval(Minutes)  RIP Interval(Minutes)
0    1              1                      1
1    BAD2           1                      1

IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.
IPX config>exit
Config>CTRL+P
*restart
Are you sure you want to restart the gateway? (Yes or -No]): y

```

Figure 129 (Part 3 of 3). Scenario 1: 2210B Configuration Using Nways MRS CONFIG Process

Notes:

- 1** Talk to the CONFIG process.
- 2** Start customization of the Ethernet interface.
- 3** Set interface 1 to X.25
- 4** Start customization of the X.25 interface.
- 5** Set the X.25 address of this router.
- 6** Set X.25 network specific parameters. In this scenario, we only have one SVC, and cannot use reverse charging, throughput class negotiation, or flow control negotiation.

- 7** Add an X.25 address to IPX host number mapping, for the destination router.
- 8** Add the IPX protocol to the X.25 interface.
- 9** List the X.25 configuration to ensure that everything is correct.
- 10** Start the IPX customization.
- 11** Enable IPX globally, and on the interfaces.
- 12** Set the IPX host number for the serial interfaces.
- 13** Set the IPX network numbers for each interface.
- 14** List the IPX configuration to ensure that everything is correct.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 12T** **2**
 Select CONFIGURE of interface 0 **3**
 ENABLE INTERFACE
 MAC ADDRESS = **40002210A001**
 Select SPEED
 Select 4
 Select PACKET SIZE
 Select 2052
 Select CABLE TYPE
 Select **UTP**
 RIF TIMER = 120
 DISABLE END NODE SOURCE ROUTING

Select PPP of interface 1
 Select **X.25** **4**

Select CONFIGURE of serial interface 1 **5**
 On the GENERAL subpanel
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select RS-232 DTE
 Select subpanel NODE CONFIG **6**
X25 NODE ADDRESS = 201002600
 Select EQUIPMENT TYPE
 Select DTE
 IDLE TIME = 30
MAX CALLS OUT = 1
DEFAULT WINDOW SIZE = 7
 LOWEST INBOUND CHANNEL = 0
 HIGHEST INBOUND CHANNEL = 0
 LOWEST TWO WAY CHANNEL = 1
HIGHEST TWO WAY CHANNEL = 1
 LOWEST OUTBOUND CHANNEL = 0
 HIGHEST OUTBOUND CHANNEL = 0

Figure 130 (Part 1 of 4). Scenario 1: 2210A Configuration Using Nways MRS Configuration Program

```

Select subpanel STANDARDS
  Select NETWORK TYPE
    Select CCITT
    ENABLE FOLLOW CCITT
  Select CCITT VERSION
    Select 1984
    ENABLE OSI 1984 FACILITIES
Select subpanel ALLOW 7
  ENABLE PACKET LAYER RESTARTS
  ENABLE CALLING ADDRESSES
  DISABLE NON-ZERO CAUSE FIELDS
  ENABLE IDLE FRAME RRs
  DISABLE FRAME EXTENDED SEQUENCE MODE
  DISABLE PACKET EXTENDED SEQUENCE MODE
  DISABLE MULTI-LINK ADDRESSES
  ENABLE INTERFACE RESETS
  ENABLE INCOMING CALLS
  ENABLE OUTGOING CALLS
Select subpanel DIAGNOSTICS
  ENABLE IN CLEAR REQUEST PACKETS
  ENABLE IN RESET REQ PACKETS
  ENABLE IN RESTART REQUEST PACKETS
  CLEAR REQUEST RETRIES = 1
  RESET REQUEST RETRIES = 1
  RESTART REQUEST RETRIES = 1
Select subpanel TIMERS
  T1 TIMER = 4
  T2 TIMER = 2
  N2 TIMEOUT = 20
  DISCONNECT TIMER = 500
  Select DISCONNECT PROCEDURE
    Select PASSIVE
  CALL REQUEST = 20
  CLEAR REQUEST = 18
  RESET REQUEST = 18
  RESTART REQUEST = 18
Select subpanel PACKET SIZE
  FRAME WINDOW SIZE = 7
  Select DEFAULT PACKET SIZE
    Select 128
  Select MAXIMUM PACKET SIZE
    Select 512
  WINDOW PACKET SIZE = 2
  Select THROUGHPUT CLASS INBOUND
    Select 2400
  Select THROUGHPUT CLASS OUTBOUND
    Select 2400
Select subpanel CHARGES 8
  DISABLE ACCEPT REVERSE CHARGES
  DISABLE REQUEST REVERSE CHARGES
Select subpanel PERFORMANCE
  DISABLE THROUGHPUT CLASS NEGOTIATION
  DISABLE FLOW CONTROL NEGOTIATION
  DISABLE DDN ADDRESS TRANSLATION

```

Figure 130 (Part 2 of 4). Scenario 1: 2210A Configuration Using Nways MRS Configuration Program

Select subpanel MAPPINGS **9**
Select PROTOCOL
Select IPX
PROTOCOL ADDRESS = 40002210B002
Select CUD Field Usage
Select STANDARD
X.25 ADDRESS = 201002700
Select ADD

Select CONFIGURATION of Serial 2
On GENERAL subpanel :
DISABLE INTERFACE **10**

On the 2210 Navigation Window:
Select X25 PER PROTOCOL CONFIGURATION ON THE DEVICES/GENERAL DIRECTORY **11**

On the X25 PER PROTOCOL CONFIGURATION Window:
Select PROTOCOL
Select IPX **12**
WINDOW SIZE = 7
Select DEFAULT PACKET SIZE
Select **512**
IDLE TIME = 30
MAX VCs = 1
Select MAXIMUM PACKET SIZE
Select **512**
Select **ADD**

On the 2210 Navigation Window:
Select GENERAL on the IPX directory **13**

On the IPX GENERAL Window: **14**
ENABLE IPX
DISABLE ACCESS CONTROLS
DISABLE SAP FILTERS
HOST NUMBER = 40002210A002
ROUTING TABLE SIZE = 32
SAP TABLE SIZE = 32
REMOTE CACHE SIZE = 64
LOCAL CACHE ENTRY SIZE = 64
MAXIMUM NUMBER OF ALTERNATE ROUTES = 128
MAXIMUM NUMBER OF ROUTES PER DESTINATION IPX NETWORK = 3

On the 2210 Navigation Window:
Select INTERFACES on the IPX directory **15**

On the IPX INTERFACES Window:
Select CONFIGURE of interface 0 **16**
ENABLE IPX
ENABLE IPX GNS
SAP INTERVAL = 1
RIP INTERVAL = 1
IPX NETWORK NUMBER = BAD1
Select FRAMING TYPE
Select TOKEN-RING MSB

Figure 130 (Part 3 of 4). Scenario 1: 2210A Configuration Using Nways MRS Configuration Program

Select CONFIGURE of interface 1 **17**

ENABLE IPX

ENABLE IPX GNS ENABLED

DISABLE WAN ENABLED

IPX NETWORK NUMBER = BAD2

SAP INTERVAL = 1

RIP INTERVAL = 1

CONNECT TIME = 60

RETRY TIME = 60

On the 2210 Navigation Window:

Select CONFIGURE from the menu bar

Select CREATE ROUTER CONFIGURATION **18**

On the FILE NAME FOR CONFIGURATION DATA, PLEASE? Window:

enter **ipxx25a**

Select OK

Figure 130 (Part 4 of 4). Scenario 1: 2210A Configuration Using Nways MRS Configuration Program

Notes:

- 1** Start a new configuration.
- 2** Use token-ring Model 12T.
- 3** Configure the token-ring interface.
- 4** Set interface 1 to X.25.
- 5** Configure the X.25 interface.
- 6** Set the general parameters, such as the X.25 address and SVC ranges.
- 7** Set the X.25 call setup and diagnostic parameters.
- 8** Disable reverse charging, and negotiation parameters for this scenario.
- 9** Map the destination X.25 address to the IPX host number.
- 10** Disable interface 2, as it is not being used in this scenario.
- 11** Select the X.25 per protocol configuration.
- 12** Add the IPX protocol to the X.25 interface.
- 13** Configure the IPX protocol.
- 14** Enable IPX globally, and set general parameters, such as the host number and RIP and SAP table sizes.
- 15** Configure IPX on the interfaces.
- 16** Configure interface 0.

- 17** Configure interface 1.
- 18** Create a router configuration file.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 12E** **2**
 Select CONFIGURE of interface 0 **3**
 ENABLE INTERFACE
 Select CONNECTOR TYPE
 Select **AUTO-CONFIG**

Select PPP of interface 1
 Select **X.25** **4**

Select CONFIGURE of serial interface 1 **5**
 On the GENERAL subpanel
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select RS-232 DTE
 Select subpanel NODE CONFIG **6**
X25 NODE ADDRESS = 201002700
 Select EQUIPMENT TYPE
 Select DTE
 IDLE TIME = 30
MAX CALLS OUT = 1
DEFAULT WINDOW SIZE = 7
 LOWEST INBOUND CHANNEL = 0
 HIGHEST INBOUND CHANNEL = 0
 LOWEST TWO WAY CHANNEL = 1
HIGHEST TWO WAY CHANNEL = 1
 LOWEST OUTBOUND CHANNEL = 0
 HIGHEST OUTBOUND CHANNEL = 0

Figure 131 (Part 1 of 4). Scenario 1: 2210B Configuration Using Nways MRS Configuration Program

```

Select subpanel STANDARDS
  Select NETWORK TYPE
    Select CCITT
    ENABLE FOLLOW CCITT
    Select CCITT VERSION
      Select 1984
    ENABLE OSI 1984 FACILITIES
Select subpanel ALLOW 7
  ENABLE PACKET LAYER RESTARTS
  ENABLE CALLING ADDRESSES
  DISABLE NON-ZERO CAUSE FIELDS
  ENABLE IDLE FRAME RRs
  DISABLE FRAME EXTENDED SEQUENCE MODE
  DISABLE PACKET EXTENDED SEQUENCE MODE
  DISABLE MULTI-LINK ADDRESSES
  ENABLE INTERFACE RESETS
  ENABLE INCOMING CALLS
  ENABLE OUTGOING CALLS
Select subpanel DIAGNOSTICS
  ENABLE IN CLEAR REQUEST PACKETS
  ENABLE IN RESET REQ PACKETS
  ENABLE IN RESTART REQUEST PACKETS
  CLEAR REQUEST RETRIES = 1
  RESET REQUEST RETRIES = 1
  RESTART REQUEST RETRIES = 1
Select subpanel TIMERS
  T1 TIMER = 4
  T2 TIMER = 2
  N2 TIMEOUT = 20
  DISCONNECT TIMER = 500
  Select DISCONNECT PROCEDURE
    Select PASSIVE
  CALL REQUEST = 20
  CLEAR REQUEST = 18
  RESET REQUEST = 18
  RESTART REQUEST = 18
Select subpanel PACKET SIZE
  FRAME WINDOW SIZE = 7
  Select DEFAULT PACKET SIZE
    Select 128
  Select MAXIMUM PACKET SIZE
    Select 512
  WINDOW PACKET SIZE = 2
  Select THROUGHPUT CLASS INBOUND
    Select 2400
  Select THROUGHPUT CLASS OUTBOUND
    Select 2400
Select subpanel CHARGES 8
  DISABLE ACCEPT REVERSE CHARGES
  DISABLE REQUEST REVERSE CHARGES
Select subpanel PERFORMANCE
  DISABLE THROUGHPUT CLASS NEGOTIATION
  DISABLE FLOW CONTROL NEGOTIATION
  DISABLE DDN ADDRESS TRANSLATION

```

Figure 131 (Part 2 of 4). Scenario 1: 2210B Configuration Using Nways MRS Configuration Program

Select subpanel MAPPINGS **9**
Select PROTOCOL
Select IPX
PROTOCOL ADDRESS = 40002210A002
Select CUD Field Usage
Select STANDARD
X.25 ADDRESS = 201002600
Select ADD

Select CONFIGURATION of Serial 2
On GENERAL subpanel :
DISABLE INTERFACE **10**

On the 2210 Navigation Window:
Select X25 PER PROTOCOL CONFIGURATION ON THE DEVICES/GENERAL DIRECTORY **11**

On the X25 PER PROTOCOL CONFIGURATION Window:
Select PROTOCOL
Select IPX **12**
WINDOW SIZE = 7
Select DEFAULT PACKET SIZE
Select **512**
IDLE TIME = 30
MAX VCs = 1
Select MAXIMUM PACKET SIZE
Select **512**
Select ADD

On the 2210 Navigation Window:
Select GENERAL on the IPX directory **13**

On the IPX GENERAL Window: **14**
ENABLE IPX
DISABLE ACCESS CONTROLS
DISABLE SAP FILTERS
HOST NUMBER = 40002210B002
ROUTING TABLE SIZE = 32
SAP TABLE SIZE = 32
REMOTE CACHE SIZE = 64
LOCAL CACHE ENTRY SIZE = 64
MAXIMUM NUMBER OF ALTERNATE ROUTES = 128
MAXIMUM NUMBER OF ROUTES PER DESTINATION IPX NETWORK = 3

On the 2210 Navigation Window:
Select INTERFACES on the IPX directory **15**

On the IPX INTERFACES Window:
Select CONFIGURE of interface 0 **16**
ENABLE IPX
ENABLE IPX GNS
IPX NETWORK NUMBER = 1
Select FRAMING TYPE
Select ETHERNET 802.3

Figure 131 (Part 3 of 4). Scenario 1: 2210B Configuration Using Nways MRS Configuration Program

Select CONFIGURE of interface 1 **17**

ENABLE IPX
ENABLE IPX GNS
DISABLE WAN
IPX NETWORK NUMBER = BAD2
SAP INTERVAL = 1
RIP INTERVAL = 1
CONNECT TIME = 60
RETRY TIME = 60

On the 2210 Navigation Window:

Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION **18**

On the FILE NAME FOR CONFIGURATION DATA, PLEASE? Window:
enter **ipxx25b**
Select OK

Figure 131 (Part 4 of 4). Scenario 1: 2210B Configuration Using Nways MRS Configuration Program

Notes:

- 1** Start a new configuration.
- 2** Use Ethernet Model 12E.
- 3** Configure the Ethernet interface.
- 4** Set interface 1 to X.25.
- 5** Configure the X.25 interface.
- 6** Set the general parameters, such as the X.25 address and SVC ranges.
- 7** Set the X.25 call setup and diagnostic parameters.
- 8** Disable reverse charging, and negotiation parameters for this scenario.
- 9** Map the destination X.25 address to the IPX host number.
- 10** Disable interface 2, as it is not used in this scenario.
- 11** Select the X.25 per protocol configuration.
- 12** Add the IPX protocol to the X.25 interface.
- 13** Configure the IPX protocol.
- 14** Enable IPX globally, and set general parameters, such as the host number and RIP and SAP table sizes.
- 15** Configure IPX on the interfaces.
- 16** Configure interface 0.

- 17** Configure interface 1.
- 18** Create a router configuration file.

9.6.2 Scenario 2: Routing IPX over PPP, between an IBM 2210 and an IBM 6611 Network Processor

In this scenario, we have one IBM 2210 Model 12T, and one IBM 6611 Network Processor Model 170.

An IPX file server running NetWare Version 3.11 was on an Ethernet network attached to the IBM 6611 Network Processor Model 170.

An IPX client station was on the token-ring attached to the IBM 2210 Model 12T.

The IBM 2210 and the IBM 6611 Network Processor were connected via a PPP link.

Figure 132 is a picture of this scenario.

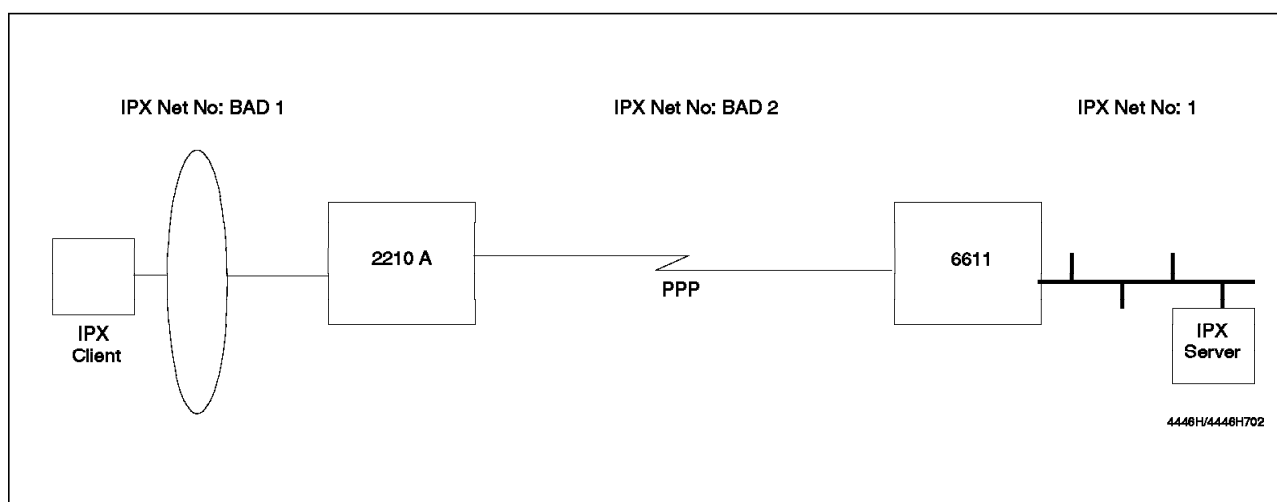


Figure 132. Scenario 2: IPX Routing between an IBM 2210 and an IBM 6611 Network Processor over PPP

Figure 133 on page 441 shows the configuration process for 2210A using the Nways MRS CONFIG process.

Figure 134 on page 444 shows the configuration process for 2210A using the Nways MRS Configuration Program.

Figure 135 on page 446 shows a part of the configuration process for the IBM 6611 Network Processor using the IBM 6611 MPNP Configuration Program. It shows only the settings relevant to this scenario.

```

*talk 6 1

Config>network 0 2
Token-Ring interface configuration
TKR config>set physical 40:00:22:10:A0:01 3
TKR config>media unshielded
TKR config>list 4
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                      4 Mb/sec
Media:                      Unshielded

RIF Aging Timer:           120
Source Routing:            Enabled
MAC Address:               40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 5
Point-to-Point user configuration
PPP Config>set hdlc cable v35 dte 6
PPP Config>list all 7

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: V.35 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

LCP Options
-----
Max Receive Unit:         2048  Magic Number:         Yes

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

IPCP Options
-----
IPCP Compression:         None
IP Address:               Don't Send or Request
PPP Config>exit

```

Figure 133 (Part 1 of 2). Scenario 2: 2210 Configuration Using Nways MRS CONFIG Process

```

Config>protocol ipx      8
IPX protocol user configuration
IPX config>enable ipx    9
IPX config>enable interface 0
IPX config>enable interface 1
IPX config>set host-number 40002210a002 10
IPX config>set net-number 0 bad1 11
IPX config>set net-number 1 bad2
IPX config>list          12

IPX globally              enabled
Host number (serial line) 40002210A002
Router Name (IPXWAN)
NodeID (IPXWAN)          0
Maximum networks          32
Maximum total alt. route entries 128
Maximum alt. routes per dest. network 3
Maximum services          32
Maximum Network Cache entries 64
Maximum Local Cache entries 64

List of configured interfaces:
      Frame
Ifc  IPX net #  Encapsulation      SAP nearest server reply  IPXWAN
0    BAD1      TOKEN-RING          MSB  Enabled              N/A
1    BAD2      N/A                  Enabled              Not Configured

RIP/SAP Timer Intervals
Net  IPX net #      SAP Interval(Minutes)  RIP Interval(Minutes)
0    BAD1           1                      1
1    BAD2           1                      1

IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.
IPX config>exit
Config>CTRL+P
*restart
Are you sure you want to restart the gateway? (Yes or -No]): y

```

Figure 133 (Part 2 of 2). Scenario 2: 2210 Configuration Using Nways MRS CONFIG Process

Notes:

- 1 Talk to the CONFIG process.
- 2 Start configuration of the token-ring interface.
- 3 In this scenario, we are using UTP on a 4 Mbps ring, and we wish to use a locally administered address.
- 4 List the token-ring configuration to ensure that everything is correct.
- 5 Start configuration of the serial interface.
- 6 Set the interface type to V.35.

- 7** List the serial interface to ensure that everything is correct.
- 8** Start configuration of the IPX protocol.
- 9** Enable IPX globally, and on the interfaces.
- 10** Set the IPX host number for the serial interfaces.
- 11** Set the IPX network numbers for each interface.
- 12** List the IPX configuration to ensure that everything is correct.

On the 2210 Navigation Window:
Select CONFIGURE from the menu bar
Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
Select MODEL
Select **MODEL 12T** **2**
Select CONFIGURE of interface 0 **3**
ENABLE INTERFACE
MAC ADDRESS = **40002210A001**
Select SPEED
Select 4
Select PACKET SIZE
Select 2052
Select CABLE TYPE
Select **UTP**
RIF TIMER = 120
DISABLE END NODE SOURCE ROUTING

Select CONFIGURE of serial interface 1 **4**
On the GENERAL subpanel
ENABLE INTERFACE
MAXIMUM TRANSMISSION UNIT = 2048
Select ENCODING
Select NRZ
Select IDLE
Select FLAG
Select CLOCKING
Select EXTERNAL
CLOCK SPEED = 0
TRANSMIT DELAY = 0
Select CABLE TYPE
Select V.35 DTE

On the 2210 Navigation Window:
Select GENERAL on the IPX directory **5**

On the IPX GENERAL Window: **6**
ENABLE **ENABLE IPX**
HOST NUMBER = **40002210A002**
ROUTING TABLE SIZE = 32
SAP TABLE SIZE = 32
REMOTE CACHE SIZE = 64
LOCAL CACHE ENTRY SIZE = 64
MAXIMUM NUMBER OF ALTERNATE ROUTES = 128
MAXIMUM NUMBER OF ROUTES PER DESTINATION IPX NETWORK = 3

Figure 134 (Part 1 of 2). Scenario 2: 2210 Configuration Using Nways MRS Configuration Program

On the 2210 Navigation Window:
 Select INTERFACES on the IPX directory **7**

On the IPX INTERFACES Window:
 Select CONFIGURE of interface 0 **8**
 ENABLE **IPX ENABLED**
 ENABLE IPX GNS ENABLED
 SAP INTERVAL = 1
 RIP INTERVAL = 1
 IPX NETWORK NUMBER = **BAD1**
 Select FRAMING TYPE
 Select **TOKEN-RING MSB**

Select CONFIGURE of interface 1 **9**
 ENABLE **IPX ENABLED**
 ENABLE IPX GNS ENABLED
 DISABLE WAN ENABLED
 IPX NETWORK NUMBER = **BAD2**
 SAP INTERVAL = 1
 RIP INTERVAL = 1
 CONNECT TIME = 60
 RETRY TIME = 60

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select CREATE ROUTER CONFIGURATION **10**

On the FILE NAME FOR CONFIGURATION DATA, PLEASE? Window:
 enter **<config.nme>**
 Select OK

Figure 134 (Part 2 of 2). Scenario 2: 2210 Configuration Using Nways MRS Configuration Program

Notes:

- 1** Start a new configuration.
- 2** Use token-ring Model 12T.
- 3** Configure the token-ring interface.
- 4** Configure the PPP interface.
- 5** Configure the IPX protocol.
- 6** Enable IPX globally, and set general parameters, such as the host number and RIP and SAP table sizes.
- 7** Configure IPX on the interfaces.
- 8** Configure interface 0.
- 9** Configure interface 1.
- 10** Create a router configuration file.

```

Select ETHERNET ADAPTER CONFIGURATION
  Enable PHYSICAL INTERFACE 1

  Enable IPX 2

  Select IPX
    IPX NETWORK NUMBER = 1 3
    ENCAPSULATION METHOD = ETHERNET 802.3
    SAP UPDATE INTERVAL = 1
    RIP UPDATE INTERVAL = 1

Select SERIAL ADAPTER CONFIGURATION

  Select PPP
    Enable PHYSICAL INTERFACE 4

    Select PHYSICAL INTERFACE CONFIGURATION
      INTERFACE CABLE = V35, V36, or EIA232 5
      TRANSMIT CLOCK SOURCE = DCE
      DATA ENCODING = NRZ 6
      LOCALLY ADMINISTERED MAC ADDRESS = 400066110001 7

    Enable PPP CONFIGURATION 8

    Enable IPX 9

    Select IPX
      IPX NETWORK NUMBER = BAD2 10
      SAP UPDATE INTERVAL = 1
      RIP UPDATE INTERVAL = 1

Select NODE CONFIGURATION
  Enable IPX 11

```

Figure 135. Scenario 2: 6611 Configuration Using IBM 6611 MPNP Configuration Program

Notes:

- 1 Enable the Ethernet interface.
- 2 Enable IPX routing on the Ethernet interface.
- 3 Configure the IPX parameters, such as network number and frame encapsulation.
- 4 Enable the serial interface.
- 5 Specify the V.35 DTE cable used for serial interface. This is required because this is not the default of the 6611.
- 6 Set to NRZ to match the IBM 2210 default.
- 7 Set the IPX host number.
- 8 Enable the PPP configuration for serial interface.
- 9 Enable IPX routing on the serial interface.

- 10** Configure the IPX parameters, such as network number, and RIP and SAP update intervals.
- 11** Enable IPX routing at the node level.

Chapter 10. Data Link Switching

This chapter provides a brief overview of Data Link Switching (DLSw), discusses configuration of Data Link Switching on the IBM 2210, and provides some configuration scenarios with the IBM 2210.

10.1 Data Link Switching Overview

DLSw is designed to facilitate integration of SNA traffic into a multiprotocol network. DLSw functions include:

- Transporting of SNA in a multiprotocol routed backbone
- Dynamic re-routing in the wide area network
- Reliable delivery of SNA traffic
- Termination of LLC acknowledgements on the LAN segments
- Broadcast traffic control through the WAN
- LAN and WAN control for congestion and data flow

DLSw uses IP encapsulation of SNA as its transport vehicle across the internetwork. To supply the reliability that SNA requires in the internetwork, DLSw uses Transmission Control Protocol (TCP) flows between edge-node routers (those routers joining the LAN segments to the IP portion of the network).

DLSw routers establish TCP connections to other DLSw routers using ports 2065 and 2067. Port 2065 is a read port on which all DLSw information is received, and port 2067 is a write port from which all DLSw information is sent.

DLSw also uses a technique known as DLC termination, or spoofing, to minimize T1 timer expirations and to keep acknowledgements isolated to the local LAN segment.

Spoofing is the process that acknowledges receipt of the frame on the local LAN segment by masquerading as the destination endstation. Spoofing keeps the receiver ready and/or supervisory poll frames from leaving their subnet media. Therefore it ensures local media response speeds to acknowledge layer 2 timers (T1 timers for example) and lessens the bandwidth overhead requirements in the WAN.

The DLSw technique is more easily understood if you consider circuit establishment between two endstations.

10.1.1 DLSw Circuit Establishment

Figure 136 on page 450 shows the configuration used in this explanation of DLSw circuit establishment.

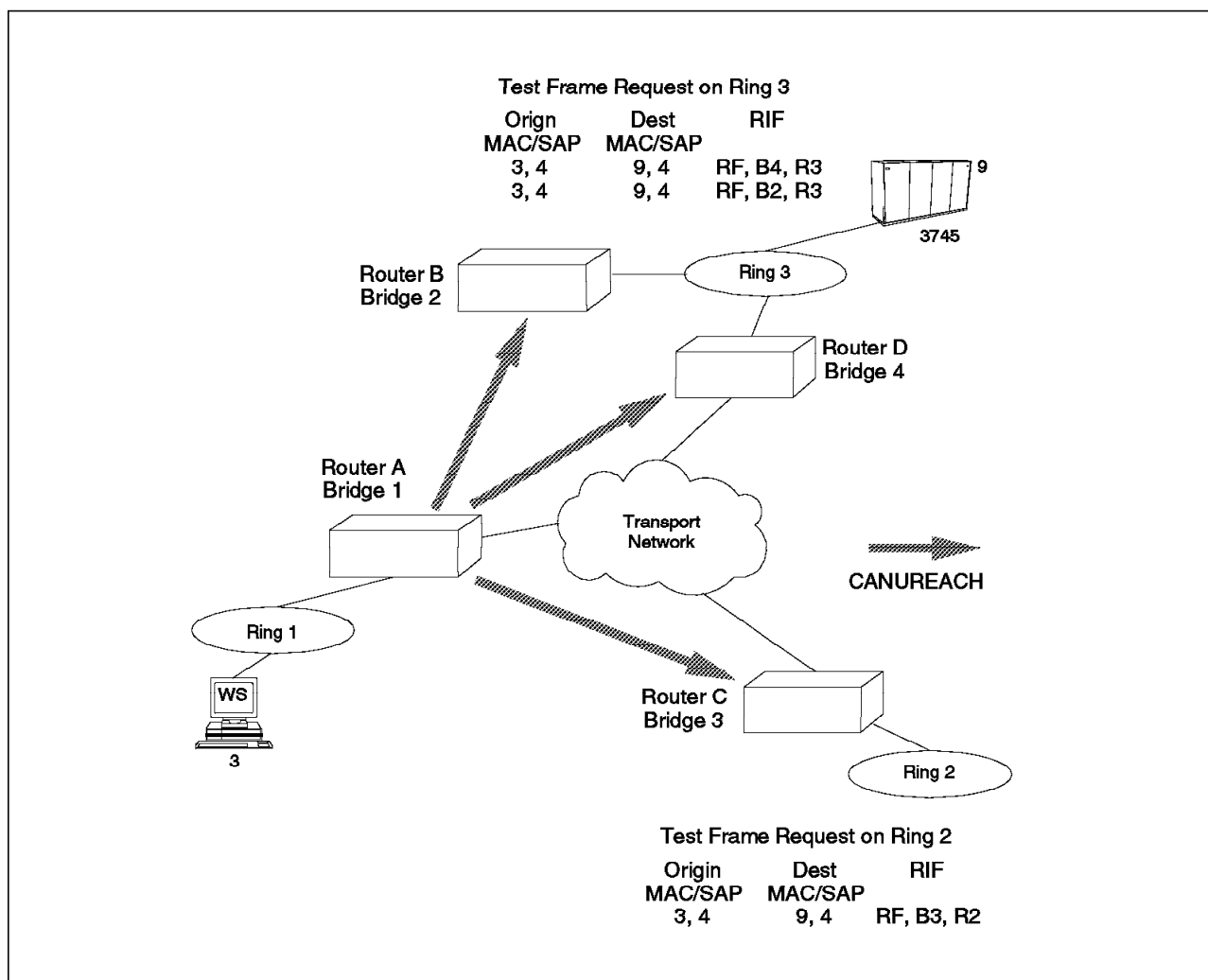


Figure 136. Circuit Establishment

An endstation (workstation 3) requests SNA connectivity to another endstation (3745) by sending out an explorer frame. This frame contains the source MAC and SAP addresses of workstation 3 and the destination MAC and SAP addresses of the 3745. When router A sees the broadcast explorer frame, the DLSw function in router A sends a CANUREACH request over the TCP/IP connections to each of the DLSw participating routers in its list. These partner routers broadcast the explorer frame on the LAN subnetworks to which they are connected. Since router B and D in this example are connected to the same LAN subnet, two explorer frames are sent to the 3745. 3745 views the data as coming from a phantom ring segment one hop beyond router B and D. This is because the RI field of the explorer frames coming from router B and D shows that the workstation 3 is on a phantom ring segment (RF) immediately on the other side of routers B and D. In effect, a 2210 with DLSw actually uses source route bridging on its LAN ports to bridge the frames into the router. However, once in the router, the DLSw code encapsulates the SNA packet in TCP packets to be routed through the IP internetwork.

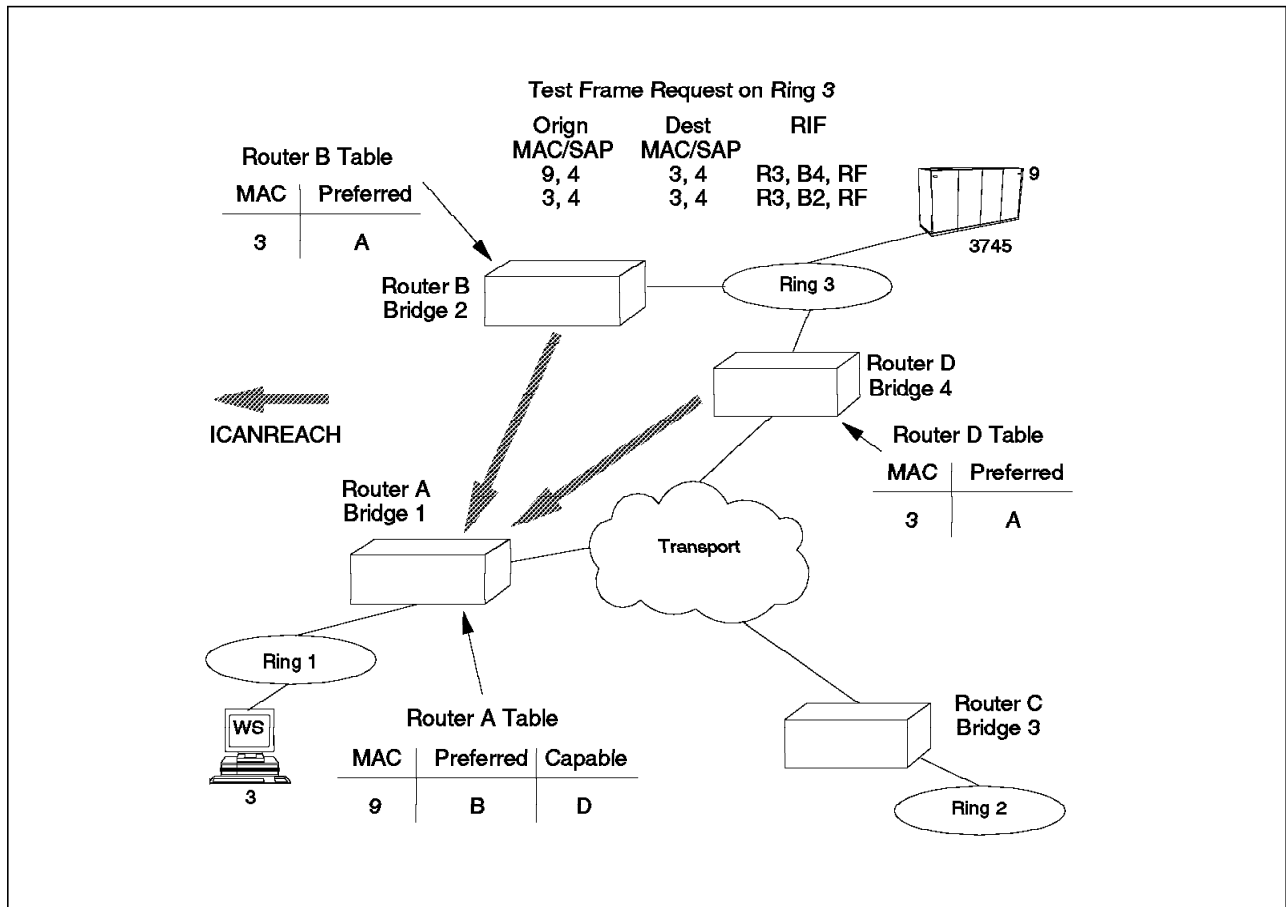


Figure 137. Circuit Establishment Completion

In Figure 137, the 3745 responds to the explorer frames. These responses are sent to routers B and D. Therefore, routers B and D both send back ICANREACH responses to router A. Routers B and D cache this information so that any future requests from workstations on their LAN ports to reach workstation 3 can be satisfied by sending a specific CANUREACH frame to router A rather than querying each of the participating router partners on the network. When router A receives the two responses to the workstation 3's explorer frame from router B and D, router A caches the first received response as the preferred router (in this case router B). Any subsequent responses from other routers (router D in this example) are cached as capable routes to use to reach the 3745. Router A now sends the explorer frame response back to the workstation, and the session setup continues.

10.2 DLSw on the IBM 2210

The DLSw function of the IBM 2210 supports the interconnection of SNA devices attached to either a LAN (token-ring or Ethernet), or an SDLC multi-point non-switched line.

As a prerequisite for DLSw, if the IBM 2210 supports LAN-attached SNA devices, it must be configured to support source route bridging on the token-ring interface, or transparent bridging on the Ethernet interface.

A DLSw virtual segment number also needs to be configured for IBM 2210s implementing DLSw. This virtual segment must be the same for all IBM 2210s

participating in the DLSw function. This is to ensure that the endstations both see the TCP/IP network as one token-ring.

SNA devices attached to an IBM 2210 via SDLC multi-point non-switched lines are each assigned a token-ring locally administered address (LAA), service access point (SAP) and SNA XID (Exchange ID). These will be used by the IBM 2210 to represent such devices to other SNA devices that are using the DLSw function as if they are attached to a token-ring LAN. SDLC-attached devices can have SNA connections with token-ring and/or Ethernet-attached devices connected to the same IBM 2210.

SNA devices attached to an IBM 2210 establish connections with SNA devices attached to other IBM 2210s as if they are on the virtual segment.

SNA devices attached to an IBM 2210 via LAN segments establish connections with SNA devices attached to the same IBM 2210 via SDLC as if they were on the virtual segment.

10.2.1 Data Link Switching Supported Topology

There are two types of data link switching:

- Local Data Link Switching
- Remote Data Link Switching

In local DLSw, the data link switching function is performed within a single IBM 2210. In remote DLSw, stations attached to two or more IBM 2210s communicate across an IP network using DLSw.

10.2.2 Local Data Link Switching

Local DLSw allows communication between a token-ring or Ethernet-attached SNA device and an SDLC secondary or primary station that is link attached to the IBM 2210.

The LAN-attached device can be locally attached to the same IBM 2210 or attached to a remote LAN which is bridged to your IBM 2210.

Each SDLC-attached device is assigned a MAC and SAP address and will appear to the other SNA devices as if it is attached to a token-ring LAN on your IBM 2210. Local DLSw converts SDLC frames to LLC2 frames. The encapsulated SDLC frames are passed to the DLSw function which will in turn use source route or transparent bridging function to deliver them to the LAN-attached device.

10.2.3 Remote Data Link Switching

SNA stations attached to an IBM 2210 via a token-ring, Ethernet or SDLC connection can establish sessions with other SNA stations which are attached to a remote IBM 2210 or IBM 6611 Network Processor via a token-ring or an Ethernet connection. The connection between the two IBM 2210s or between the IBM 2210 and the IBM 6611 Network Processor is over an IP network which can include OEM routers which support compatible IP functions such as RIP or OSPF. Note that only the two routers connected to the endstations must be enabled for DLSw. DLSw function is not required in the routers which might exist between the two edge-node routers.

The DLSw in the IBM 2210 encapsulates the SNA frames in a TCP/IP datagram and delivers the encapsulated frames to its partner over the IP network.

Remote DLSw supports:

- SDLC to LAN over WAN

SDLC frames are converted into LLC2 frames. This allows a link-attached SDLC device to communicate with a LAN (token-ring and Ethernet) attached device.

- LAN to LAN over WAN

Remote DLSw allows communication between SNA devices attached to token-ring or Ethernet networks. Remote DLSw can convert frames between the token-ring and Ethernet allowing token-ring and Ethernet-attached devices to communicate to each other using DLSw.

10.2.4 DLSw Using MOSPF

The IBM 2210 supports use of the DLSw Group Membership function to allow it to dynamically discover its DLSw partners, instead of having to manually configure the partner addresses. This feature utilizes the Multicast OSPF (MOSPF) function, which is described in 8.1.5, “MOSPF” on page 335.

The DLSw Group Membership defines two types of group:

- Client/server
- Peer-to-peer

Client/server groups have members that are designated as either a client or a server. Server routers only form DLSw connections with client routers. This group type is used for subarea SNA connections.

Peer-to-peer groups have members that are all designated peers. All members of a peer-to-peer group will form DLSw connections with all other members of the group. This group type could be used for APPC connections.

DLSw group membership will only work between routers that support it, so a combination of group membership and pre-configured DLSw partner definitions may be required in your network.

10.3 DLSw Configuration on the IBM 2210

The IBM 2210 supports DLSw over PPP, frame relay and X.25.

To configure DLSw on the IBM 2210 you can use either the Nways MRS Configuration Program or the CONFIG process of Nways MRS.

10.3.1 DLSw Configuration Commands

This section summarizes the DLSw configuration commands available within the CONFIG process of Nways MRS. To access the commands, you need to issue the following command:

```
Config>protocol dls
```

Table 68 on page 454 shows the commands available. The *Nways MRS Protocol Configuration and Monitoring Reference* covers these commands in detail.

<i>Table 68. DLSw Configuration Commands</i>	
Command	Function
? (Help)	Lists all the DLSw configuration commands, or lists the options associated with specific commands.
Add	Adds an SDLC link station, a TCP neighbor IP address, or a QLLC station or destination.
Ban	Allows access to the Boundary Access Node (BAN) configuration prompt so that BAN configuration commands can be entered.
Close-Sap	Closes a currently opened service access point (SAP). DLSw uses SAPs for communication on interfaces that support LLC.
Delete	Deletes an SDLC link station, a TCP neighbor IP address, a QLLC station or a destination.
Disable	Disables DLSw, SDLC link stations, LLC disconnect functionality, dynamic neighbors, or a QLLC station on interface.
Enable	Enables DLSw, SDLC link stations, LLC disconnect functionality, dynamic neighbors, or a QLLC station on interface.
Join-Group	Adds the router to a DLSw group, allows DLSw neighbors to dynamically find each other.
Leave-Group	Removes the router from specified DLSw group.
List	Displays information for SDLC link stations, SAPs, circuit priority, DLSw groups, DLSw global information, and QLLC destinations, stations, and interfaces. The command also provides detailed information on TCP connections.
Open-Sap	Allows DLSw to transmit data over the specified SAP. DLSw use SAPs for communication on interfaces that support LLC.
Set	Sets LLC attributes, TCP buffer size, the maximum number of DLSw sessions supported, the memory allocated to DLSw, the DLSw virtual SRB segment number, protocol timers, circuit priority, parameters for dynamic neighbors, and parameters for QLLC operations.
Exit	Exits the DLSw configuration environment and returns to the CONFIG environment.

10.3.2 DLSw Configuration Overview

In addition to the DLSw specific configuration, you will also need to configure IP and bridging. If you intend to use the DLSw group functionality, you will also have to configure OSPF.

IP is configured via the IP Config> prompt on Nways MRS, or via the Protocols/IP panels of the Nways MRS Configuration Program. If you wish to use RIP, this is configured via the IP Config> prompt on Nways MRS, or via the Protocols/IP/RIP panels of the Nways MRS Configuration Program.

If you wish to use OSPF, this is configured via the OSPF Config> prompt on Nways MRS, or via the Protocols/IP/OSPF panels of the Nways MRS Configuration Program.

Bridging is configured via the ASRT Config> prompt of Nways MRS, or via the Protocols/Bridging panels of the Nways MRS Configuration Program.

Configuration of DLSw requires you to:

- Enable DLSw.

- Set the DLSw SRB virtual segment number. (This value must be set on Ethernet models as well, and it should be the same value on all participating DLSw routers.)
- Add the TCP neighbor IP addresses, or join a DLSw group.
- Open the SAPs that you wish to be DLSw switched.
- Set the default MAC address for SDLC link stations, if required.
- Add an SDLC link station, if required.

10.3.2.1 Enabling DLSw

To enable DLSw, you need to:

- Enter DLSw Config>**enable dls**, or
- Enable DLSw on the Protocols/DLSw/General panel of the Nways MRS Configuration Program

10.3.2.2 Setting the SRB Virtual Segment Number

To set the SRB virtual segment number:

- Enter DLSw Config>**set srb**, or
- Complete the SRB Segment field on the Protocols/DLSw/General panel of the Nways MRS Configuration Program.

10.3.2.3 Adding TCP Neighbors

To add TCP neighbors:

- Enter DLSw Config>**add tcp**, or
- Complete the information on the Protocols/DLSw/TCP Connections panel of the Nways MRS Configuration Program

10.3.2.4 Joining a DLSw Group

To join a DLSw group:

- Enter DLSw Config>**join-group**, or
- Complete the information on the Protocols/DLSw/Multicast Groups panel of the Nways MRS Configuration Program

10.3.2.5 Opening SAPs for DLSw Switching

To open SAPs for DLSw switching:

- Enter DLSw Config>**open-sap**, or
- Select **Configure** for interface 0 on the Protocols/DLSw/Interfaces panel of the Nways MRS Configuration Program, and add the required SAPs.

Note: The Nways MRS Configuration Program opens SAPs 00 and 04 for the LAN interface by default.

10.3.2.6 Adding an SDLC Link Station to DLSw

To add an SDLC link station to DLSw:

- Enter DLSw Config>**add sdlc**, or
- Select **Configure** for the SDLC interface on the Protocols/DLSw/Interfaces panel of the Nways MRS Configuration Program, and complete the fields.

10.3.3 Further DLSw Configuration Considerations

The DLSw configuration process allows you to set the memory allocation for DLSw, which will probably be required if you intend to have a large number of concurrent DLSw sessions. To set the memory allocation you need to use:

- The DLSw Config>**set memory** command, or
- Complete the memory allotment fields on the Protocols/DLSw/General panel of the Nways MRS Configuration Program

To calculate the memory required for DLSw, you should take into consideration the estimated number of DLSw sessions and TCP neighbors, and the amount of memory available in the IBM 2210.

The memory required can be calculated using the following formula:

$(\text{session allocation} * \text{number of sessions} * 75\%) +$
 $(\text{number of TCP neighbors} * 512)$

For example, if you have 8192 bytes allocated per LLC session, and 4096 bytes per SDLC session, and you estimate that there will be 40 LLC DLSw sessions and 20 SDLC sessions, using two TCP neighbors, then the calculation would be:

$(8192 * 40 * 75\%) + (4096 * 20 * 75\%) + (512 * 2) = 308224 \text{ bytes}$

If many small packets are anticipated on the DLSw sessions, then the 75% value should be increased to 85%.

You are also able to limit the maximum number of DLSw sessions permitted. You do this by using:

- The DLSw Config>**set maximum** command, or
- Complete the maximum DLSw sessions field on the Protocols/DLSw/General panel of the Nways MRS Configuration Program.

10.4 DLSw Enhancements with V1R2 of Nways MRNS Software

Some new capabilities for this release of the Nways MRNS software are as follows:

- SDLC X.21 support
SDLC is now supported over X.21 links.
- PU2.0 and PU2.1 multi-drop

Support for the IBM 2210 routers for coexistence of SNA T2.0 and T2.1 link stations on SDLC multipoint lines.

Note: To mix roles among the link stations on a single SDLC link, you must configure the IBM 2210 to support whichever remote nodes do not match the default.

- On-demand vs static TCP sessions

DLSw now has the capability to automatically re-establish TCP connections after they break and upon power-up. Previously, TCP sessions were established only when they were needed for this first time (for a CANUREACH, for example) or if the DLSw Group functionality has found a neighbor.

The following new commands have been added to the DLSw configurator and console in order to implement this:

- **Enable Auto-TCP-Connection:** Allows pre-configured TCP sessions to be automatically established, and causes broken sessions to be re-established. This is the default.
- **Disable Auto-TCP-Connection:** TCP sessions are not established until DLSw needs them. TCP connections caused by DLSw groups are still created automatically. Broken TCP group connections will be re-established after the user-specified group join timer interval expires. This timer is set with the Set Timers command from the DLSw configuration or console command.

- Large frame support for SDLC relay

SDLC Relay now supports frame sizes larger than 2048 bytes, up to the maximum allowed by the device over which SDLC relay runs.

Although the router now supports the larger frame sizes, care should be taken to ensure that IP fragmentation does not occur in the IP cloud. If fragmentation does occur, performance will suffer between two routers which have reachability via multiple paths.

Note: Keep in mind that the time required to transmit larger frames over slower WAN links will lengthen the round-trip times, and this should be accounted for by lengthening the data link's response timeout values at the connected endstations.

- User-settable TCP receive buffer

The ability to set the receive buffer size is useful when communicating over networks that have a high bandwidth delay, such as a frame relay network running over a T1 line.

Note: Unless you have a reason to increase the buffer size, you should accept the default value of 4096. Setting the buffer too high will use up memory on the router.

- Configurable MAC address cache size

DLSw uses information stored in this cache to discover routes to remote stations. The larger the cache the better the chances of DLSw finding a desired remote station without sending out CANUREACH frames to all known TCP/IP neighbors.

Note: Setting this option too high will cause a reduction in router memory and in the number of DLSw sessions that can be handled by the router.

- MIB extensions

Two additional objects have been added to the `ibmdlsRouterTable`. They are `ibmdlsRouterInFrames`, which is a count of the number of frames received from the partner router, and `ibmdlsRouterOutFrames`, which is a count of the number of frames sent to the partner router.

One additional object has been added to the `ibmdlsCirTable`. The `ibmdlsCirKicakAddress` object indicates which of the source or destination MAC addresses for the circuit is local to this router.

10.5 DLSw Enhancements with V1R1 of Nways MRS Software

Recent enhancements to the DLSw function of MRS include the following:

- Multicast exploration and frame forwarding (multicast DLSw)

This is the initial implementation of enhancements to improve the scalability of DLSw to large networks. Rather than bringing up static TCP connections to configured neighbor routers, the code uses both multicast and directed UDP packets to propagate address and name resolution messages, and NetBIOS UI-frame traffic. Transport connections between multicast-capable DLSw nodes are established only on-demand, and are taken down after they are no longer needed. These scalability enhancements are compatible with back-level DLSw nodes that have no multicast IP support, and with MRNS releases that provide for MOPF-based discovery of DLSw partners.

- NetBIOS name list support

This allows a user with a structured naming convention to have more control over the broadcasting of NetBIOS datagrams. DLSw builds and sends a list of local NetBIOS names (with wildcard characters), and uses the information in received lists to minimize the number of destinations to which it sends NetBIOS SSP messages.

- APPN remote device attachment

The introduction of APPN had implications for DLSw. DLSw had an internal interface to APPN that connects APPN and endstations attached to remote routers. It does not support DLSw between locally attached APPN devices. No DLSw configuration is required to support the interface but APPN must be configured to use a specific DLS virtual interface to reach a given endstation. Please refer to *IBM 2210 Nways Multiprotocol Router*, *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios*, SG24-4956.

- DLSw acts as secondary for multiple PU types

It is now possible for the 2210 to be configured as a secondary SDLC endstation, rather than just a primary. This means that it is no longer necessary to configure the 2210 for SDLC relay (SDLC frames encapsulated in IP packets).

DLSw can support SDLC endstations that are PU types 2.0, 2.1, 4 (for NCP-NCP traffic) or 4/5 (a host or NCP performing the SNA boundary function).

For DLSw to support an SDLC interface, the configuration is done in two phases. Firstly, the SDLC interface parameters are configured. Most of the default values can be taken, but it is advisable to configure the link station name and SDLC address. Secondly, each SDLC link station must be defined from the DLSw perspective. During this process, the PU type of the link station must be defined. The options are 2, 4 or 5. If the station is either PU type 2.0 or 2.1, enter 2. These PU types are differentiated between by the next two options, which ask for SID0 block number and XID0 ID number. If the station is PU 2.1, these fields should be left as zero. If the station is PU 2.0, these fields must match the definitions in the link station's configuration.

- Poll PU 2.0 via SNRM

This allows the user to have PU 2.0 SDLC devices polled with SNRM rather than TEST frames.

- PU4 INN support

It allows PU4s on point-to-point SDLC to connect through DLSw to other PU4s on LANs, SDLC and frame relay.

- Local SDLC to SDLC support

DLSw sessions between two SDLC devices attached to the same DLSw box are now supported.

- IETF DLSw MIB Support

This DLSw implementation supports the recently approved IETF Proposed Standard MIB for DLSw. At this time, the MIB has not received an RFC number but is available on Internet-Draft directories under the name draft-ietf-dlswmib-mib-09.txt.

- LNM support

DLSw has been enhanced so that it can be used to transport LAN network manage packets. LNM had the SAP c'F4'. While this was initially introduced in V1R3 with enhancements, further improvements have been introduced. For example, with first implementation it was only possible to link remote 8230s, but not to manage them. With this release, the 8230 management function has been added.

- No-cache-aging option

The no-cache-aging option will drastically reduce the amount of DLSw-search traffics. This option is only advantageous over ISDN links where the location of the endstations is fixed. It is configured using the set timers command, and setting the first option, database age timeout, to zero. This is not generally recommended, as it disables a number of other DLSw functions.

10.6 DLSw Configuration Scenarios

The following configuration scenarios were implemented with Nways MRNS. Although there are minimal differences, refer to *IBM 2210 and 2216 N Ways Description and Configuration Scenarios - Volume II*, SG24-4956-00, for implementations using Nways MRS.

This section provides some scenarios and configurations for DLSw using the IBM 2210. Included is one scenario using the IBM 6611 Network Processor, along with the IBM 2210 to demonstrate their interoperability.

For each scenario, the configuration process using the Nways MRNS user interface is shown, along with the equivalent process using the Nways MRS Configuration Program.

The two IBM 2210s used were running Nways MRNS Version 1 Release 1, and the one IBM 6611 Network Processor used was running IBM 6611 MPNP Version 1 Release 3.

10.6.1 Scenario 1: DLSw between Two 2210s over PPP

In this scenario, we have one IBM 2210 Model 125, and one IBM 2210 Model 124. There was a CM/2 PU Type 2.0 on the Ethernet attached to the IBM 2210 Model 126, and there was a CM/2 PU Type 2.0 also attached to the IBM 2210 Model 126, via an SDLC link.

Both CM/2 stations had a session with the host that was bridged to the token-ring attached to the 2210 Model 125. Multicast OSPF was also enabled, to allow the use of the DLSw group functionality.

Figure 138 is a picture of the scenario.

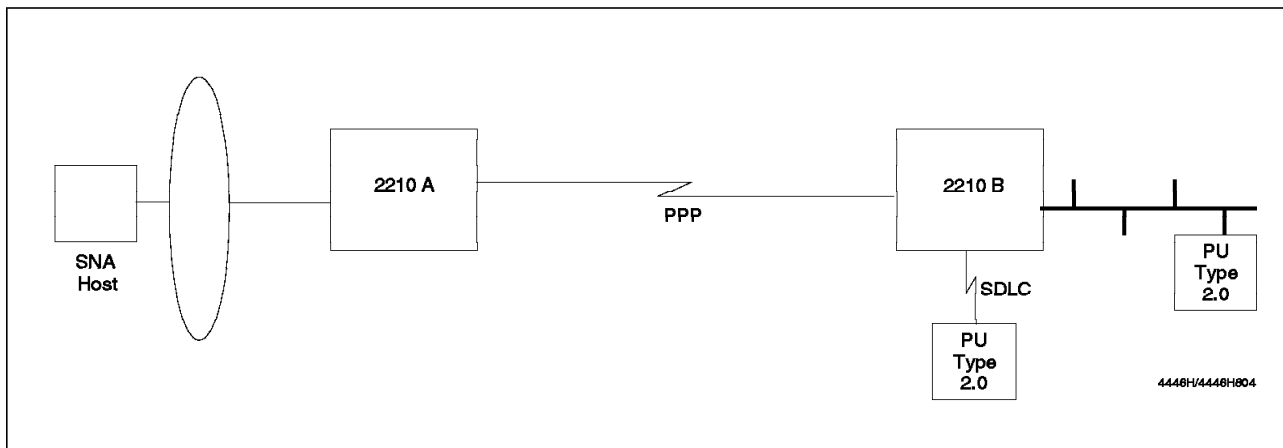


Figure 138. Scenario 1: DLSw Switching Between IBM 2210s over PPP

Figure 139 on page 461 shows the configuration process for 2210A using the Nways MRNS CONFIG process.

Figure 140 on page 466 shows the configuration process for 2210B using the Nways MRNS CONFIG process.

Figure 141 on page 474 shows the configuration process for 2210A using the Nways MRS Configuration Program.

Figure 142 on page 479 shows the configuration process for 2210B using the Nways MRS Configuration Program.

```

*talk 6 1

Config>network 0 2
Token-Ring interface configuration
TKR config>media unshielded 3
TKR config>set physical 40:00:22:10:A0:01
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                     4 Mb/sec
Media:                     Unshielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 4
Point-to-Point user configuration
PPP Config>set hdlc cable v35 dte 5
PPP Config>list all

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: V.35 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit

```

Figure 139 (Part 1 of 4). Scenario 1: 2210A Nways MRNS Configuration

```

Config>disable interface 2 6
Config>protocol ip 7
Internet protocol user configuration
IP config>add address 8
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.131
Address mask [255.0.0.0]? 255.255.255.240
IP config>list all 9
Interface addresses
IP addresses for each interface:
    intf 0                                IP disabled on this interface
    intf 1    9.67.46.131        255.255.255.240    Network broadcast,    fill 0
    intf 2                                IP disabled on this interface

Routing

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled

IP config>exit
Config>protocol ospf 10
Open SPF-Based Routing Protocol configuration console
OSPF Config>enable ospf 11
Estimated # external routes [0]? 20
Estimated # OSPF routers [0]? 20
OSPF Config>set interface 12
Interface IP address [0.0.0.0]? 9.67.46.131
Attaches to area [0.0.0.0]? 0.0.0.0
Retransmission Interval (in seconds) [5]? 5
Transmission Delay (in seconds) [1]? 1
Router Priority [1]? 1
Hello Interval (in seconds) [10]? 10
Dead Router Interval (in seconds) [40]? 40
Type Of Service 0 cost [1]? 1
Authentication Key []?
Retype Auth. Key []?
OSPF Config>enable multicast 13
Inter-area multicasting enabled? [No]: no

```

Figure 139 (Part 2 of 4). Scenario 1: 2210A Nways MRNS Configuration

```

OSPF Config>list all 14

--Global configuration--
  OSPF Protocol:      Enabled
  # AS ext. routes:   20
  Estimated # routers: 20
  External comparison: Type 2
  AS boundary capability: Disabled
  Multicast forwarding: Enabled
  Inter-area multicast: Disabled
  Inter-AS multicast:  Disabled

--Area configuration--
Area ID      AuType      Stub? Default-cost Import-summaries?
0.0.0.0      0=None      No      N/A      N/A

--Interface configuration--
IP address    Area      Cost Rtrns TrnsDly Pri Hello Dead
9.67.46.131   0.0.0.0      1     5     1     1    10   40

Multicast parameters
IP address    MCForward DLUnicast IGMPPoll IGMPtimeout
9.67.46.131   On        Off       60      180

OSPF Config>exit
Config>protocol asrt 15
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 16
ASRT config>disable transparent 1
ASRT config>enable source-routing 1 ffb 1
ASRT config>enable dls 17
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 1        No. of Source routing segments: 1
SRB: Max ARE Hop cnt: 14               Max STE Hop cnt: 14
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED    FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: ENABLED
Number of ports added: 1
Port Number: 1   Interface Number: 0 Port Behaviour: SRB Only

ASRT config>exit
Config>protocol dls 18
DLSw protocol user configuration
DLSw config>enable dls 19
DLSw config>set srb aaa 20

```

Figure 139 (Part 3 of 4). Scenario 1: 2210A Nways MRNS Configuration

```

DLSw config>join-group 21
Group ID (1-64 Decimal) [1]? 1
Client/Server or Peer Group Member(C/S/P)- [C]? S 22
Transmit Buffer Size (Decimal) [5120]? 5120
Maximum Segment Size (Decimal) [1024]? 1024
Enable/Disable Keepalive?(E/D)- [D]? e
DLSw config>open-sap 0 00 23
DLSw config>open-sap 0 04
DLSw config>exit
Config>CTRL+P
*restart
Are you sure you want to restart the gateway? (Yes or [No]): y

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 24

CGW Operator Console

+protocol dls 25
Data Link Switching Console
DLSw>list tcp sessions 26
  Group      IP Address  Conn State  Pkts Sent  Pkts Rcvd  Bytes Sent  Bytes Rcvd
-----
1  Svr1      9.67.46.130  ESTABLISHED    945         54      86706      2836
DLSw>list dls sessions all 27
      Source      Destination      State      Flags      Dest IP Addr      Id
-----
1  400030000001 04  000000000000 04  CONNECTED      9.67.46.130      243
2  400030000001 04  08005A415A56 04  CONNECTED      9.67.46.130      198
DLSw>list dls sessions detail 198 28
      Source      Destination      State      Flags      Dest IP Addr      Id
-----
0  400030000001 04  08005A415A56 04  CONNECTED      9.67.46.130      198

  Personality:      TARGET
  XIDs sent:         4
  XIDs rcvd:         5
  Datagrams sent:    0
  Datagrams rcvd:    0
  Info frames sent:  19
  Info frames rcvd:  21
  RIF:               0E21 AAA1 FFBF 5827 581D C31C 5D10

```

Figure 139 (Part 4 of 4). Scenario 1: 2210A Nways MRNS Configuration

Notes:

- 1 Talk to the CONFIG process.

- 2** Start customization of the token-ring interface.
- 3** In this scenario, we are using UTP on a 4 MBps ring, and we wish to use a locally administered address.
- 4** Start customization of the PPP interface.
- 5** Set the cable type to V.35.
- 6** Disable interface 2 as it is not used in this scenario.
- 7** Start customization of IP.
- 8** Add an IP address for interface 1.
- 9** List the IP configuration to ensure that everything is correct.
- 10** Start customization of OSPF.
- 11** Enable OSPF.
- 12** Enable OSPF on interface 1.
- 13** Enable MOSPF for use with the DLSw groups.
- 14** List the OSPF configuration to ensure that everything is correct.
- 15** Start customization of bridging.
- 16** Enable the bridge, and set interface 0 (port 1) to SRB mode.
- 17** Enable DLSw on the bridge.
- 18** Start customization of DLSw.
- 19** Enable DLSw.
- 20** Set the DLSw virtual segment number.
- 21** Join DLSw group number 1.
- 22** Join the group as a server.
- 23** Open the 00 and 04 SAPs for DLSw switching.
- 24** Talk to the GWCON process.
- 25** Talk to the DLSw process.
- 26** List the TCP sessions. In this scenario, we have just one TCP session, and it is established.
- 27** List the DLSw sessions. In this scenario we have two DLSw sessions; one for SDLC and one for Ethernet. They have both been successfully connected.
- 28** List the detail for the DLSw session ID 198.

```

*talk 6 1

Config>network 0 2
Ethernet interface configuration
ETH config>list
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:       ETHER

ETH config>exit
Config>network 1 3
Point-to-Point user configuration
PPP Config>set hdlc cable v35 dte 4
PPP Config>list all 5

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: V.35 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:             2048   Magic Number:             Yes

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

IPCP Options
-----
IPCP Compression:             None
IP Address:                   Don't Send or Request
PPP Config>exit

```

Figure 140 (Part 1 of 6). Scenario 1: 2210B Nways MRNS Configuration


```

Config>set data sdlc 2 6
Config>network 2 7
SDLC user configuration
Creating a default configuration for this link
SDLC 2 Config>set link type multipoint 8
SDLC 2 Config>set link cable rs-232 dte
SDLC 2 Config>list link 9
Link configuration for: LINK_2 (ENABLED)

Role:          PRIMARY          Type:          MULTIPOINT
Duplex:        FULL             Modulo:        8
Idle state:    FLAG             Encoding:      NRZ
Clocking:      EXTERNAL         Frame Size:    2048
Speed:         0                Cable:         RS-232 DTE

Timers:  XID/TEST response: 2.0 sec
         SNRM response:    2.0 sec
         Poll response:    0.5 sec
         Inter-poll delay: 0.2 sec
         RTS hold delay:   DISABLED
         Inter-frame delay: DISABLED

Counters: XID/TEST retry: 4
          SNRM retry:    6
          Poll retry:    10
SDLC 2 Config>add remote-secondary 10
Enter station address (in hex) [C1]? c1
Enter remote station name [SDLC_C1]? wtr33350
Enter max packet size [2048]? 1024
Enter receive window [7]? 7
Enter transmit window [7]? 7
SDLC 2 Config>list remote-secondary wtr33350 11

Address   Name       Status   Max BTU  Rx Window  Tx Window
-----
C1        WTR33350   ENABLED   1024     7          7
SDLC 2 Config>exit
Config>protocol ip 12
Internet protocol user configuration
IP config>add address 13
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.130
Address mask [255.0.0.0]? 255.255.255.240

```

Figure 140 (Part 2 of 6). Scenario 1: 2210B Nways MRNS Configuration

```

IP config>list all 14
Interface addresses
IP addresses for each interface:
    intf 0                                IP disabled on this interface
    intf 1    9.67.46.131        255.255.255.240    Network broadcast,    fill 0
    intf 2                                IP disabled on this interface

Routing

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled
IP config>exit
Config>protocol ospf 15
Open SPF-Based Routing Protocol configuration console
OSPF Config>enable ospf 16
Estimated # external routes [0]? 20
Estimated # OSPF routers [0]? 20
OSPF Config>set interface 17
Interface IP address [0.0.0.0]? 9.67.46.130
Attaches to area [0.0.0.0]? 0.0.0.0
Retransmission Interval (in seconds) [5]? 5
Transmission Delay (in seconds) [1]? 1
Router Priority [1]? 1
Hello Interval (in seconds) [10]? 10
Dead Router Interval (in seconds) [40]? 40
Type Of Service 0 cost [1]? 1
Authentication Key []?
Retype Auth. Key []?
OSPF Config>enable multicast forwarding 18
Inter-area multicasting enabled? [No]: no

```

Figure 140 (Part 3 of 6). Scenario 1: 2210B Nways MRNS Configuration

```

OSPF Config>list all 19

--Global configuration--
  OSPF Protocol:      Enabled
  # AS ext. routes:   20
  Estimated # routers: 20
  External comparison: Type 2
  AS boundary capability: Disabled
  Multicast forwarding: Enabled
  Inter-area multicast: Disabled
  Inter-AS multicast:  Disabled

--Area configuration--
Area ID      AuType      Stub? Default-cost Import-summaries?
0.0.0.0      0=None      No      N/A      N/A

--Interface configuration--
IP address    Area      Cost Rtrns TrnsDly Pri Hello Dead
9.67.46.131   0.0.0.0      1     5     1     1    10   40

Multicast parameters
IP address    MCForward DUnicast IGMPPoll IGMPTimeout
9.67.46.131   On        Off      60      180

OSPF Config>exit
Config>protocol asrt 20
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 21
ASRT config>enable dls 22
ASRT config>list bridge 23

Source Routing Transparent Bridge Configuration
=====

Bridge:  ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: ENABLED
Number of ports added: 1
Port Number: 1 Interface Number: 0 Port Behaviour: STB Only

ASRT config>exit
Config>protocol dls 24
DLSw protocol user configuration
DLSw config>enable dls 25
DLSw config>set srb aaa 26

```

Figure 140 (Part 4 of 6). Scenario 1: 2210B Nways MRNS Configuration

```

DLSw config>join-group 27
Group ID (1-64 Decimal) [1]? 1
Client/Server or Peer Group Member(C/S/P)- [C]? c 28
Transmit Buffer Size (Decimal) [5120]? 5120
Maximum Segment Size (Decimal) [1024]? 1024
Enable/Disable Keepalive?(E/D)- [D]? e
DLSw config>add sdlc 29
Interface # [0]? 2
SDLC Address [C1]? c1
Source MAC Address [000000000000]? 400000033350
Idblk in Hex (0-0xfff) [0]? 05d
Idnum in Hex (0-0xfffff) [0]? 33350
LLC Source SAP (0 for auto-assign) [0]? 0
LLC Destination SAP [4]? 4
Destination MAC Address [000000000000]? 400030000001
DLSw config>list sdlc 30
Interface #, or 'ALL' [0]? 2
SDLC Address [C1]? c1

Interface:      2
Link Address: C1

State:      Enabled
Idblk:      05D
Idnum:      33350
Src SAP:    AUTO
Dest SAP:    04
Src MAC:    40:00:00:03:33:50
Dest MAC:    40:00:30:00:00:01

DLSw config>open-sap 0 00 31
DLSw config>open-sap 0 04
DLSw config>list dls global 32
DLSw is                ENABLED
LLC2 send Disconnect is  ENABLED

SRB Segment number      AAA
Max DLSw sessions       1000
DLSw global memory allotment 153344
LLC per-session memory allotment 8192
SDLC per-session memory allotment 4096

DLSw MAC Address        40:00:00:03:33:50

Database age timer      1200 seconds
Age timer resolution    300 seconds
Max wait timer for ICANREACH 20 seconds
Wait timer for LLC test response 15 seconds
Wait timer for SDLC test response 15 seconds
Join Group Interval     900 seconds
DLSw config>exit

```

Figure 140 (Part 5 of 6). Scenario 1: 2210B Nways MRNS Configuration

```

Config>CTRL+P
*restart
Are you sure you want to restart the gateway? (Yes or [No]): y

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5
33

+protocol dls
34
Data Link Switching Console
DLSw>list tcp sessions
35
  Group      IP Address  Conn State  Pkts Sent  Pkts Rcvd  Bytes Sent  Bytes Rcvd
-----
1 CInt 1     9.67.46.131 ESTABLISHED      50        486        2772        47528
DLSw>list dls sessions all
36
  Source      Destination  State  Flags  Dest IP Addr  Id
-----
1 000000000000 04 400030000001 04 CONNECTED      9.67.46.131  18
2 08005A415A56 04 400030000001 04 CONNECTED      9.67.46.131  347
DLSw>list dls sessions detail 18
37
  Source      Destination  State  Flags  Dest IP Addr  Id
-----
0 000000000000 04 400030000001 04 CONNECTED      9.67.46.131  18

  Personality:  ORIGINATOR
  XIDs sent:    2
  XIDs rcvd:    1
  Datagrams sent: 0
  Datagrams rcvd: 0
  Info frames sent: 18
  Info frames rcvd: 16
  RIF:
DLSw>list sdlc sessions
38
  Net  Addr  Src Sap  Dst Sap  Dest MAC  OutQ  State
1. 2    C1    04      04      40:00:30:00:00:01  00  CONTACTED

```

Figure 140 (Part 6 of 6). Scenario 1: 2210B Nways MRNS Configuration

Notes:

- 1 Talk to the CONFIG process.
- 2 Start the customization of the Ethernet interface.
- 3 Start the customization of the PPP interface.
- 4 Set the cable type to V.35.
- 5 List the PPP interface to check that everything is correct.
- 6 Set the data link for interface 2 to SDLC.
- 7 Start the customization of the SDLC interface.

- 8** Set the SDLC link to a multipoint one, using an RS-232 cable.
- 9** List the SDLC link to check that everything is correct.
- 10** Add a remote SDLC device. In this scenario, the remote device has an address of C1 and a maximum packet size of 1024 bytes.
- 11** List the SDLC secondary device to check that everything is correct.
- 12** Start the customization of IP.
- 13** Add an IP address for the PPP interface.
- 14** List the IP configuration to check that everything is correct.
- 15** Start the customization of OSPF.
- 16** Enable OSPF.
- 17** Enable OSPF on the PPP interface.
- 18** Enable MOSPF, for use with the DLSw groups.
- 19** List the OSPF configuration to ensure that everything is correct.
- 20** Start the customization of bridging.
- 21** Enable bridging.
- 22** Enable DLSw for the bridge.
- 23** List the bridge to ensure that everything is correct.
- 24** Start the customization of DLSw.
- 25** Enable DLSw.
- 26** Set the DLSw virtual segment number.
- 27** Join DLSw group number 1.
- 28** Join the group as a client.
- 29** Add an SDLC device to DLSw. In this scenario, interface 2 is the SDLC link and the remote device has the address C1; the source MAC address, IDBLK and IDNUM values are as coded at the host, and we are auto-assigning the SAP to be used by the device.
- 30** List the SDLC device to ensure that everything is correct.
- 31** Open the 00 and 04 SAPs for DLSw switching.
- 32** List the DLSw configuration to ensure that everything is correct.
- 33** Talk to the GWCON process.
- 34** Access the DLSw monitoring commands.

35 List the TCP sessions. In this scenario we have just one TCP session and it is established.

36 List the DLSw sessions. In this scenario we have two DLSw sessions; one for SDLC and one for Ethernet. They are both successfully connected.

37 List the detail for DLSw session ID 18.

38 List the SDLC DLSw sessions.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 125** **2**
 Select CONFIGURE of interface 0 **3**
 ENABLE INTERFACE
 MAC ADDRESS = **40002210A001**
 Select SPEED
 Select 4
 Select PACKET SIZE
 Select 2052
 Select CABLE TYPE
 Select **UTP**
 RIF TIMER = 120
 DISABLE END NODE SOURCE ROUTING

Select the data-link protocol of Serial 1 (PPP by default)
 Select PPP

Select CONFIGURATION of Serial 1 **4**
 On GENERAL subpanel :
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select **V.35 DTE**
 Select subpanel LCP
 RETRY TIMER = 3000
 CONFIG TRIES = 20
 NAK TRIES = 10
 TERMINATE TRIES = 10
 MAXIMUM RECEIVE UNIT = 2048
 Select subpanel BNCP
 ENABLE MAGIC NUMBER
 DISABLE TINYGRAM COMPRESSION
 Select subpanel IPCP
 DISABLE IP Compression
 Number of Slots = 16
 DISABLE SEND IP ADDRESS
 DISABLE REQUEST IP ADDRESS
 Select CONFIGURATION of Serial 2
 On GENERAL subpanel :
DISABLE INTERFACE **5**

Figure 141 (Part 1 of 4). Scenario 1: 2210A Configuration Using Nways MRS Configuration Program

On the 2210 Navigation Window:
Select GENERAL on the IP directory

On the IP GENERAL Window:

ENABLE IP **6**
DISABLE ACCESS CONTROL
ENABLE DIRECTED-BROADCAST
INTERNAL ADDRESS = **9.67.46.131**
ROUTING TABLE SIZE = 768
CACHE SIZE = 64

On the 2210 Navigation Window:
Select INTERFACES on the IP directory

On the IP INTERFACES Window:

Select IP ADDRESSES for interface 1 **7**
IP ADDRESS = **9.67.46.131**
SUBNET MASK = **255.255.255.240**
select **ADD**

On the 2210 Navigation Window:
Select GENERAL on the OSPF directory

On the OSPF GENERAL window:

ENABLE OSPF **8**
DISABLE PER-PACKET-MULTIPATH
NUMBER OF EXTERNAL ROUTES = 20
NUMBER OF OSPF ROUTERS = 20

On the 2210 Navigation Window:
Select IP MULTICAST on the OSPF directory

On the OSPF MULTICAST Window:

ENABLE MULTICAST **9**
DISABLE INTER-AS MULTICASTING

On the 2210 Navigation Window:
Select AREA CONFIGURATION on the OSPF directory

On the OSPF AREA CONFIGURATION Window:

On the GENERAL subpanel:
AREA = 0.0.0.0 **10**
AUTHENTICATION TYPE = 00
SELECT **ADD**

Figure 141 (Part 2 of 4). Scenario 1: 2210A Configuration Using Nways MRS Configuration Program

On the 2210 Navigation Window:
 Select INTERFACES on the OSPF directory
 On the OSPF INTERFACES GENERAL Window:
 Select CONFIGURE of interface 1 **11**
 On the MULTICAST EXT subpanel
 ENABLE OSPF **12**
 ENABLE MULTICAST
 DISABLE FORW/REC AS UNICAST
 COST = 1
 PRIORITY = 1
 IGMP POLLING INTERVAL = 60
 IGMP TIMEOUT 180
 Select AREA NUMBER
 Select 0.0.0.0
 AUTHENTICATION KEY = 0
 Select subpanel TIMERS
 RETRANS INTERVAL = 5
 HELLO INTERVAL = 10
 TRANSMISSION DELAY = 1
 DEAD ROUTER INTERVAL = 40

On 2210 Navigation Window :
 Select GENERAL on the DLSw directory

On 2210 DLSw General Window :
 ENABLE DLSw **13**
 SRB SEGMENT = aaa

On 2210 Navigation Window :
 Select MULTICAST GROUPS on the DLSw directory

On 2210 DLSw Multicast Groups Window :
 GROUP ID = 1 **14**
 ROLE = SERVER
 TRANSMIT BUFFER SIZE = 5120
 MAXIMUM SEGMENT SIZE = 1024
 ENABLE KEEPALIVE
 SELECT **ADD**

On 2210 Navigation Window :
 Select BRIDGING - GENERAL panel of BRIDGING directory
 On BRIDGING - GENERAL Window :
 ENABLE BRIDGING **15**
 ENABLE DLSw

In SOURCE ROUTING BRIDGE box
 BRIDGE NUMBER = 1
 MAXIMUM ARE HOP COUNT = 14
 MAXIMUM STE HOP COUNT = 14
 INTERNAL VIRTUAL SEGMENT = 1
 Select LF BIT INTERPRETATION
 Select EXTENDED
 ENABLE FA-GA

Figure 141 (Part 3 of 4). Scenario 1: 2210A Configuration Using Nways MRS Configuration Program

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE Token-Ring **16**
Select CONFIGURE of Token-Ring
Select INTERFACE SUPPORTS
Select **SRB** **17**
Select DUPLICATE FRAMES
Select STE&TSF
SEGMENT NUMBER = **FFB** **18**
MTU UNIT = 4399
ENABLE STE

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION **19**

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter **d1spppa**
Select OK

Figure 141 (Part 4 of 4). Scenario 1: 2210A Configuration Using Nways MRS Configuration Program

Notes:

- 1** Start a new configuration.
- 2** Use Model 125.
- 3** Configure the token-ring interface.
- 4** Configure the PPP interface.
- 5** Disable interface 2 as it is not used in this scenario.
- 6** Enable IP and set the internal IP address.
- 7** Set the IP address for interface 1.
- 8** Enable OSPF.
- 9** Enable MOSPF.
- 10** Add area 0.0.0.0 to the OSPF configuration.
- 11** Configure OSPF on interface 1.
- 12** Enable OSPF and MOSPF on interface 1.
- 13** Enable DLSw and set the virtual segment number.
- 14** Add this router to DLSw group number 1 as a server.
- 15** Enable bridging and DLSw on the bridge.
- 16** Enable bridging on the token-ring.

- 17** Set the bridging method to SRB.
- 18** Set the segment number for this token-ring.
- 19** Create a router configuration file.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 126** **2**
 Select CONFIGURE of interface 0 **3**
 ENABLE INTERFACE
 Select CONNECTOR TYPE
 Select **AUTO-CONFIG**

Select CONFIGURE of Serial 1 **4**
 On GENERAL subpanel :
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select **V.35 DTE**
 Select subpanel LCP
 RETRY TIMER = 3000
 CONFIG TRIES = 20
 NAK TRIES = 10
 TERMINATE TRIES = 10
 MAXIMUM RECEIVE UNIT = 2048
 Select subpanel BNCP
 ENABLE MAGIC NUMBER
 DISABLE TINYGRAM COMPRESSION
 Select subpanel IPCP
 DISABLE IP Compression
 Number of Slots = 16
 DISABLE SEND IP ADDRESS
 DISABLE REQUEST IP ADDRESS

Figure 142 (Part 1 of 5). Scenario 1: 2210B Nways MRS Configuration Program Configuration

Select the data-link protocol of Serial 2 (PPP by default)

Select **SDLC** **5**

Select CONFIGURE of Serial 2 **6**

On GENERAL subpanel :

ENABLE INTERFACE

MAXIMUM TRANSMISSION UNIT = 2048

Select ENCODING

Select NRZ

Select IDLE

Select FLAG

Select CLOCKING

Select EXTERNAL

CLOCK SPEED = 0

TRANSMIT DELAY = 0

Select CABLE TYPE

Select RS-232 DTE **7**

On DETAIL subpanel : **8**

ENABLE LINK

LINK NAME = LINK0001

Select ROLE

Select PRIMARY

Select TYPE

Select **MULTIPOINT**

Select DUPLEX

Select FULL

Select MODULO

Select 8

XID TIMEOUT = 2000

XID RETRY = 4

SNRM TIMEOUT = 2000

SNRM RETRY = 6

RTS HOLD = 0

On REMOTE SEC subpanel : **9**

ENABLE REMOTE SECONDARY

ADDRESS = C1

RECEIVE WINDOW SIZE = 7

TRANSMIT WINDOW SIZE = 7

NAME = WTR33350

PACKET SIZE = 1024

Select **ADD**

On the 2210 Navigation Window:

Select GENERAL on the IP directory

On the IP GENERAL Window:

ENABLE IP **10**

DISABLE ACCESS CONTROL

ENABLE DIRECTED-BROADCAST

INTERNAL ADDRESS = **9.67.46.130**

ROUTING TABLE SIZE = 768

CACHE SIZE = 64

Figure 142 (Part 2 of 5). Scenario 1: 2210B Nways MRS Configuration Program Configuration

On the 2210 Navigation Window:
 Select INTERFACES on the IP directory

On the IP INTERFACES Window:
 Select IP ADDRESSES for interface 1 **11**
 IP ADDRESS = **9.67.46.130**
 SUBNET MASK = **255.255.255.240**
 select **ADD**

On the 2210 Navigation Window:
 Select GENERAL on the OSPF directory

On the OSPF GENERAL window:
ENABLE OSPF **12**
 DISABLE PER-PACKET-MULTIPATH
NUMBER OF EXTERNAL ROUTES = 20
NUMBER OF OSPF ROUTERS = 20

On the 2210 Navigation Window:
 Select IP MULTICAST on the OSPF directory

On the OSPF MULTICAST Window:
ENABLE MULTICAST **13**
 DISABLE INTER-AS MULTICASTING

On the 2210 Navigation Window:
 Select AREA CONFIGURATION on the OSPF directory

On the OSPF AREA CONFIGURATION Window:
 On the GENERAL subpanel:
 AREA = 0.0.0.0 **14**
 AUTHENTICATION TYPE = 00
 SELECT **ADD**

On the 2210 Navigation Window:
 Select INTERFACES on the OSPF directory

On the OSPF INTERFACES GENERAL Window:
 Select CONFIGURE of interface 1 **15**
 On the MULTICAST EXT subpanel
ENABLE OSPF **16**
ENABLE MULTICAST
 DISABLE FORW/REC AS UNICAST
 COST = 1
 PRIORITY = 1
 IGMP POLLING INTERVAL = 60
 IGMP TIMEOUT 180
 Select AREA NUMBER
 Select 0.0.0.0
 AUTHENTICATION KEY = 0
 Select subpanel TIMERS
 RETRANS INTERVAL = 5
 HELLO INTERVAL = 10
 TRANSMISSION DELAY = 1
 DEAD ROUTER INTERVAL = 40

Figure 142 (Part 3 of 5). Scenario 1: 2210B Nways MRS Configuration Program Configuration

On 2210 Navigation Window :
Select GENERAL on the DLSw directory

On 2210 DLSw General Window :
ENABLE DLSw **17**
SRB SEGMENT = aaa
DLSw MAC ADDRESS = 400000033350

On 2210 Navigation Window :
Select MULTICAST GROUPS on the DLSw directory

On 2210 DLSw Multicast Groups Window :
GROUP ID = 1 **18**
ROLE = CLIENT
TRANSMIT BUFFER SIZE = 5120
MAXIMUM SEGMENT SIZE = 1024
ENABLE KEEPALIVE
SELECT **ADD**

On 2210 Navigation Window :
Select INTERFACES on the DLSw directory

On the DLSw INTERFACES Window:
Select CONFIGURE of Interface 2 **19**
SOURCE MAC ADDRESS = 000000000000
DESTINATION MAC ADDRESS = 400030000001
ID BLOCK = 05D
ID NUMBER = 33350
LINK ADDRESS = C1
DESTINATION SAP = 4
SOURCE SAP = 0
ENABLE SDLC ADDRESS
Select **ADD**

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING **20**
ENABLE DLSw

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE Ethernet **21**
Select CONFIGURE of Ethernet
Select INTERFACE SUPPORTS
Select **STB** **22**
Select DUPLICATE FRAMES
Select STE&TSF

Figure 142 (Part 4 of 5). Scenario 1: 2210B Nways MRS Configuration Program Configuration

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
Select CREATE ROUTER CONFIGURATION **23**

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter **d1spppb**
Select OK

Figure 142 (Part 5 of 5). Scenario 1: 2210B Nways MRS Configuration Program Configuration

Notes:

- 1** Start a new configuration.
- 2** Use Ethernet Model 126.
- 3** Configure the Ethernet interface.
- 4** Configure the PPP interface.
- 5** Set the data link for interface 2 to SDLC.
- 6** Configure the SDLC interface.
- 7** Set the cable type for the SDLC interface.
- 8** Configure the SDLC link.
- 9** Configure the SDLC secondary device.
- 10** Enable IP and set the internal IP address.
- 11** Add an IP address to interface 1.
- 12** Enable OSPF.
- 13** Enable MOSPF.
- 14** Add area 0.0.0.0 to the OSPF configuration.
- 15** Configure OSPF on interface 1.
- 16** Enable OSPF and MOSPF on interface 1.
- 17** Enable DLSw, set the virtual segment number, and set a default MAC address for SDLC stations.
- 18** Add this router to DLSw group number 1 as a client.
- 19** Add the SDLC device configuration to DLSw.
- 20** Enable bridging and DLSw on the bridge.
- 21** Enable bridging on the ethernet.
- 22** Set the bridging method to STB.

23 Create a router configuration file.

10.6.2 Scenario 2: DLSw between Two 2210s and 6611 over Frame Relay

In this scenario, we have one IBM 2210 Model 125, one IBM 2210 Model 126, and one IBM 6611 Network Processor Model 170. There was a CM/2 PU Type 2.0 on the Ethernet attached to the IBM 2210 Model 126, and there was a CM/2 PU Type 2.1 attached to the IBM 2210 Model 125, via an SDLC link.

An SNA host and another CM/2 PU Type 2.1 were attached via token-ring to the IBM 6611 Network Processor.

The two IBM 2210s and the IBM 6611 Network Processor were connected via a fully meshed frame relay network.

The CM/2 PU Type 2.0 was successfully connected to the SNA host, and the two CM/2 PU Type 2.1s successfully established communications.

Figure 143 is a picture of the scenario.

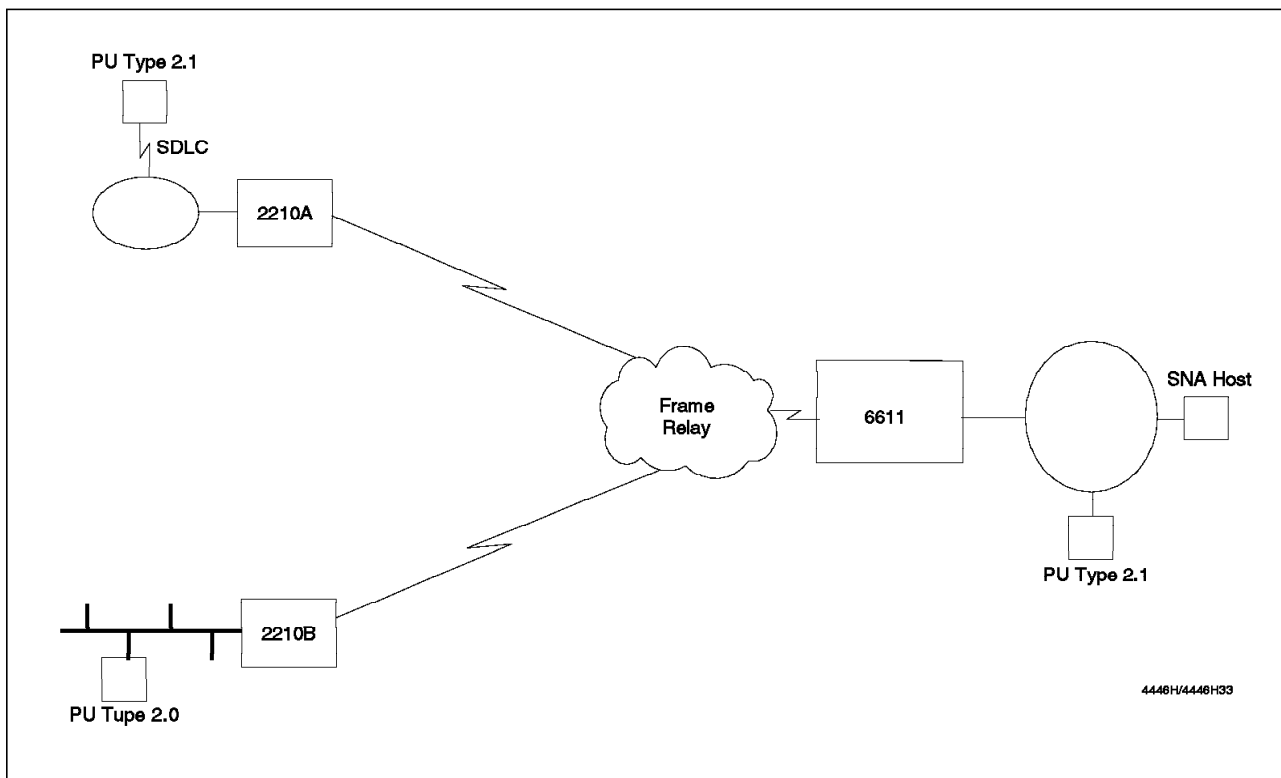


Figure 143. Scenario 2: DLSw Switching between IBM 2210s and an IBM 6611 Network Processor over Frame Relay

Figure 144 on page 486 shows the configuration process for 2210A using the Nways MRNS CONFIG process.

Figure 145 on page 493 shows the configuration process for 2210B using the Nways MRNS CONFIG process.

Figure 146 on page 498 shows the configuration process for 2210A using the Nways MRS Configuration Program.

Figure 147 on page 504 shows the configuration process for 2210B using the Nways MRS Configuration Program.

```

*talk 6 1
Gateway user configuration
Config>network 0 2
Token-Ring interface configuration
TKR config>media unshielded
TKR config>exit
Config>set data-link fr 3
Interface Number [0]? 1
Config>set data-link sdlc 4
Interface Number [0]? 2
Config>network 1 5
Frame Relay user configuration
FR Config>set lmi-type ansi 6
FR Config>exit
Config>network 2 7
SDLC user configuration
Creating a default configuration for this link
SDLC 2 Config>set link role negotiable 8
SDLC 2 Config>list link 9
Link configuration for: LINK_2 (ENABLED)

Role:          NEGOTIABLE      Type:          POINT-TO-POINT
Duplex:        FULL           Modulo:        8
Idle state:    FLAG           Encoding:      NRZ
Clocking:      EXTERNAL       Frame Size:    2048
Speed:         0              Cable:         Unknown, assuming DTE (other than X.2
1)

Timers:
XID/TEST response: 2.0 sec
SNRM response:     2.0 sec
Poll response:     0.5 sec
Inter-poll delay:  0.2 sec
RTS hold delay:    DISABLED
Inter-frame delay: DISABLED

Counters:
XID/TEST retry:    4
SNRM retry:        6
Poll retry:        10
SDLC 2 Config>add remote-secondary 10
Enter station address (in hex) [C1]? c1
Enter remote station name [SDLC_C1]? sdlc_c1
Enter max packet size [2048]? 1024
Enter receive window [7]? 7
Enter transmit window [7]? 7
SDLC 2 Config>list remote-secondary all 11

Address   Name      Status    Max BTU  Rx Window  Tx Window
-----
C1        SDLC_C1   ENABLED   1024     7          7
SDLC 2 Config>exit

```

Figure 144 (Part 1 of 5). Scenario 2: 2210A Nways MRNS Configuration

```

Config>protocol ip 12
Internet protocol user configuration
IP config>add address 13
Which net is this address for [0]? 0
New address [0.0.0.0]? 9.67.46.162
Address mask [255.0.0.0]? 255.255.255.240
IP config>add address 14
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.130
Address mask [255.0.0.0]? 255.255.255.240
IP config>set internal-ip-address 15
Internal IP address [9.67.46.162]? 9.67.46.162
IP config>set router-id 16
Router-ID [9.67.46.162]? 9.67.46.162
IP config>list address 17
IP addresses for each interface:
    intf 0   9.67.46.162      255.255.255.240  Network broadcast,    fill 0
    intf 1   9.67.46.130      255.255.255.240  Network broadcast,    fill 0
    intf 2                                     IP disabled on this interface
Router-ID: 9.67.46.162
Internal IP address: 9.67.46.162
IP config>exit
Config>protocol ospf 18
Open SPF-Based Routing Protocol configuration console
OSPF Config>enable ospf 19
Estimated # external routes [0]? 20
Estimated # OSPF routers [0]? 20
OSPF Config>set area 20
Area number [0.0.0.0]? 0.0.0.0
Authentication Type [0]? 1
OSPF Config>set interface 21
Interface IP address [0.0.0.0]? 9.67.46.130
Attaches to area [0.0.0.0]? 0.0.0.0
Retransmission Interval (in seconds) [5]? 5
Transmission Delay (in seconds) [1]? 1
Router Priority [1]? 1
Hello Interval (in seconds) [10]? 10
Dead Router Interval (in seconds) [40]? 40
Type Of Service 0 cost [1]? 1
Authentication Key []? abcdefg 22
Retype Auth. Key []? abcdefg
OSPF Config>add neighbor 23
Interface IP address [0.0.0.0]? 9.67.46.130
IP Address of Neighbor [0.0.0.0]? 9.67.46.131
Can that router become Designated Router on this net [Yes]? yes
OSPF Config>set non-broadcast 24
Interface IP address [0.0.0.0]? 9.67.46.130
Poll Interval [120]? 120

```

Figure 144 (Part 2 of 5). Scenario 2: 2210A Nways MRNS Configuration

```

OSPF Config>enable as boundary routing 25
Import EGP routes? [No]: no
Import BGP routes? [No]: no
Import RIP routes? [No]: no
Import static routes? [No]: no
Import direct routes? [No]: yes
Import subnet routes? [No]: yes
Always originate default route? [No]: no
Originate default if EGP/BGP routes available? [No]: no
OSPF Config>exit
Config>protocol dls 26
DLSw protocol user configuration
DLSw config>enable dls 27
DLSw config>set srb 28
Enter segment number in hex (1-FFF)- [0]? aaa
DLSw config>add tcp 29
Enter the DLSw neighbor IP Address [0.0.0.0]? 9.67.46.17
Transmit Buffer Size (Decimal) [5120]? 5120
Maximum Segment Size (Decimal) [1024]? 1024
Enable/Disable Keepalive?(E/D)- [D]? e
DLSw config>open-sap 0 00 30
DLSw config>open-sap 0 04
DLSw config>add sdlc 31
Interface # [0]? 2
SDLC Address [C1]? c1
Source MAC Address [000000000000]? 400000033316
Idblk in Hex (0-0xffff) [0]? 05d
Idnum in Hex (0-0xfffff) [0]? 33316
LLC Source SAP (0 for auto-assign) [0]? 0
LLC Destination SAP [4]? 4
Destination MAC Address [000000000000]? 400000033338
DLSw config>list dls global 32
DLSw is                ENABLED
LLC2 send Disconnect is  ENABLED

SRB Segment number      AAA
Max DLSw sessions       1000
DLSw global memory allotment 153344
LLC per-session memory allotment 8192
SDLC per-session memory allotment 4096

DLSw MAC Address        40:00:00:03:33:16

Database age timer      1200 seconds
Age timer resolution    300  seconds
Max wait timer for ICANREACH 20  seconds
Wait timer for LLC test response 15  seconds
Wait timer for SDLC test response 15  seconds
Join Group Interval     900  seconds
DLSw config>exit

```

Figure 144 (Part 3 of 5). Scenario 2: 2210A Nways MRNS Configuration

```

Config>protocol asrt 33
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 34
ASRT config>enable dls 35
ASRT config>disable transparent 36
Port Number [1]? 1
ASRT config>enable source-routing
Port Number [1]? 1
Segment Number for the port in hex(1 - FFF) [1]? abc
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>list bridge 37

          Source Routing Transparent Bridge Configuration
          =====

Bridge:   ENABLED                      Bridge Behaviour: Unknown
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 1        No. of Source routing segments: 1
SRB: Max ARE Hop cnt: 14               Max STE Hop cnt: 14
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE         Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED    FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: ENABLED
Number of ports added: 1
Port Number: 1   Interface Number: 0 Port Behaviour: SRB Only

ASRT config>CTRL+P
*restart 38
Are you sure you want to restart the gateway? (Yes or [No]): yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 39

CGW Operator Console

+network 2 40
SDLC Console
SDLC-2>list remote-secondary all 41

Address      Name      Status      Max BTU  Rx Window  Tx Window
-----
C1          SDLC_C1    CONNECTED    1024      7          7

```

Figure 144 (Part 4 of 5). Scenario 2: 2210A Nways MRNS Configuration

```

SDLC-2>list link counters 42
Link counters for: LINK_2 (ENABLED)

      I-Frames  I-Bytes  Re-Xmit  UI-Frames  UI-Bytes
      -----
Send      0        0        0        0        0
Recv      0        0        0        0        0

      RR      RNR      REJ
      -----
Send      165      0        0
Recv      164      0        0

SDLC-2>exit
+protocol dls 43
Data Link Switching Console
DLSw>list sdlc sessions 44
  Net   Addr   Src Sap  Dst Sap  Dest MAC          OutQ  State
  1. 2   C1     04      04      40:00:00:03:33:38  00   CONTACTED
DLSw>list tcp sessions all 45
  Group   IP Address   Conn State   Pkts Sent  Pkts Rcvd  Bytes Sent  Bytes Rcvd
  -----
1         9.67.46.17  ESTABLISHED      11        31        948       2738
DLSw>exit

```

Figure 144 (Part 5 of 5). Scenario 2: 2210A Nways MRNS Configuration

Notes:

- 1 Talk to the CONFIG process.
- 2 Configure the token-ring interface. Set the cable type to UTP.
- 3 Set the data link for interface 1 to frame relay.
- 4 Set the data link for interface 2 to SDLC.
- 5 Start configuration of the frame relay interface.
- 6 Set the LMI type to ANSI.
- 7 Start configuration of the SDLC interface.
- 8 Set the link role to negotiable, indicating that this link will have a PU Type 2.1 attached.
- 9 List the SDLC link to ensure that everything is correct.
- 10 Add the SDLC PU Type 2.1 information.
- 11 List the remote station information.
- 12 Start the configuration of IP.
- 13 Add an IP address to the token-ring interface.
- 14 Add an IP address to the frame relay interface.

- 15** Set the internal IP address for use by DLSw.
- 16** Set the router ID IP address.
- 17** List the IP addresses to ensure that everything is correct.
- 18** Start the configuration of OSPF.
- 19** Enable OSPF.
- 20** Set the characteristics for area 0.0.0.0. In this scenario we are using an authentication key for the area.
- 21** Add the frame relay interface to OSPF area 0.0.0.0.
- 22** Enter the authentication key for area 0.0.0.0.
- 23** Add an OSPF neighbor.
- 24** Set the frame relay interface to non-broadcast.
- 25** Enable AS boundary routing, to allow us to import our direct and subnet routes into the OSPF routing table.
- 26** Start the configuration of DLSw.
- 27** Enable DLSw.
- 28** Set the DLSw virtual segment number.
- 29** Add a DLSw TCP neighbor.
- 30** Open SAPs 00 and 04 for DLSw.
- 31** Add a DLSw SDLC station.
- 32** List the DLSw configuration to ensure that everything is correct.
- 33** Start the configuration of bridging.
- 34** Enable bridging.
- 35** Enable DLSw on the bridge.
- 36** Disable transparent bridging, and enable source route bridging on the token-ring interface.
- 37** List the bridge configuration to ensure that everything is correct.
- 38** Restart the router.
- 39** Talk to the GWCON process.
- 40** Enter the SDLC monitoring console.
- 41** List the status of all SDLC remote stations. In this scenario only one station is defined, and it is connected.

- 42** List the traffic statistics for the SDLC link.
- 43** Enter the DLSw monitoring console.
- 44** List the DLSw SDLC sessions. In this scenario there is one DLSw SDLC session, and the status is contacted.
- 45** List the DLSw TCP sessions. In this scenario only one TCP session is defined, and it is established.

```

*talk 6 1
Gateway user configuration
Config>set data-link fr 2
Interface Number [0]? 1
Config>disable interface 2 3
Config>network 1 4
Frame Relay user configuration
FR Config>set lmi-type ansi 5
FR Config>exit
Config>protocol ip 6
Internet protocol user configuration
IP config>add address 7
Which net is this address for [0]? 0
New address [0.0.0.0]? 9.67.46.113
Address mask [255.0.0.0]? 255.255.255.240
IP config>add address 8
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.132
Address mask [255.0.0.0]? 255.255.255.240
IP config>set internal-ip-address 9
Internal IP address [9.67.46.113]? 9.67.46.113
IP config>set router-id 10
Router-ID [9.67.46.113]? 9.67.46.113
IP config>exit
Config>protocol ospf 11
Open SPF-Based Routing Protocol configuration console
OSPF Config>enable ospf 12
Estimated # external routes [0]? 20
Estimated # OSPF routers [0]? 20
OSPF Config>set area 13
Area number [0.0.0.0]? 0.0.0.0
Authentication Type [0]? 1
OSPF Config>set interface 14
Interface IP address [0.0.0.0]? 9.67.46.132
Attaches to area [0.0.0.0]? 0.0.0.0
Retransmission Interval (in seconds) [5]? 5
Transmission Delay (in seconds) [1]? 1
Router Priority [1]? 1
Hello Interval (in seconds) [10]? 10
Dead Router Interval (in seconds) [40]? 40
Type Of Service 0 cost [1]? 1
Authentication Key []? abcdefg 15
Retype Auth. Key []? abcdefg
OSPF Config>set non-broadcast 16
Interface IP address [0.0.0.0]? 9.67.46.132
Poll Interval [120]? 120
OSPF Config>add neighbor 17
Interface IP address [0.0.0.0]? 9.67.46.132
IP Address of Neighbor [0.0.0.0]? 9.67.46.131
Can that router become Designated Router on this net [Yes]? yes

```

Figure 145 (Part 1 of 4). Scenario 2: 2210B Nways MRNS Configuration

```

OSPF Config>enable as boundary routing 18
Import EGP routes? [No]: no
Import BGP routes? [No]: no
Import RIP routes? [No]: no
Import static routes? [No]: no
Import direct routes? [No]: yes
Import subnet routes? [No]: yes
Always originate default route? [No]: no
Originate default if EGP/BGP routes available? [No]: no
OSPF Config>exit
Config>protocol dls 19
DLSw protocol user configuration
DLSw config>enable dls 20
DLSw config>set srb 21
Enter segment number in hex (1-FFF)- [0]? AAA
DLSw config>open-sap 0 00 22
DLSw config>open-sap 0 04
DLSw config>add tcp 23
Enter the DLSw neighbor IP Address [0.0.0.0]? 9.67.46.17
Transmit Buffer Size (Decimal) [5120]? 5120
Maximum Segment Size (Decimal) [1024]? 1024
Enable/Disable Keepalive?(E/D)- [D]? e
DLSw config>list dls global 24
DLSw is                               ENABLED
LLC2 send Disconnect is              ENABLED

SRB Segment number                   AAA
Max DLSw sessions                    1000
DLSw global memory allotment         153344
LLC per-session memory allotment     8192
SDLC per-session memory allotment    4096

                                     No MAC Address set

Database age timer                   1200 seconds
Age timer resolution                 300 seconds
Max wait timer for ICANREACH         20 seconds
Wait timer for LLC test response     15 seconds
Wait timer for SDLC test response    15 seconds
Join Group Interval                  900 seconds
DLSw config>exit
Config>protocol asrt 25
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge 26
ASRT config>enable dls 27

```

Figure 145 (Part 2 of 4). Scenario 2: 2210B Nways MRNS Configuration

ASRT config>**list bridge**

28

Source Routing Transparent Bridge Configuration

=====

Bridge: ENABLED Bridge Behaviour: Unknown
Bridge Address: Not Specified By User Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0 No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0 Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: ENABLED
Number of ports added: 1
Port Number: 1 Interface Number: 0 Port Behaviour: STB Only
ASRT config>**exit**

Config>**CTRL+P**

***restart**

29

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

Copyright Notices:

Copyright 1985-1994 Proteon, Inc.

Copyright 1984-1987, 1989 by J. Noel Chiappa

Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

***talk 5**

30

CGW Operator Console

+protocol ospf

31

Open SPF-Based Routing Protocol console

OSPF>**neighbor**

32

Neighbor addr	Neighbor ID	State	LSrxl	DBsum	LSreq	Ifc
9.67.46.131	9.67.46.17	8	0	0	0	FR/0

OSPF>**dump**

33

Type	Dest net	Mask	Cost	Age	Next hop(s)
Sbnt	9.0.0.0	FF000000	1	0	None
SPE1	9.67.46.16	FFFFFFF0	2	1	9.67.46.131
Dir*	9.67.46.112	FFFFFFF0	1	0	Eth/0
SPF	9.67.46.113	FFFFFFF0	0	0	SINK/0
SPF*	9.67.46.128	FFFFFFF0	1	1	FR/0
SPE2	9.67.46.160	FFFFFFF0	1	1	9.67.46.130
SPF	9.67.46.162	FFFFFFF0	1	1	9.67.46.130

Routing table size: 768 nets (49152 bytes), 7 nets known

Figure 145 (Part 3 of 4). Scenario 2: 2210B Nways MRNS Configuration

```

OSPF>routeers 34
DType RType Destination      Area      Cost      Next hop(s)
ASBR  SPF    9.67.46.17    0.0.0.0   1         9.67.46.131
ASBR  SPF    9.67.46.162  0.0.0.0   1         9.67.46.130
OSPF>interface 35

Ifc Address      Phys  assoc. Area  Type  State  #nbrs  #adjs
9.67.46.132      FR/0  0.0.0.0     Multi 32     1      1

```

Figure 145 (Part 4 of 4). Scenario 2: 2210B Nways MRNS Configuration

Notes:

- 1** Talk to the CONFIG process.
- 2** Set the data link for interface 1 to frame relay.
- 3** Disable interface 2 as it is not used in this scenario.
- 4** Start the configuration of the frame relay interface.
- 5** Set the LMI type to ANSI.
- 6** Start the configuration of IP.
- 7** Add an IP address to the Ethernet interface.
- 8** Add an IP address to the frame relay interface.
- 9** Set the internal IP address, for use by DLSw.
- 10** Set the router ID IP address.
- 11** Start the configuration of OSPF.
- 12** Enable OSPF.
- 13** Set the characteristics for area 0.0.0.0. In this scenario, we are using an authentication key for the area.
- 14** Add the frame relay interface to OSPF area 0.0.0.0.
- 15** Enter the authentication key for area 0.0.0.0.
- 16** Set the frame relay interface to non-broadcast.
- 17** Add an OSPF neighbor.
- 18** Enable AS boundary routing to allow us to import our direct and subnet routes into the OSPF routing table.
- 19** Start the configuration of DLSw.
- 20** Enable DLSw.
- 21** Set the DLSw virtual segment number.

- 22** Open SAPs 00 and 04 for DLSw.
- 23** Add a DLSw TCP neighbor.
- 24** List the DLSw configuration to ensure that everything is correct.
- 25** Start the configuration of bridging.
- 26** Enable bridging.
- 27** Enable DLSw on the bridge.
- 28** List the bridge configuration to ensure that everything is correct.
- 29** Restart the router.
- 30** Talk to the GWCON process.
- 31** Enter the OSPF monitoring console.
- 32** List the OSPF neighbors. In this scenario only one neighbor is defined, and it is active.
- 33** List the OSPF routing table.
- 34** List the OSPF routers.
- 35** List the OSPF interface statistics.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 125** **2**
 Select CONFIGURE of interface 0 **3**
 ENABLE INTERFACE
 MAC ADDRESS = **40002210A001**
 Select SPEED
 Select 4
 Select PACKET SIZE
 Select 2052
 Select CABLE TYPE
 Select **UTP**
 RIF TIMER = 120
 DISABLE END NODE SOURCE ROUTING

Select PPP of interface 1
 Select **FRAME RELAY** **4**

Select CONFIGURE of serial interface 1 **5**
 On the GENERAL subpanel
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select RS-232 DTE
 Select subpanel LMI
 Select LMI TYPE
 Select **ANSI** **6**
 ENABLE LMI
 ENABLE ORPHAN-CIR
 ENABLE MULTICAST EMULATION
 DISABLE CIR-MONITOR
 ENABLE PROTOCOL BROADCAST
 FRAME SIZE = 2048
 P1 = 64
 T1 = 10
 N1 = 6
 N2 = 3
 N3 = 4
 CIR ADJUSTMENT = 1
 LINE SPEED = 64000

Figure 146 (Part 1 of 5). Scenario 2: 2210A Nways MRS Configuration Program Configuration

Select the data-link protocol of Serial 2 (PPP by default)

Select **SDLC** **7**

Select CONFIGURE of Serial 2 **8**

On GENERAL subpanel :

ENABLE INTERFACE

MAXIMUM TRANSMISSION UNIT = 2048

Select ENCODING

Select NRZ

Select IDLE

Select FLAG

Select CLOCKING

Select EXTERNAL

CLOCK SPEED = 0

TRANSMIT DELAY = 0

Select CABLE TYPE

Select RS-232 DTE

On DETAIL subpanel :

ENABLE LINK

LINK NAME = LINK_2

Select ROLE

Select **NEGOTIABLE** **9**

Select TYPE

Select POINT TO POINT

Select DUPLEX

Select FULL

Select MODULO

Select 8

XID TIMEOUT = 2000

XID RETRY = 4

SNRM TIMEOUT = 2000

SNRM RETRY = 6

RTS HOLD = 0

On REMOTE SEC subpanel : **10**

ENABLE REMOTE SECONDARY

ADDRESS = C1

RECEIVE WINDOW SIZE = 7

TRANSMIT WINDOW SIZE = 7

NAME = SDLC_C1

PACKET SIZE = 1024

Select **ADD**

On the 2210 Navigation Window:

Select GENERAL on the IP directory

On the IP GENERAL Window: **11**

ENABLE IP

DISABLE ACCESS CONTROL

ENABLE DIRECTED-BROADCAST

INTERNAL ADDRESS = 9.67.46.162

ROUTING TABLE SIZE = 768

CACHE SIZE = 64

ROUTER-ID = 9.67.46.162

Figure 146 (Part 2 of 5). Scenario 2: 2210A Nways MRS Configuration Program Configuration

On the 2210 Navigation Window:
 Select INTERFACES on the IP directory

On the IP INTERFACES Window: **12**
 Select IP ADDRESSES for interface 0
 IP ADDRESS = **9.67.46.162**
 SUBNET MASK = **255.255.255.240**
 select **ADD**
 Select IP ADDRESSES for interface 1
 IP ADDRESS = **9.67.46.130**
 SUBNET MASK = **255.255.255.240**
 select **ADD**

On the 2210 Navigation Window:
 Select GENERAL on the OSPF directory

On the OSPF GENERAL window:
ENABLE OSPF **13**
 DISABLE PER-PACKET-MULTIPATH
NUMBER OF EXTERNAL ROUTES = 20
NUMBER OF OSPF ROUTERS = 20

On the 2210 Navigation Window:
 Select AS BOUNDARY ROUTING on the OSPF directory

On the AS BOUNDARY ROUTING window: **14**
ENABLE AS BOUNDARY
 DISABLE IMPORT EGP ROUTES
 DISABLE IMPORT RIP ROUTES
 DISABLE IMPORT STATIC ROUTES
ENABLE IMPORT DIRECT ROUTES
 ENABLE IMPORT SUBNET ROUTES
FROM AS NUMBER = 0

On the 2210 Navigation Window:
 Select AREA CONFIGURATION on the OSPF directory

On the OSPF AREA CONFIGURATION Window:
 On the GENERAL subpanel: **15**
 AREA = 0.0.0.0
AUTHENTICATION TYPE = 1
 SELECT **ADD**

Figure 146 (Part 3 of 5). Scenario 2: 2210A Nways MRS Configuration Program Configuration

On the 2210 Navigation Window:
Select INTERFACES on the OSPF directory

On the OSPF INTERFACES GENERAL Window:

Select CONFIGURE of interface 1 **16**

On the MULTICAST EXT subpanel

ENABLE OSPF

DISABLE MULTICAST

DISABLE FORW/REC AS UNICAST

COST = 1

PRIORITY = 1

IGMP POLLING INTERVAL = 60

IGMP TIMEOUT 180

Select AREA NUMBER

Select 0.0.0.0

AUTHENTICATION KEY = abcdefg **17**

Select subpanel TIMERS

RETRANS INTERVAL = 5

HELLO INTERVAL = 10

TRANSMISSION DELAY = 1

DEAD ROUTER INTERVAL = 40

Select subpanel NEIGHBORS **18**

NEIGHBOR IP ADDRESS = 9.67.46.131

ENABLE DESIGNATED ROUTER

Select **ADD**

Select subpanel NON-BROADCAST

ENABLE NON-BROADCAST **19**

On 2210 Navigation Window :
Select GENERAL on the DLSw directory

On 2210 DLSw General Window: **20**

ENABLE DLSw

SRB SEGMENT = aaa

On 2210 Navigation Window :
Select TCP CONNECTIONS on the DLSw directory

On 2210 DLSw TCP Connections Window: **21**

DLSw NEIGHBOR IP ADDRESS = 9.67.46.17

TRANSMIT BUFFER SIZE = 5120

MAXIMUM SEGMENT SIZE = 1024

ENABLE KEEPALIVE

Select **ADD**

Figure 146 (Part 4 of 5). Scenario 2: 2210A Nways MRS Configuration Program Configuration

On 2210 Navigation Window:
 Select INTERFACES on the DLSw directory

On the DLSw INTERFACES Window:
 Select CONFIGURE of Interface 2 **22**
SOURCE MAC ADDRESS = 400000033316
DESTINATION MAC ADDRESS = 400000033338
ID BLOCK = 05D
ID NUMBER = 33316
 LINK ADDRESS = C1
 DESTINATION SAP = 4
 SOURCE SAP = 0
 ENABLE SDLC ADDRESS
 Select **ADD**

On 2210 Navigation Window :
 Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window : **23**
ENABLE BRIDGING
ENABLE DLSw

On 2210 Navigation Window :
 Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window : **24**
ENABLE Token-Ring
 Select CONFIGURE of Token-Ring
 Select INTERFACE SUPPORTS
 Select **SRB**
 Select DUPLICATE FRAMES
 Select STE&TSF

On 2210 Navigation Window :
 Select CONFIGURE from the menu bar
 Select CREATE ROUTER CONFIGURATION

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window : **25**
 Enter **dlsfmfra**
 Select OK

Figure 146 (Part 5 of 5). Scenario 2: 2210A Nways MRS Configuration Program Configuration

Notes:

- 1** Start a new configuration.
- 2** Use Model 125.
- 3** Configure the token-ring interface.
- 4** Set the data link for interface 1 to frame relay.
- 5** Configure the frame relay interface.
- 6** Set the LMI type to ANSI.
- 7** Set the data link for interface 2 to SDLC.
- 8** Configure the SDLC interface.

- 9** Set the SDLC role to negotiable, for PU Type 2.1 support.
- 10** Add the PU Type 2.1 information.
- 11** Enable IP and add the internal address and router ID.
- 12** Add IP addresses to the token-ring and frame relay interfaces.
- 13** Enable OSPF.
- 14** Enable AS boundary routing and enable the import of direct and subnet routes into the OSPF routing table. The Nways MRS Configuration Program also requires the *FROM AS NUMBER* field to be completed.
- 15** Add area 0.0.0.0, specifying an authentication type of 1.
- 16** Add the frame relay interface to area 0.0.0.0.
- 17** Specify the authentication key for area 0.0.0.0.
- 18** Add an OSPF neighbor.
- 19** Set the frame relay interface to non-broadcast.
- 20** Enable DLSw and specify the virtual segment number.
- 21** Add a DLSw TCP neighbor.
- 22** Add an SDLC station to the DLSw configuration.
- 23** Enable bridging, and enable DLSw on the bridge.
- 24** Enable SRB on the token-ring interface.
- 25** Create a router configuration file.

On the 2210 Navigation Window:
 Select CONFIGURE from the menu bar
 Select NEW CONFIGURATION **1**

On the 2210 Navigation Window:
 Select INTERFACES on the DEVICES directory

On the DEVICE INTERFACE Window:
 Select MODEL
 Select **MODEL 126** **2**
 Select CONFIGURE of interface 0
 ENABLE INTERFACE
 Select CONNECTOR TYPE
 Select **AUTO-CONFIG**
 Select PPP of interface 1
 Select **FRAME RELAY** **3**

Select CONFIGURE of serial interface 1 **4**
 On the GENERAL subpanel
 ENABLE INTERFACE
 MAXIMUM TRANSMISSION UNIT = 2048
 Select ENCODING
 Select NRZ
 Select IDLE
 Select FLAG
 Select CLOCKING
 Select EXTERNAL
 CLOCK SPEED = 0
 TRANSMIT DELAY = 0
 Select CABLE TYPE
 Select RS-232 DTE
 Select subpanel LMI
 Select LMI TYPE
 Select **ANSI** **5**
 ENABLE LMI
 ENABLE ORPHAN-CIR
 ENABLE MULTICAST EMULATION
 DISABLE CIR-MONITOR
 ENABLE PROTOCOL BROADCAST
 FRAME SIZE = 2048
 P1 = 64
 T1 = 10
 N1 = 6
 N2 = 3
 N3 = 4
 CIR ADJUSTMENT = 1
 LINE SPEED = 64000
 Select CONFIGURE of Serial 2
 On GENERAL subpanel :
DISABLE INTERFACE **6**

Figure 147 (Part 1 of 4). Scenario 2: 2210A Configuration Using Nways MRS Configuration Program

On the 2210 Navigation Window:
Select GENERAL on the IP directory

On the IP GENERAL Window: **7**
ENABLE IP
DISABLE ACCESS CONTROL
ENABLE DIRECTED-BROADCAST
INTERNAL ADDRESS = 9.67.46.113
ROUTING TABLE SIZE = 768
CACHE SIZE = 64
ROUTER-ID = 9.67.46.113

On the 2210 Navigation Window:
Select INTERFACES on the IP directory

On the IP INTERFACES Window: **8**
Select IP ADDRESSES for interface 0
IP ADDRESS = **9.67.46.113**
SUBNET MASK = **255.255.255.240**
select **ADD**
Select IP ADDRESSES for interface 1
IP ADDRESS = **9.67.46.132**
SUBNET MASK = **255.255.255.240**
select **ADD**

On the 2210 Navigation Window:
Select GENERAL on the OSPF directory

On the OSPF GENERAL window:
ENABLE OSPF **9**
DISABLE PER-PACKET-MULTIPATH
NUMBER OF EXTERNAL ROUTES = 20
NUMBER OF OSPF ROUTERS = 20

On the 2210 Navigation Window:
Select AS BOUNDARY ROUTING on the OSPF directory

On the AS BOUNDARY ROUTING window: **10**
ENABLE AS BOUNDARY
DISABLE IMPORT EGP ROUTES
DISABLE IMPORT RIP ROUTES
DISABLE IMPORT STATIC ROUTES
ENABLE IMPORT DIRECT ROUTES
ENABLE IMPORT SUBNET ROUTES
FROM AS NUMBER = 0

On the 2210 Navigation Window:
Select AREA CONFIGURATION on the OSPF directory

On the OSPF AREA CONFIGURATION Window:
On the GENERAL subpanel:
AREA = 0.0.0.0
AUTHENTICATION TYPE = 1
SELECT **ADD** **11**

Figure 147 (Part 2 of 4). Scenario 2: 2210A Configuration Using Nways MRS Configuration Program

On the 2210 Navigation Window:
Select INTERFACES on the OSPF directory

On the OSPF INTERFACES GENERAL Window:
Select CONFIGURE of interface 1
On the MULTICAST EXT subpanel

ENABLE OSPF

DISABLE MULTICAST

DISABLE FORW/REC AS UNICAST

COST = 1

PRIORITY = 1

IGMP POLLING INTERVAL = 60

IGMP TIMEOUT 180

Select AREA NUMBER

Select 0.0.0.0

AUTHENTICATION KEY = abcdefg

Select subpanel TIMERS

RETRANS INTERVAL = 5

HELLO INTERVAL = 10

TRANSMISSION DELAY = 1

DEAD ROUTER INTERVAL = 40

Select subpanel NEIGHBORS

NEIGHBOR IP ADDRESS = 9.67.46.131

ENABLE DESIGNATED ROUTER

Select **ADD**

Select subpanel NON-BROADCAST

ENABLE NON-BROADCAST

On 2210 Navigation Window :
Select GENERAL on the DLSw directory

On 2210 DLSw General Window:

ENABLE DLSw

SRB SEGMENT = aaa

On 2210 Navigation Window :
Select TCP CONNECTIONS on the DLSw directory

On 2210 DLSw TCP Connections Window:

DLSw NEIGHBOR IP ADDRESS = 9.67.46.17

TRANSMIT BUFFER SIZE = 5120

MAXIMUM SEGMENT SIZE = 1024

ENABLE KEEPALIVE

Select **ADD**

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory
On BRIDGING - GENERAL Window :

ENABLE BRIDGING

ENABLE DLSw

Figure 147 (Part 3 of 4). Scenario 2: 2210A Configuration Using Nways MRS Configuration Program

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :

ENABLE Ethernet

Select CONFIGURE of Ethernet

Select INTERFACE SUPPORTS

Select **STB** **19**

Select DUPLICATE FRAMES

Select STE&TSF

On 2210 Navigation Window :

Select CONFIGURE from the menu bar

Select CREATE ROUTER CONFIGURATION **20**

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :

Enter **dlsfmfrb**

Select OK

Figure 147 (Part 4 of 4). Scenario 2: 2210A Configuration Using Nways MRS Configuration Program

Notes:

- 1** Start a new configuration.
- 2** Use Model 126.
- 3** Set the data link for interface 1 to frame relay.
- 4** Configure the frame relay interface.
- 5** Set the LMI type to ANSI.
- 6** Disable interface 2, because it is not used in this scenario.
- 7** Enable IP and add the internal address and router ID.
- 8** Add IP addresses to the token-ring and frame relay interfaces.
- 9** Enable OSPF.
- 10** Enable AS boundary routing and enable the import of direct and subnet routes into the OSPF routing table. The Nways MRS Configuration Program also requires the *FROM AS NUMBER* field to be completed.
- 11** Add area 0.0.0.0 specifying an authentication type of 1.
- 12** Add the frame relay interface to area 0.0.0.0.
- 13** Specify the authentication key for area 0.0.0.0.
- 14** Add an OSPF neighbor.
- 15** Set the frame relay interface to non-broadcast.
- 16** Enable DLSw and specify the virtual segment number.
- 17** Add a DLSw TCP neighbor.

- 18** Enable bridging, and enable DLSw on the bridge.
- 19** Enable STB on the Ethernet interface.
- 20** Create a router configuration file.

10.7 DLSw RFC 1795 Implementation in IBM 2210

Data Link Switching (DLSw) is a methodology developed by IBM to transport SNA and NetBIOS protocol traffic across IP networks. Supported endstations attach to the box via LAN interfaces, remote-bridging WAN interfaces, and SDLC interfaces. DLSw communicates with neighbor DLSw router using TCP/IP through any IP-enabled interface.

Key customer benefits provided by DLSw are in the areas of availability and efficient WAN utilization. Availability is improved and because DLSw enables the box to internally terminate the 802.2 layer and locally acknowledge frames, while encapsulating the data in TCP/IP. Local acknowledgement minimizes timeouts and the resulting session losses. Availability improvements are achieved through the automatic route switching provided by IP which re-routes traffic around failed nodes and through the reliable WAN transport provided by TCP.

Efficient WAN utilization is achieved because DLSw permits all supported protocols (including SNA and NetBIOS traffic) to be consolidated on a link. In addition, DLSw handles the link layer flow control for SNA endstations. Therefore, WAN and LAN traffic overhead is minimized because DLSw can handle the polling for SDLC and the keep-alive messages for the 802.2 logical link control (LLC) on either the token-ring or Ethernet LAN.

This DLSw implementation is compliant with AIW Version 1 Standard DLSw, which is also published as RFC 1795. DLSw interoperates with the DLSw implementation in MRNS V1 R1 and R2 for SNA traffic and with MRNS V1 R3 and later for SNA and NetBIOS.

The DLSw RFC 1795 support includes:

- Base functions
 - SNA explorer flows
 - Circuit-level pacing
 - Required capability exchange CVs
 - LF bit propagation
- Options implemented
 - SNA backward compatibility to RFC 1434 implementations
 - NetBIOS (see below)
 - Adaptive pacing
 - Version string control vector in capabilities exchange
 - Run-time capabilities exchange
 - Circuit priority (based on protocol type)
 - Single full-duplex TCP connection

- Remote SAP list filter
- Capabilities exchange of NetBIOS names

The NetBIOS Support includes:

- AIW_V1 explorer flows
- UI-frame type filters
- Duplicate UI-frame filters
- Dynamic name caching (learning)
- Integrated cache/filter and bridge code
- Bridge NetBIOS filters extended to DLSw

Specific areas of note in the DLSw base RFC 1795 support are as follows:

- Capabilities Exchange

When RFC 1795 compliant DLSw routers establish a transport connection with each other, they exchange configuration messages, which convey the supported feature set of the DLSw router such as optional DLSw features, number of TCP connections per DLSw neighbor, and supported SAP/NetBIOS name lists.

- Improved Flow Control (circuit-level pacing)

RFC 1795 formally defines per circuit flow control using an adaptive or fixed pacing mechanism. This implementation supports adaptive pacing, but it will also work with the less powerful fixed pacing mechanism. Although RFC 1434 did not formally define a flow control mechanism, this DLSw implementation used the SSP_ENTER_BUSY and SSP_EXIT_BUSY messages to halt and restart the flow of data on congested DLSw circuits. SSP_ENTER_BUSY and SSP_EXIT_BUSY will be used only when operating with RFC 1434 routers.

- Largest Frame Size Handling

RFC 1795 provides for the propagation of bits from the source-routing information field that indicate the largest frame that can flow on a particular source-routed path. This enables an endstation on one side of the IP network to see frame size restrictions imposed by bridges on the opposite side of the IP network. This DLSw implementation includes these flows and also uses LF bit information to help choose which of several neighbor routers to use to establish a new DLSw session.

- Circuit Prioritization

The prioritization of DLSw circuits is supported in RFC 1795. Each circuit being started by DLSw may request one of four different priorities or unspecified priority in the CANUREACH_cs SSP message. Unspecified indicates that circuit prioritization is not supported. MRS's initial circuit prioritization scheme will allocate transport bandwidth according to the circuit's priority and also according to the protocol type (SNA vs NetBIOS).

- Single TCP Connection between Routers

To improve performance, DLSw routers supporting RFC 1795 may elect to communicate using only one TCP connection instead of the two connections required by RFC 1434 implementations. This DLSw implementation will always attempt to operate using only one TCP connection, but will still use

two connections if the remote RFC 1795 DLSw requests it, when interoperating with a remote RFC 1434 DLSw product is necessary.

- SDLC PIU Segmenting

SNA FID-2 frames are now segmented when LIC frames from a host are too large to be handled by a remote SDLC controller.

- DLSw Neighbor Priority

All DLSw Groups and TCP connections may be assigned one of three priorities, which allows transport (TCP) connections to be used in preference to other connections. This is useful for backup connections between DLSw routers. When an endstation search message is broadcasted to multiple destinations and multiple responses are received for a given destination, the neighbor with the highest priority will be used. Without transport priority, or with transports of equal priority, the first neighbor with the highest priority will be used, seemingly at random. Transport priority functions are usable with any connected RFC 1434 or RFC 1795 DLSw.

- Multicast Group Support

This is an implementation feature allowing DLSw neighbor to dynamically discover each other, rather than requiring that each neighbor be statically configured. Multicast OSPF provides the multicase IP routing capability that this feature uses.

10.8 DLSw and NetBIOS Commands

All the NetBIOS commands will be found under DLS and ASRT feature.

Table 69. Process Description

Command	Function
?(help)	Lists the commands or actions associated with the specific commands.
Enable	Enables the duplicate frame filtering and route caching.
Disable	Disables the duplicate frame filtering and route caching.
List	Displays the cache, filters, statistics and general info about the cache.
ADD	Adds permanent entries in the cache.
Delete	Deletes cache entries.
SET	Sets the cache parameters, filters and general.
EXIT	Returns to previous prompt.

10.8.1 DLSw and NetBIOS Scenarios and Configuration

The scenario for this configuration is to enable NetBIOS, prioritizing between SNA and NetBIOS and showing the new display commands. DLSw configuration is already done. In the figure, the 2210A and 2210B have DLSw configured and have the IP address of token-ring as DLS partner (neighbor).

We changed 2210B to an IBM 6611 without changing any of the parameters in 2210A. There are some interoperability criteria to be considered. No LQM (Line Quality Monitoring) at the PPP link should be defined in IBM 6611. The join group feature in IBM 2210 cannot be used, because IBM 6611 does not support

that. The DLS partner must be the internal address of IBM 2210 and IBM 2210 should have IBM 6611 DLSw ID as partner.

RFC 1795 has the support to transport the NetBIOS packets over the TCP connection. The RFC does not specify how the NetBIOS packets are handled before they arrive to DLSw. The NetBIOS name caching and duplicate filter works as before.

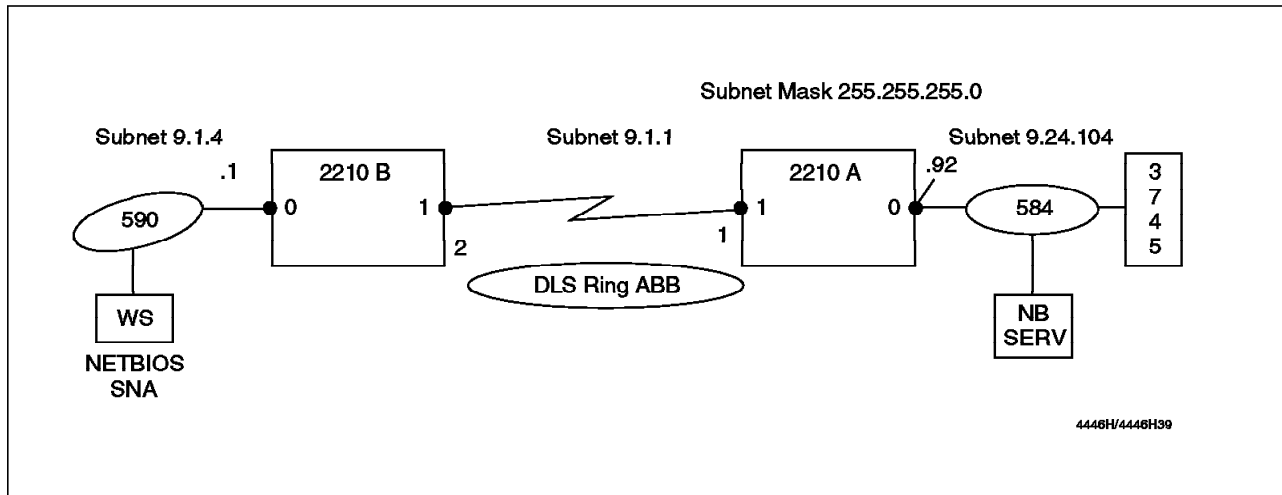


Figure 148. DLS Configuration

The first scenario shows the new DLSw configuration parameters in 2210A and some differences in the display commands.

```
*t 6

Config>proto dls
DLSw protocol user configuration
DLSw config>list priority
Priority for SNA DLSw sessions is          MEDIUM
Priority for NetBIOS DLSw sessions is      MEDIUM
Message allocation by C/H/M/L priority is  4/3/2/1
Maximum frame size for NetBIOS is          2052
DLSw config>set priority
Priority for SNA DLSw sessions (C/H/M/L) M? h 1
Priority for NetBIOS DLSw sessions (C/H/M/L) M? m
Message allocation by C/H/M/L priority (4 digits) 4/3/2/1? 6/5/1/1
Maximum NetBIOS frame size (516,1470,2052,or 4399) 2052? 516 2
DLSw config>set mem 3
Number of bytes to allocate for DLSw (at least 26368) 141056?
Number of bytes to allocate per LLC session 8192? 4
Number of bytes to allocate per SDLC session 4096? 4
Number of bytes to allocate for NetBIOS UI-frames 40960? 4
DLSw config>
Are you sure you want to restart the gateway? (Yes or No): y

*
```

Figure 149. DLSw Prioritizing and Memory Allocating for 2210A

1 There are four different priorities to define. In this example the IBM 2210 will send five SNA frames and then one NetBIOS frame. The SNA priority is defined as High and NetBIOS as Medium and frame count for High is 5 and for Medium is 1. The priority will only take place when there is a congestion situation and that means when DLS messages are queued up before sending them to TCP.

2 The priority is counting frames not bytes. Normally SNA frames are shorter than NetBIOS file transfer frames. NB frame segmentation will be an important parameter to give the SNA traffic a higher throughput.

3 This command allocates memory for the DLSw overall and to each DLSw session.

4 These commands allocate DLSw overall memory, but they are not used; use the default settings instead. The LLC and SDLC buffers are per circuit. When these buffers reach their limit, the IBM 2210 starts to send RNR and when they are free RR will flow again. NetBIOS frame allocation is for all NetBIOS UI frames; when this limit is reached, DLSw will discard frames and sessions can be lost. Do not set this limit too low. If you have DLS.161 messages, you have run out of NetBIOS memory.

```

Protocol name or number IP? dls
Data Link Switching Console
DLSw>list tcp sess all 1

```

Group	IP Address	Conn State	Version	Active Sess	Sess Creates
1	9.1.4.1	ESTABLISHED	AIW V1R0	1	74
2	9.9.9.9	PENDING R/W	UNKNOWN	0	0

```

DLSw>list tcp stat 2
Enter the DLSw neighbor IP Address 0.0.0.0? 9.1.4.1

```

	Transmitted	Received
Data Messages	6907	1408
Data Bytes	1251781	94137
Control Messages	2804	459
CanYouReach Explorer Messages	1051	4
ICanReach Explorer Messages	3	0
NameQuery Explorer Messages	1518	91
NameRecognized Explorer Messages	72	0

```

DLSw>list list tcp ?
CAPABILITIES
CONFIG
SESSIONS
STATISTICS
DLSw>list tcp capabilities
Enter the DLSw neighbor IP Address 0.0.0.0? 9.1.4.1
Vendor ID: 10005A 3
Vendor product version: IBM 2210 Nways MNRS V1 R3.0 Z71 4
Initial pacing window: 12
Preferred TCP connections: 1 5
Supported SAPs: 00 04 08 0C F0 6
DLSw>

```

Figure 150. DLSw TCP Displays Output from 2210A

1 The TCP displays the version of the partner. It can be RFC 1434+ (the '+' sign means RFC 1434 or higher) or, as in this case, AIW Release and Version means RCF 1795.

2 To get statistics from the TCP sessions you must enter this command. You can only get statistics from one partner at each display.

3 Means IBM.

4 The software release level and the patch level (Z71).

5 2210 now can have one TCP connection between neighbors instead of two. To have one TCP connection between each partner saves memory and should be used when applicable.

6 Displays open SAPs in the neighbor. With the new feature, Auto-open-SAP, IBM 2210 can automatically open new SAPs; if one IBM 2210 has more open SAPs than the neighbor, the neighbor can open the extra SAPs needed.

```

t 5

+P
Protocol name or number IP? dls
Data Link Switching Console
DLSw>list dls sess all

```

	Source	Destination	State	Flags	Dest IP Addr	Id
1	400008220210 04	400052005292 04	CONNECTED		9.1.4.1	74

```

DLSw>list dls sess det
Session Identifier 1? 74 1

```

	Source	Destination	State	Flags	Dest IP Addr	Id
0	400008220210 04	400052005292 04	CONNECTED		9.1.4.1	74

```

    Personality:    TARGET
    XIDs sent:      4
    XIDs rcvd:      5
    Datagrams sent: 0
    Datagrams rcvd: 0
    Info frames sent: 12
    Info frames rcvd: 13
    RIF:            0820 ABB1 5844 5800
    Local CID :     314AA660:7E00004A 2
    Remote CID:     014C72B8:7E000057
    Priority:       HIGH 3
DLSw>list dls sess stat
DLSw Session States:

    DISCONNECT = 0, RSLV_PEND = 1
    CIRC_PEND = 2, CIRC_EST = 3
    CIR_RSTRT = 4, CONN_PEND = 5
    CONT_PEND = 6, CONNECTED = 7
    DISC_PEND = 8, HALT_PEND = 9
    REST_PEND = 10, WAIT_NOACK = 11
    CIRC_STRT = 12, HLT_NOACK = 12

Enter state value 7? 7 (next page)

```

	Source	Destination	State	Flags	Dest IP Addr	Id
0	400008220210 04	400052005292 04	CONNECTED		9.1.4.1	74

Figure 151. DLSw Displays Output from 2210A

- 1** This display gives you the statistics of a DLS session.
- 2** New in this display are the fields for local CID and remote CID. Normally you do not need this information.
- 3** You can also see the priority of this session.


```

DLSw>list dls sess ip
Enter the DLS neighbor IP Address 0.0.0.0? 9.1.4.1
      Source      Destination      State      Flags      Dest IP Addr Id
-----
1 400008220210 04 400052005292 04 CONNECTED      9.1.4.1      74

DLSw>list dls cache all
      Mac Address      Secs to live      IP Address(es)      Largest Frame
-----
1. 00608C22AB6C      1181
11. 400052005008      1190
12. 400052005292      916      9.1.4.1      2052
13. 400066660018      1182

DLSw>list dls global
DLSw is      ENABLED
LLC2 send Disconnect is      ENABLED
Automatic TCP connection      ALWAYS CONNECT

SRB Segment number      ABB
MAC <-> IP mapping cache size      128
Max DLSw sessions      1000
DLSw global memory allotment      141056
LLC per-session memory allotment      8192
SDLC per-session memory allotment      4096
NetBIOS UI-frame memory allotment      40960 1

Database age timer      1200 seconds
Max wait timer for ICANREACH      20 seconds
Wait timer for LLC test response      15 seconds
Wait timer for SDLC test response      15 seconds
Join Group Interval      900 seconds
Neighbor priority wait timer      2.0 seconds

DLSw>list dls mem
Total DLSw bytes requested:      141056
Global receive pool bytes granted:      84633
  Currently in use:      86
Global transmit pool bytes granted:      56423
  Currently in use:      2056

NetBIOS UI-frame pool total bytes:      40960
  Currently in use:      40962 1

      Id      Source      Destination      Initial      Current      Congest      DLCXmits
      ---      ---      ---      ---      ---      ---      ---
      74      400008220210 04      400052005292 04      8192      8192      READY      0
DLSw>

```

Figure 152. DLSw Displays Output from 2210A

1 Shows the NetBIOS buffers. In the NetBIOS cache there were more than 500 entries.

The next scenario is to add NetBIOS support to the 2210A and do NetBIOS display commands.

```
*t 6
Config>protocol dls
DLSw protocol user configuration
DLSw config>open-sap
Interface # 0?
Enter SAP in hex (range 0-F0), 'SNA' or 'NB' 4? nb 1
SAP F0 already opened on interface 0
DLSw config>netbios

NetBIOS Support User Configuration

NetBIOS config>enable
DUPLICATE-FILTERING
ROUTE-CACHING
NetBIOS config>enable duplicate-filtering 2
Duplicate frame filtering is ON
NetBIOS config>enable route-caching 3
Route caching is ON
Netbios config>list general
Bridge-only Information:
Bridge duplicate filtering is ON
Bridge duplicate frame filter t/o 1.5 seconds

DLS-only Information:
DLS command frame retry count 5
DLS max remote name cache entries 100
DLS command frame retry timeout 0.5 seconds

DLS-Bridge Common Information:

Route caching is ON
Significant characters in name 15
Max local name cache entries 500
Duplicate frame detect timeout 5.0 seconds
Best path aging timeout 60.0 seconds
Reduced search timeout 1.5 seconds
Unreferenced entry timeout 5000 minutes

NetBIOS config>
```

Figure 153. DLSw NetBIOS Configuration Output from 2210A

1 To enable the NetBIOS for DLS you must enable the NB SAP. This enables NetBIOS packets to be forwarded to DLS.

2 Enables the duplicate-filtering and route-caching.

3 Enables the route-caching. If the NB name is in the router name-cache and is an individual local, the router will send the frame to the proper port indicated from the RIF field. If the route-cache is not enabled, the frame will be sent to all bridge ports.

```

NetBIOS>exit
DLSw>list d s a
      Source          Destination      State      Flags      Dest IP Addr Id
-----
1 400008220210 04 400052005292 04 CONNECTED      9.1.4.1      1
2 400000033320 F0 400052005292 F0 CONNECTED      9.1.4.1 1      2
3 400052005064 F0 400052005292 F0 CONNECTED      9.1.4.1      3
DLSw>exit
+
*restart

*t 5

Protocol name or number IP? dls
Data Link Switching Console
DLSw>netbios

NetBIOS Support User Console

NetBIOS>list cache local 2

Cnt  NetBIOS Name      Loc Path State  MAC Address  Routing Information
---
14 ABHAY 3 <00> UNKNOWN 4
15 ALEXANDEPEER <00> UNKNOWN
22 WTRAS1 <00> UNKNOWN
23 WTRAS1X <00> SEARCH ALL 5
24 WTRAS2 <00> UNKNOWN
25 WTRAS3 <00> UNKNOWN
26 WTRDC <00> BEST FOUND 400000033320 5844-5800 6
27 WTRN1ITS <2B> BEST FOUND 400052005060 5844-5803-5830
28 WTRPS1 <20> BEST FOUND 400052005064 5844-5800

```

Figure 154. DLSw NetBIOS Display Output from 2210A

- 1** Normal list of all DLS sessions, but now the NetBIOS sessions will show up. The F0 SAP is the SAP used by NetBIOS. Two NetBIOS sessions can be seen at the display 2 and 3.
- 2** Shows the NetBIOS names learned from the local bridge network.
- 3** <XX> is the last character in the NetBIOS name.
- 4** NetBIOS clients always show up as unknown without MAC and RIF information. Only servers will have this information when known.
- 5** The router conducts a full search, which means the router sends the search to all DLS partners.
- 6** The router knows the best way to the server. The MAC address and the ROF field are displayed (ring 584 bridge 4 ring 580).

```

NetBIOS>list cache remote 1

Cnt  NetBIOS Name      Entry Type  Rem Path St  IP Address(es)
---  -
  1  WTR05292      <00>  DYNAMIC      UNKNOWN

NetBIOS>list cache name ABHAY 2

      NetBIOS Name      Name Type      Entry Type
      -
      ABHAY      <00>  INDIVIDUAL LOCAL  DYNAMIC 3

Count of name cache entry hits ..... 0

Age of name cache entry ..... 9034
Age of name cache last reference ..... 9038

Local path information:

  Loc Path St  Timestamp  MAC Address  LFS  Routing Information
  -
  UNKNOWN      55900

Remote path information:

  Rem Path St  Timestamp  LFS  IP Address(es)
  -
  UNKNOWN      55910

NetBIOS>list cache active

Cnt  NetBIOS Name      Name Type      Entry Type
---  -
  13  A2104      <00>  INDIVIDUAL LOCAL  DYNAMIC
  14  ABHAY      <00>  INDIVIDUAL LOCAL  DYNAMIC
  15  ADCLAN1      <00>  UNKNOWN          DYNAMIC
  16  ADCLAN1D      <00>  INDIVIDUAL LOCAL  DYNAMIC
  17  ADSRV1      <00>  INDIVIDUAL LOCAL  DYNAMIC
  18  AIXPEERS      <00>  UNKNOWN          DYNAMIC
  19  ALEXANDEPEER <00>  INDIVIDUAL LOCAL  DYNAMIC
  20  ALVIPEER      <00>  INDIVIDUAL LOCAL  DYNAMIC
  21  ANDERSON1      <00>  INDIVIDUAL LOCAL  DYNAMIC

NetBIOS>

```

Figure 155. DLSw NetBIOS Configuration Output from 2210A

- 1** The remote cache will show the NetBIOS names learned from the WAN side (from 2210C).
- 2** An individual NetBIOS name can be displayed.
- 3** An individual local is reached over the locally bridged network. The MAC address can be found in the cache. If the route-caching is enabled, the best route will be stored.

```

NetBIOS>
NetBIOS>list statistic cache 1

Local name cache entries          493
Remote name cache entries         106
Local individual names            493
Remote individual names           0
Group names                       0
Unknown names                     109
Name cache hits                   31519
Name cache misses                 19799

NetBIOS>list stat frames bridge 2

Frames in cache                   6
Name query frames                 2016
Status query frames              1384
Add name frames                   0
Add group name frames             0
Name in conflict frames           0
Frames not filtered as duplicates 11990

NetBIOS>list stat frames dls

Name query frames                 0
Status query frames              0
Add name frames                   0
Add group name frames             0
Name in conflict frames           0
Frames not filtered as duplicates 4

NetBIOS>list stat gen bridge 3

Frames received                   41130
Frames discarded                  17430
Frames forwarded to bridge        23696
Frames forwarded to DLS           14008

NetBIOS>list stat gen dls

Frames received                   8
Frames discarded                  0
Frames forwarded to bridge        8

```

Figure 156. DLSw NetBIOS Filtering Output from 2210A

- 1** List statistics from the cache.
- 2** List statistics for the bridge of different frame types.
- 3** List the total frames received and forwarded.

```

t 5

+p
Protocol name or number IP? dls
Data Link Switching Console
DLSw>netbios

NetBIOS Support User Console

NetBIOS>list cache local

Cnt  NetBIOS Name          Loc Path State  MAC Address  Routing Information
---  -
16  10005AEBCE86VIP<53>  UNKNOWN  1
17  A2104                  <00>  UNKNOWN
18  ABHAY                  <00>  UNKNOWN
19  ADCLAN1D              <00>  UNKNOWN
20  ADSRV1                <00>  UNKNOWN
21  ALEXANDEPEER         <00>  UNKNOWN
Would you like to continue? Yes: yes

Cnt  NetBIOS Name          Loc Path State  MAC Address  Routing Information
---  -
22  ALVIPEER              <00>  UNKNOWN
41  BIGBAD95              <00>  UNKNOWN
42  BOENSC00              <00>  UNKNOWN
Would you like to continue? Yes: no

NetBIOS>list stat cache

Local name cache entries          490  2
Remote name cache entries         120
Local individual names            490
Remote individual names           0
Group names                       0
Unknown names                     120
Name cache hits                   88410
Name cache misses                 35455

NetBIOS>

```

Figure 157. DLSw NetBIOS Display Output from 2210A

- 1** The cache contains all NetBIOS names.
- 2** 490 NetBIOS names are stored in the cache.

Third scenario will add a name filter in 2210A.

```
*t 6

Config>p
Protocol name or number IP? dls
DLSw protocol user configuration
DLSw config>netbios

NetBIOS Support User Configuration

NetBIOS config>set filter name 1
NETBIOS Filtering configuration
NETBIOS Filter config>create name 2
Handle for Name Filter List ? test
NETBIOS Filter config>update test 3
NETBIOS Name test config>add inclusive ascii W* 4

NETBIOS Name test config>default exclusive 5
NETBIOS Name test config>list
NAME Filter List Default: Exclusive

  Item #   Type   Inc/Ex   Hostname   Last Char
    ----   -
     1     ASCII   Inc      W*
```

Figure 158. DLSw NetBIOS Filtering Configuration Output from 2210A

- 1** The set filter name/byte allows you to create filters.
- 2** Create a filter list with a name of test.
- 3** Update the filter list with the name test.
- 4** Add an inclusive NetBIOS name filter with a wild card (*).
- 5** This means that all NetBIOS names that do not match the inclusive filter will be discarded.

```

NETBIOS Filter config>?
CREATE
DELETE
DISABLE
ENABLE
FILTER-ON
LIST
UPDATE
EXIT
NETBIOS Filter config>filter-on input 1
Port Number ? 1
Filter List ? test
NETBIOS Filter config>list

NETBIOS Filtering: Enabled 2

NETBIOS Filter Lists
----- 3

      Handle      Type
      test        Name

NETBIOS Filters
-----

      Port #      Direction      Filter List Handle(s)
      1           Input          test

NETBIOS Filter config>
*restart

*t 5

CGW Operator Console

```

Figure 159. DLSw NetBIOS Filtering Configuration from 2210A

1 You must tell at which port the filter will be applied, and whether it is an input or output filter. Port 1 is the token-ring bridge and the filter will be the input.

2 The filter function must be enabled.

3 This command displays all filters configured, the name of the filter and what type it is (NAME/BYTE), to which port the filter is applied and at what direction.


```

+p
Protocol name or number IP? dls
Data Link Switching Console
DLSw>netbios

NetBIOS Support User Console

NetBIOS>list cache local

```

Cnt	NetBIOS Name	Loc Path State	MAC Address	Routing Information
1	BIGBAD95	<00> UNKNOWN		
6	WFS1SER	<00> UNKNOWN		
7	WGMSTSRV	<00> UNKNOWN		
8	WSSERVER	<00> UNKNOWN		
9	WTRAS1	<00> UNKNOWN		
10	WTRAS1X	<00> UNKNOWN		
11	WTRAS2	<00> UNKNOWN		
12	WTRDC	<00> UNKNOWN		
13	WTRN1ITS	<2B> BEST FOUND	400052005060	5844-5803-5830
14	WTRPS1	<00> UNKNOWN		

```

NetBIOS>list stat cache

Local name cache entries          18
Remote name cache entries         16
Local individual names            18
Remote individual names           0
Group names                       0
Unknown names                     16
Name cache hits                   150
Name cache misses                 648

NetBIOS>set filter name
NETBIOS Filter>list filters

NETBIOS Filtering: Enabled

Port #      Direction  Filter List Handle(s)  Pkts Filtered
-----
1           Input      test                   2468

```

NETBIOS Filter>

Figure 160. DLSw NetBIOS Filtering Display Output from 2210A

1 The cache shows the NetBIOS names not filtered. The name filter only applies at add name query, add group name query, source name, name query and datagram for destination name.

2 The list filter command under NetBIOS filter shows how many packets have been filtered.

Chapter 11. Features and Facilities

This chapter describes the different features provided by the IBM 2210: Bandwidth Reservation (BRS), MAC Filtering (MCF), and WAN Restoral (WRS), also called Dial Backup. It also describes some facilities provided by the IBM 2210, such as the Dial-on-Demand, NetBIOS name caching, and NetBIOS Filtering.

For each feature or facility, a scenario is provided either via the Nways MRS Program on ASCII console connected to the IBM 2210 or via the Nways MRS Configuration Program.

11.1 EasyStart Feature

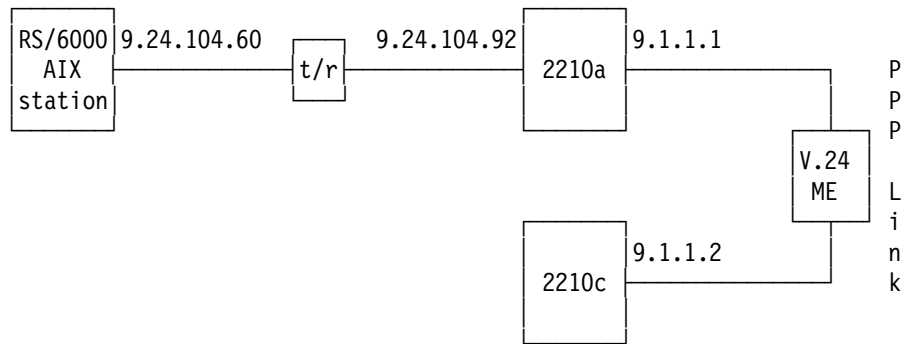
The IBM 2210 now also offers the EasyStart function for automatic configuration capability. When a box is installed in a network, it uses the BootP client/server protocol to solicit its configuration file from a server, typically located at the customer's central site. This does require the host site router to be another IBM 2210 or an IBM 6611 with the complementary EasyStart support, and an associated BootP server containing the respective configuration files. These functions, coupled with the IBM 2210 Configuration Program's capability to easily distribute multiple new configuration files with the timed activation option, make the IBM 2210 an industry leader in the area.

11.2 EasyStart Scenario and Configuration

In this scenario, the RS/6000 AIX station acts both as a BootP and a TFTP server. When IBM 2210 is installed, without any configuration, the BootP command is sent over all connected interfaces. The prerequisite that the IBM 2210 needs to have is an IP address, and if the IBM 2210 is not on the same network as the server a gateway address is also required. The configuration file name is also provided in the first request. When the IBM 2210 has received all the required information, it will restart and do a TFTP to the server defined as BootP server. The configuration file name, stored in the RS/6000 AIX Station, will be transferred to the newly installed IBM 2210 ('2210c' in our case). After the transfer, the IBM 2210 is restarted and the installation is complete.

11.2.1 EasyStart Scenario and Configuration with RS/6000

The following scenario was used to test the EasyStart feature:



Note: 'V.24 ME' means '9.6 kbps V.24 Modem Eliminator'.

At the RS/6000 AIX station the following command (bootptab) was issued:

```
label:vm=rfc1048:sm=255.255.255.0:ht=6:ha=800009010101:ip=9.1.1.2:
T200="ricardo/router.cfg":gw=9.1.1.1:
```

where:

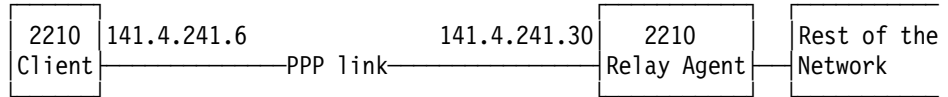
- vm=rfc1048 means that the server must behave according to RFC 1048.
- sm is the host subnet mask.
- If you are in an Ethernet interface then ht=1 (host hardware-type code) and ha= MAC address of the Ethernet adapter.
- If you are in a token-ring interface, then ht=6 and ha= MAC address of the token-ring adapter.
- If you are in a WAN interface, then ht=6 and the address is created as follows:

bit				
47	46-42	41-32	31-0	
must be 1	Unused	Frame Relay DLCI	IP address in hex	

- ip is the IP address of the 2210 to be initialized.
- T200 parameter is a vendor-specific tag as described in RFC 1048.
- gw is the IP address of the gateway address list.

Note

The DLCI and IP addresses refer to the DLCI and IP addresses of the interface on the *relay agent*, not the client. For example, suppose you have the following:



Subnet mask for this link is 255.255.248.0

The bootptab entry would look like this:

```
label:vm=rfc1048:sm=255.255.248.0:ht=6:ha=80008D04F11E:ip=141.4.241.6:  
T200="tmp/router.cfg":
```

Notice that the 8D04F11E is 141.4.241.30 in hex.

The tmp/router.cfg would be replaced with the name of your configuration file.

The configuration process is as follows:

***talk 6**

Config>**protocol ip**

Internet protocol user configuration

IP config>**enable bootp** **1**

Maximum number of forwarding hops [4]?

Minimum seconds before forwarding [0]?

IP config>**add bootp-server**

BOOTP server address [0.0.0.0]? **9.24.104.60** **2**

IP config>**list all**

Interface addresses

IP addresses for each interface:

intf 0	9.24.104.92	255.255.255.0	Network broadcast, fill 1
intf 1			IP disabled on this interface
intf 2	9.1.2.1	255.255.255.0	Network broadcast, fill 1
intf 3	9.1.1.1	255.255.255.0	Network broadcast, fill 1
intf 4			IP disabled on this interface
intf 5			IP disabled on this interface

Internal IP address: 9.24.104.92

Routing

Protocols

BOOTP forwarding: enabled

Max number of BOOTP forwarding hops: 4

Min secs of retry before forwarding: 0

Configured BOOTP servers: 9.24.104.60

Directed broadcasts: enabled

ARP Subnet routing: disabled

RFC925 routing: disabled

OSPF: disabled

Per-packet-multipath: disabled

RIP: enabled

RIP default origination: disabled

Per-interface address flags:

intf 0	9.24.104.92	Send net and subnet routes
		Receive No Dynamic host routes
intf 1		IP & RIP are disabled on this interface
intf 2	9.1.2.1	Send net and subnet routes
		Receive No Dynamic host routes
intf 3	9.1.1.1	Send net and subnet routes
		Receive No Dynamic host routes
intf 4		IP & RIP are disabled on this interface
intf 5		IP & RIP are disabled on this interface

Accept RIP updates always for:

[NONE]

EGP: disabled

IP config>

***restart**

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

MOS Operator Control

*

Figure 161. Configuration

The EasyStart process, with the test parameters, looked like this:

```
PROM Load/Dump Program * Revision: 1.0 *
Copyright 1985-1994 Proteon, Inc. All rights reserved

No valid boot records found, attempting IBD load
Loading using IBD Load Image "v1r3"
-----
Starting at 1040000

Copyright Notices:
Copyright 1985-1995 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

Entering EasyStart operation. Type 'stop' or ^C to terminate.
ELS messages are automatically displayed in this mode.

00:00:00  EZ.001: EasyStart>

Starting.
00:00:01  EZ.007: Waiting up to 6 seconds for devices to pass self-test.
00:00:07  AI.001: Changed params on ifc 0 (Token Ring),
           from 16Mb/s, UTP to 16Mb/s, STP.
00:00:07  EZ.002: Changed one or more cfg params.
00:00:07  BTP.011: net 0, int TKR/0, Could not snd client req because: Ifc not up
00:00:07  BTP.010: net 1, int PPP/0, Sent client request (htype: 6)
00:00:07  BTP.011: net 2, int PPP/1, Could not snd client req because: Ifc not up
00:00:07  BTP.013: net 1, int PPP/0 Unsupported vend tag: 3, len: 4
00:00:07  BTP.007: net 1, int PPP/0, Valid Resp,
           Server: Unknown(9.24.104.60),
           Bootfile: None
           VendOpts config file: /ricardo/router.cfg 3
           IpAddr 9.1.1.2, gwAddr 9.1.1.1 3
00:00:07  EZ.004: Rcvd boot info: ipAddr 9.1.1.2,
           ipMask 255.255.255.0 on intf 1
00:00:07  EZ.009: *** Restarting Router ***
Copyright Notices:
Copyright 1985-1995 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

Entering EasyStart operation. Type 'stop' or ^C to terminate.
ELS messages are automatically displayed in this mode.
00:00:00  EZ.001: EasyStart>
```

Figure 162 (Part 1 of 2). EasyStart

```
Starting.
00:00:01  EZ.007: Waiting up to 6 seconds for devices to pass self-test.
00:00:07 TFTP.025: Starting tftp of file /ricardo/router.cfg from 9.24.104.60 4
00:00:10 TFTP.027: Transfer completed successfully.
          Writing to NVRAM.
00:00:14 TFTP.028: Writing to NVRAM completed.
00:00:14  EZ.008: TFTP transfer completed successfully.
          *** EasyStart Completed Successfully ***
00:00:14  EZ.009: *** Restarting Router ***
```

Copyright Notices:
Copyright 1985-1995 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

Figure 162 (Part 2 of 2). EasyStart

- 1 The enable bootp command: indicates that IBM 2210 must act as a BootP relay agent and forward BootP requests.
- 2 When IBM 2210 acts as BootP agent the BootP servers must be known.
- 3 From the captured EasyStart display you can see the router configuration name, path, gateway address and IP address for the new router.
- 4 Displays the TFTP process.

Note: the IBM 6611 Release V1R4 code *will* have the possibility to act as BootP server to the IBM 2210. This topic has not been tested yet.

11.3 Bandwidth Reservation (BRS)

In this section, we explain what the Bandwidth Reservation (BRS) feature is, we show the Bandwidth Reservation configuration commands, and a scenario of Bandwidth Reservation is provided.

11.3.1 Introduction to Bandwidth Reservation (BRS)

The Bandwidth Reservation feature allows you to reserve part of the bandwidth on the link for a specific traffic type.

Note:

- For Version 1 Release 1 of the Nways MRNS software for the IBM 2210, Bandwidth Reservation is supported only over PPP serial links and applies to outbound traffic only.
- For Version 1 Release 2 of the Nways MRNS software for the IBM 2210, Bandwidth Reservation (BRS) supports the point-to-point protocol, frame relay, and dial circuits (ISDN and V.25bis). Again, this applies to outbound traffic only.

Figure 163 on page 531 shows specific data streams assigned to a part of the WAN bandwidth.

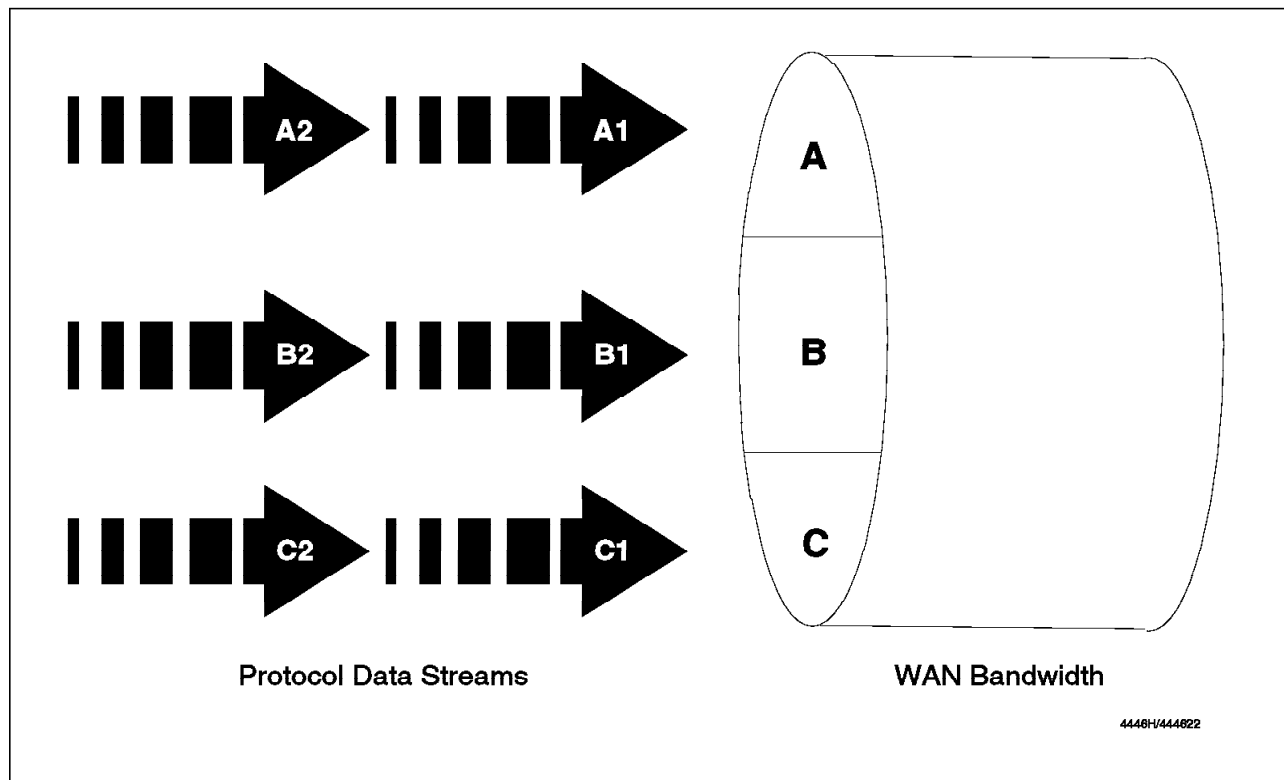


Figure 163. Bandwidth Reservation

First of all, you assign a name to a percentage of the bandwidth. This is called *class name*.

Note: All the names of the classes are case-sensitive.

By default, there are two classes that you can neither delete nor change the name. You are just allowed to change their percentage of the bandwidth. These two classes by default are:

- *LOCAL* with 10% of the bandwidth by default
- *DEFAULT* with 40% of the bandwidth by default

The total of all the percentages of all the classes defined must not exceed 100%.

The reserved percentages are the guaranteed minimum slice of the bandwidth for the network connection. If the network is operating at full capacity, the messages from a specific traffic class can only be transmitted as long as they don't use more bandwidth than allocated for that class. If the rate of the messages exceeds the reserved bandwidth, the messages are held until other bandwidth transmissions have been satisfied.

In the case of light traffic on the network, packet streams can use bandwidth exceeding their allowed minimum (up to a maximum of 100% of the bandwidth) if there is no other traffic.

When you assign a class to a type of traffic, you must also assign the priority class of this traffic within its class. There are four priority classes:

- Low
- Normal

- High
- Urgent

For example, traffic assigned with class *DEFAULT* and priority *urgent* will be delivered faster than traffic assigned with class *DEFAULT* and priority *normal*.

The priority setting within the bandwidth class has no effect on other bandwidth classes. That is, none of the bandwidth classes has priority over the others.

Note: If no priority is assigned within a class, the default priority is *normal*.

After defining the class names, you may assign these classes to the following traffic types:

- The DEFAULT traffic class

The DEFAULT traffic class is used by all traffic that is not assigned to a specific class. By default the DEFAULT traffic class uses the class DEFAULT, with the default class priority normal.

- The protocols (IP, ARP, IPX, ASRT, APL or AP2)

For the protocols, you can assign a specific class and priority for each of the following protocols:

- IP
- ARP
- IPX
- ASRT (Means bridged traffic)
- APL (Appletalk phase 1)
- AP2 (Appletalk phase 2)

- The filter (RLOGIN_IP, TELNET-IP, NetBIOS, SNA Bridged, SNMP-IP, DLSw-IP, MULTICAST-IP, TUNNELING-IP and SDLC-IP)

For the filters, you can assign a specific class and priority for each of the following filters:

- RLOGIN_IP
- TELNET-IP
- NetBIOS (bridged NetBIOS traffic)
- SNA (bridged SNA traffic)
- SNMP-IP
- DLSw-IP (SNA traffic via DLSw)
- MULTICAST-IP
- TUNNELING-IP
- SDLC-IP

- Five tags (from MAC Filtering on bridged traffic only)

You can assign a specific class and priority for the following tags defined by the MAC Filtering (MCF) feature:

- TAG1
- TAG2

- TAG3
- TAG4
- TAG5

Note: The tag number is assigned to a bridged traffic with the MAC Filtering features. See 11.4, “MAC Filtering (MCF)” on page 566 about MAC Filtering.

11.3.2 Bandwidth Reservation (BRS) Configuration Commands

This section summarizes the BRS configuration commands available within the CONFIG process of the Nways MRS and Nways MRS Configuration Program.

To access the BRS feature, you must enter the following command from the CONFIG process:

Config>**feature brs**

Table 70 on page 534 shows the commands available. The *Nways MRS Software User's Guide* covers these commands in detail.

<i>Table 70. BRS Configuration Commands</i>	
Command	Function
? (Help)	Displays the BRS configuration commands, or lists the subcommand options for specific commands (if available).
*Add-circuit-class	Sets the name of a bandwidth class and its percentage of bandwidth.
Add-class	Allocates a designated amount of bandwidth to a user-defined bandwidth class.
Assign	Assigns protocols, filters or tags to a reserved class.
*Assign-circuit	Assigns a specified circuit to the specified bandwidth class.
*Change-circuit-class	Changes the percentage of the bandwidth to be used by the group of circuits assigned to the designated class.
Change-class	Changes the amount of bandwidth configured for a specific bandwidth class.
Clear-block	Clears the current reservation configuration from SRAM. (This command requires a router restart.)
Deassign	Restores the priority and class value of a specified protocol packet or filter to its default class and priority.
*Deassign-circuit	Deassigns the specified circuit from the bandwidth class to which it was assigned.
*Default-circuit-class	Assigns the name of a default bandwidth class and its percentage of the bandwidth to be used by circuits.
Default-class	Sets the default class and priority to a desired value.
*Del-circuit-class	Deletes the specified bandwidth class.
Del-class	Deletes a previously configured bandwidth class from the specified interface.
Disable	Disables bandwidth reservation on the network. (This command requires a router restart.)
Enable	Enables bandwidth reservation on the network. (This command requires a router restart.)
Interface	Selects the serial interface that will run bandwidth reservation. Use this command to enable BRS on a PPP link. (This command must be entered before using any other configuration commands.)
List	Displays the currently defined bandwidth classes by their guaranteed percentage rates and priority queuing values stored in the SRAM display. Also display all assigned protocols and filters.
Show	Displays the currently defined bandwidth classes stored in RAM.
Tag	Assigns a class and priority to a filter that has been tagged during the configuration of the MAC Filtering feature.
Untag	Removes the tag/tag name relationship and the tag name from the list of assignable filters.
Exit	Exits the BRS configuration environment and returns to the CONFIG process.

Note: The commands marked with an asterisk (*) are used only with frame relay.

When configuring frame relay, configure the circuit and the network interface. For PPP, ISDN, and V.25bis, you only need to configure the network interface.

For the Nways MRS Configuration Program, select the **Interface** panel of BRS subdirectory of Features directory.

For example, follow the following steps to customize a Bandwidth Reservation of 60% for IP protocol with priority HIGH, on serial 1 interface:

1. Specify the interface number you wish to customize for Bandwidth Reservation, using the following command:

```
Reservation Config>interface 1
```

For the Nways MRS Configuration Program, select the **Configure** box of serial 1 line of the BRS Interfaces panel.

2. Enable the BRS feature for this interface. This is done using the following command:

```
Reservation Config>enable
```

For the Nways MRS Configuration Program, select **BRS Enable** in the serial 1 line of the BRS Interface panel.

3. When using the Nways MRS Program on the ASCII Console configuration only, restart the 2210 for the above command to take effect. You can do this by returning to the Bandwidth Reservation configuration of interface 1 and issuing the following commands:

```
Reservation Config>exit
Config>Ctrl+p
*Restart
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 6
Gateway user configuration
Config>feature brs
Bandwidth Reservation user configuration
Reservation Config>interface 1
```

Figure 164. Restarting IBM 2210

4. Add a class using 60% of the bandwidth. We will call the name of this class *ipclass*. You can do this by using the following command:

```
Reservation Config>add-class ipclass 60
```

For the Nways MRS Configuration Program, use the Classes subpanel of serial 1 line configuration of the BRS Interfaces panel.

5. Assign the class named *ipclass* to the IP protocol using high priority. This can be done using the following command:

```
Reservation Config>assign ip ipclass high
```

For the Nways MRS Configuration Program, use the Protocol subpanel of the serial 1 line configuration of BRS Interfaces panel.

6. Assign the default class for the protocol, filter or TAGs that are not assigned to any class. To set the default class to the class DEFAULT, issue the following command:

Reservation Config>**default-class default normal**

For the Nways MRS Configuration Program, use the Default Class subpanel of serial 1 line configuration of the BRS Interface panel.

11.3.3 Scenario 1: Bandwidth Reservation (BRS) with IP, IPX and Bridging

In this scenario, we have a 2210 with token-ring interface (2210A) and another 2210 with Ethernet interface (2210B). Both 2210s are linked together through a PPP link with RS-232 modems.

2210A is an IP router, an IPX router and a source route-translational bridge.

2210B is an IP router, an IPX router and a transparent bridge.

- For the interfaces:

2210A token-ring interface runs at 4 Mbps, and is connected to the LAN via the UTP connector and uses the MAC address 40002210A001.

2210B is connected to the Ethernet LAN via the 10Base-T connector.

- For the bridging:

2210A is a source route-translational bridge, with SRB on a token-ring interface, and STB on serial 1 interface. The bridge number of 2210A is 1. The LAN segment number of the token-ring LAN is FF1, and the TB-Domain is seen from SRB Domain as LAN segment number FFF.

2210B is a transparent bridge with STB on both serial 1 and Ethernet interfaces.

- For the IP routing:

2210A is an IP router with IP address 9.67.46.146 on its token-ring interface and IP address 9.67.46.132 on its serial 1 interface. Its internal IP address is 9.67.46.146, and RIP is enabled on both interfaces.

2210B is an IP router with IP address 9.67.46.77 on its Ethernet interface and IP address 9.67.46.131 on its serial 1 interface. Its internal IP address is 9.67.46.77, and RIP is enabled on both interfaces.

- For the IPX routing:

2210A is an IPX router with IPX enabled on both interfaces. IPXWAN is enabled to route IPX over the serial 1 interface. The host number is 40002210A002. The router name is ROUTERA. The node ID is 2210A. The IPX network number of the token-ring interface is BAD1. The IPX network number of the serial 1 interface is BAD2.

2210B is an IPX router with IPX enabled on both interfaces. IPXWAN is enabled to route IPX over the serial 1 interface. The host number is 40002210B002. The router name is ROUTERB. The node ID is 2210B. The IPX network number of the Ethernet interface is 1. The IPX network number of the serial 1 interface is BAD2.

- Bandwidth Reservation feature:

The BRS configuration will be done on both 2210A and 2210B. In this scenario, we wish to set the following classes:

- LOCAL with 10% of the bandwidth
- DEFAULT with 10% of the bandwidth
- IPCALSS with 60% of the bandwidth
- ASRTCLASS with 20% of the bandwidth

Table 71 shows the class and priority assigned to each traffic type.

<i>Table 71. Class and Priority Assigned for Protocols and Filters</i>						
	Default class	IP	IPX	ASRT	Telnet - IP	SNMP - IP
CLASS name	DEFAULT	IPCLASS	DEFAULT	ASRTCLASS	IPCLASS	IPCLASS
priority	normal	high	low	high	normal	urgent

In the notes of this scenario, the customization of the IP protocol, IPX protocol and bridging (ASRT) protocol are not fully described. For more information about IP protocol customization, see 8.2, "Configuring IP on the IBM 2210" on page 341. For more information about IPX Protocol customization, see 9.4, "IPX Configuration on the IBM 2210" on page 413. For more information about Bridging (ASRT) Protocol customization, see 4.4, "Bridging Scenarios and Configurations" on page 138.

- Figure 165 on page 538 shows the configuration of the network for this scenario.
- Figure 166 on page 539 shows the 2210A configuration via the ASCII console.
- Figure 167 on page 546 shows the 2210B configuration via the ASCII console.
- Figure 168 on page 554 shows the 2210A configuration via the Nways MRS Configuration Program.
- Figure 169 on page 560 shows the 2210B configuration via the Nways MRS Configuration Program.

In testing this scenario, OS2PING and TCP/IP PING and IPX client logging were all successful between end user A and B.

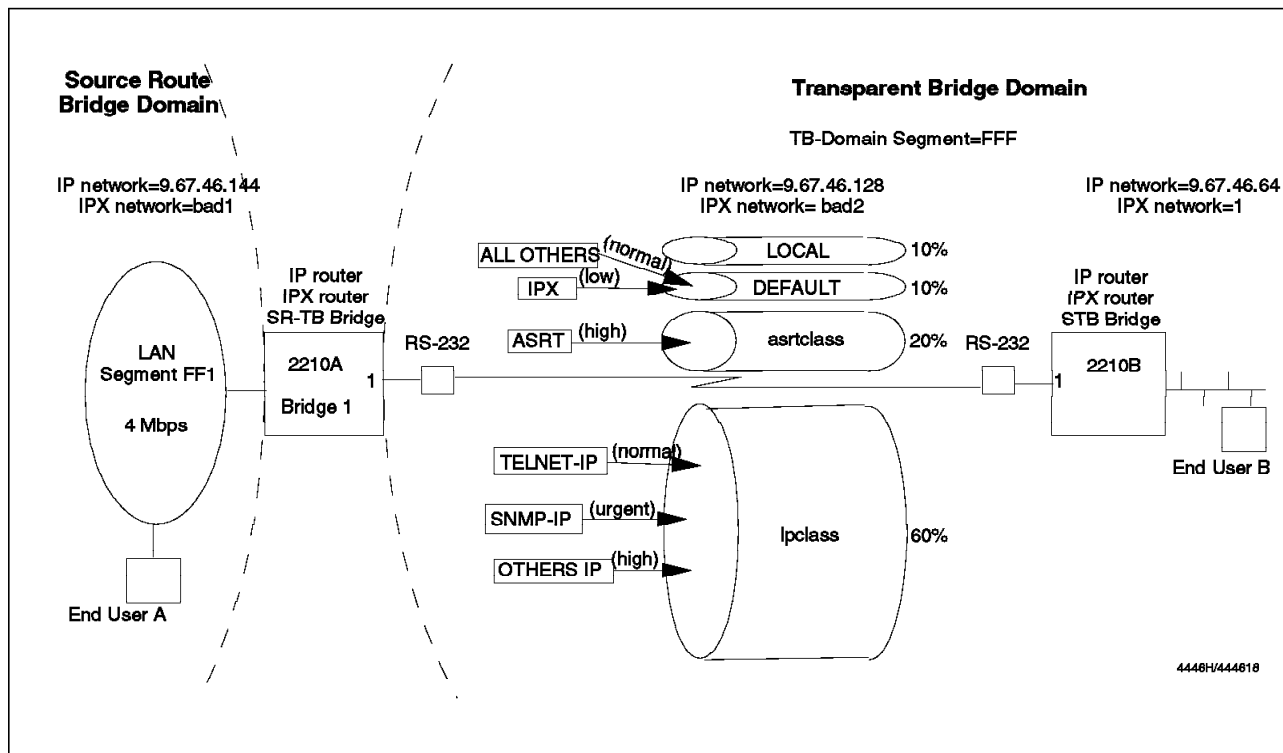


Figure 165. Scenario 1: Bandwidth Reservation (BRS)


```

*
*talk 6 1
Gateway user configuration
Config>network 0 2
Token-Ring interface configuration
TKR config>media unshielded
TKR config>set physical-address 40:00:22:10:A0:01
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec
Media:                    Unshielded

RIF Aging Timer:         120
Source Routing:          Enabled
MAC Address:             40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 3
Point-to-Point user configuration
PPP Config>set hdlc cable rs-232 dte
PPP Config>exit
Config>disable interface 2 4
Config>list devices 5
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
      (Disabled)
Config>protocol ipx 6
IPX protocol user configuration
IPX config>enable ipx
IPX config>enable interface 0
IPX config>enable interface 1
IPX config>enable ipxwan
Which interface [0]? 1
Connection Time-out (in sec) [60]?
Retry Timer (in sec) [60]?
IPX config>set host 40002210A002
IPX config>set node-id 2210a
IPX config>set name routera
IPX config>set net 0 bad1
IPX config>set net 1 bad2

:

```

Figure 166 (Part 1 of 6). Scenario 1: 2210A Configuration via the ASCII Console

```

:
IPX config>list

IPX globally                enabled
Host number (serial line)   40002210A002
Router Name (IPXWAN)        routera
NodeID (IPXWAN)             2210A
Maximum networks            32
Maximum total alt. route entries 128
Maximum alt. routes per dest. network 3
Maximum services            32
Maximum Network Cache entries 64
Maximum Local Cache entries 64
List of configured interfaces:
      Frame
Ifc  IPX net #  Encapsulation      SAP nearest server reply  IPXWAN
0    BAD1      TOKEN-RING        MSB   Enabled              N/A
1    BAD2      N/A                Enabled              Enabled

RIP/SAP Timer Intervals
Net  IPX net #      SAP Interval(Minutes)  RIP Interval(Minutes)
  0    BAD1          1                      1
  1    BAD2          1                      1
IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.
IPX config>exit
Config>protocol ip
Internet protocol user configuration
IP config>add address
Which net is this address for [0]? 0
New address [0.0.0.0]? 9.67.46.146
Address mask [255.0.0.0]? 255.255.255.240
IP config>add address
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.132
Address mask [255.0.0.0]? 255.255.255.240
IP config>set internal IP address 9.67.46.146
IP config>enable rip
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.146      255.255.255.240  Network broadcast,    fill 0
  intf 1  9.67.46.132      255.255.255.240  Network broadcast,    fill 0
  intf 2                                IP disabled on this interface
Internal IP address: 9.67.46.146

Routing

:

```

Figure 166 (Part 2 of 6). Scenario 1: 2210A Configuration via the ASCII Console

```

:
Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0  9.67.46.146      Send net and subnet routes
    intf 1  9.67.46.132      Send net and subnet routes
    intf 2                          IP & RIP are disabled on this interface
Accept RIP updates always for:
[NONE]

EGP: disabled

IP config>exit
Config>protocol asrt 8
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port 1 2
ASRT config>disable transparent 1
ASRT config>enable source-routing 1
Segment Number for the port in hex(1 - FFF) [1]? FF1
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>enable sr-tb
TB-Domain Segment Number in hex(1 - FFF) [1]? FFF
TB-Domain's MTU [1470]?
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:  ENABLED                      Bridge Behaviour: SR<=>TB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number:  1       No. of Source routing segments: 1
SRB: Max ARE Hop cnt:  14             Max STE Hop cnt: 14
SR-TB Conversion: ENABLED  TB-Virtual Segment:0xFFFF  MTU for TB-Domain: 1470
1:N Source Routing:  NOT ACTIVE                Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d on TB ports and IBM-8209 on SR
ports
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number:  1      Interface Number:  0 Port Behaviour: SRB Only
Port Number:  2      Interface Number:  1 Port Behaviour: STB Only

:

```

Figure 166 (Part 3 of 6). Scenario 1: 2210A Configuration via the ASCII Console

```

:
ASRT config>exit
Config>feature brs 9
Bandwidth Reservation user configuration
Reservation Config>interface 1 10
Reservation Config>enable 11
Please restart router for this command to take effect.
Reservation Config>Ctrl+p
*restart 12
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 6 13
Gateway user configuration
Config>feature brs 14
Bandwidth Reservation user configuration
Reservation Config>interface 1 15
Reservation Config>change-class 16
class name: [DEFAULT]?
percent bandwidth to reserve : [10]? 10
Reservation Config>add-class 17
class name: [DEFAULT]? ipclass
percent bandwidth to reserve : [10]? 60
Reservation Config>add-class asrtclass 18
percent bandwidth to reserve : [10]? 20
Reservation Config>assign 19
Protocol or filter name [IP]? ip
class name: [DEFAULT]? ipclass
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]? high
Reservation Config>default-class 20
class name: [DEFAULT]?
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]?
Reservation Config>assign ipx DEFAULT low 21
Reservation Config>assign asrt asrtclass high 22
Reservation Config>assign telnet-ip ipclass normal 23
Reservation Config>assign snmp-ip ipclass urgent 24
:

```

Figure 166 (Part 4 of 6). Scenario 1: 2210A Configuration via the ASCII Console

```

:
Reservation Config>list 25

BANDWIDTH RESERVATION listing from SRAM
network interface number 1
total bandwidth allocated 100%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
  no protocols or filters are assigned to this class.

class DEFAULT has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority
    protocol IPX with priority LOW
    protocol APL with default priority
    protocol AP2 with default priority

class ipclass has 60% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority HIGH
    filter TELNET-IP with priority NORMAL
    filter SNMP-IP with priority URGENT

class asrtclass has 20% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority HIGH

assigned tags:

default class is DEFAULT with priority NORMAL

Reservation Config>exit
Config>Ctrl+p
*restart 26
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

:

```

Figure 166 (Part 5 of 6). Scenario 1: 2210A Configuration via the ASCII Console

```

:
*talk 5 27

CGW Operator Console

+feature brs 28
Bandwidth Reservation console
Reservation>?
INTERFACE
COUNTERS
CLEAR
LAST
EXIT
Reservation>interface 1 29
Reservation>counters 30

Bandwidth Reservation Counters
Interface 1

Class      Pkt Xmit      Bytes Xmit      Bytes Ovfl
LOCAL      87             10541           0
DEFAULT    548            469915          0
ipclass    94             115007           0
asrtclass  587            22999           0

TOTAL      1316           618462           0

Reservation>exit
+Ctrl+p
*
```

Figure 166 (Part 6 of 6). Scenario 1: 2210A Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Customization of network 0. This is the token-ring interface. We specify the unshielded media connector (UTP) and the locally administered address for this interface.
- 3** Customization of network 1. This is the serial 1 interface and uses an RS-232 DTE cable.
- 4** Interface 2 is not used in this scenario.
- 5** List the devices (interfaces) configuration.
- 6** Customization of the IPX protocol. Enable IPXWAN to route IPX over serial 1 link. Also, assign host number, node ID, router name and network number for both interfaces.
- 7** Customization of the IP protocol. Assign IP addresses to both interfaces. Specify the internal IP address and enable RIP.

- 8** Customization of the bridging function. Customize a source route - translational bridge with SRB for token-ring interface and STB for serial 1 interface. Assign LAN segment numbers and bridge number.
- 9** Access the Bandwidth Reservation feature (BRS) configuration.
- 10** This is required each time you enter into the BRS customization and before any other commands. This means the following command will apply for interface 1 (serial 1) only.
- 11** It enables serial 1 for Bandwidth Reservation. You must restart the router for this command to take effect. Otherwise, you will not be allowed to customize Bandwidth Reservation parameters for serial 1.
- 12** Restarting the router as requested.
- 13** Talk to the CONFIG process.
- 14** Access the Bandwidth Reservation feature (BRS) configuration.
- 15** This step is required each time you enter the BRS customization and must be done before you issue any other command. As a result of this step, the commands following the step will apply to interface 1 (serial 1) only.
- 16** Change the DEFAULT class to 10% of the bandwidth.
- 17** Add the IPCLASS class with 60% of the bandwidth.
- 18** Add the ASRTCLASS class with 20% of the bandwidth.
- 19** Assign IP protocol to class IPCALSS with priority HIGH.
- 20** Set the default class to class DEFAULT with priority NORMAL. This step is not really required as it is done by default.
- 21** Assign IPX protocol to class DEFAULT with priority LOW.
- 22** Assign ASRT protocol to class ASRTCLASS with priority HIGH.
- 23** Assign TELNET-IP filter to class IPCLASS with priority NORMAL.
- 24** Assign SNMP-IP filter to class IPCLASS with priority URGENT.
- 25** List the BRS configuration.
- 26** Restart the 2210A to get the configuration running.
- 27** Talk to the gateway operator console.
- 28** Access the Bandwidth Reservation feature (BRS) monitoring.
- 29** This is required each time you enter into BRS monitoring and before you issue any other command.
- 30** List the counters statistic for serial 1.

```

*
*talk 6      1

Config>list devices      2
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>network 1      3
Point-to-Point user configuration
PPP Config>set hdlc cable rs-232 dte
PPP Config>exit
Config>disable interface 2      4
Config>protocol asrt      5
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port 1 2
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:  ENABLED                      Bridge Behaviour: STB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED TB-Virtual Segment:0x0 MTU for TB-Domain: 0
1:N Source Routing: NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation: EXTENDED    FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge: DISABLED
Number of ports added: 2
Port Number: 1      Interface Number: 0 Port Behaviour: STB Only
Port Number: 2      Interface Number: 1 Port Behaviour: STB Only

ASRT config>exit
Config>protocol IP      6
Internet protocol user configuration
IP config>add address
Which net is this address for [0]? 0
New address [0.0.0.0]? 9.67.46.77
Address mask [255.0.0.0]? 255.255.255.240
IP config>add address
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.131
Address mask [255.0.0.0]? 255.255.255.240
IP config>set internal IP address 9.67.46.77
IP config>enable rip

:

```

Figure 167 (Part 1 of 7). Scenario 1: 2210B Configuration via the ASCII Console


```

:
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.77      255.255.255.240  Network broadcast,    fill 0
  intf 1  9.67.46.131     255.255.255.240  Network broadcast,    fill 0
  intf 2                                     IP disabled on this interface
Internal IP address: 9.67.46.77

Routing

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0  9.67.46.77      Send net and subnet routes
    intf 1  9.67.46.131     Send net and subnet routes
    intf 2                                     IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

EGP: disabled

IP config>exit
Config>protocol ipx      7
IPX protocol user configuration
IPX config>enable ipx
IPX config>enable interface 0
IPX config>enable interface 1
IPX config>enable ipxwan
Which interface [0]? 1
Connection Time-out (in sec) [60]?
Retry Timer (in sec) [60]?
IPX config>set host 40002210B002
IPX config>set node-id 2210B
IPX config>set name routerb
IPX config>set net 0 1
IPX config>set net 1 bad2
:

```

Figure 167 (Part 2 of 7). Scenario 1: 2210B Configuration via the ASCII Console

```

:
IPX config>list

IPX globally          enabled
Host number (serial line) 40002210B002
Router Name (IPXWAN)    routerb
NodeID (IPXWAN)         2210B
Maximum networks        32
Maximum total alt. route entries    128
Maximum alt. routes per dest. network 3
Maximum services        32
Maximum Network Cache entries    64
Maximum Local Cache entries    64

List of configured interfaces:

Ifc  IPX net #  Frame Encapsulation      SAP nearest server reply  IPXWAN
0    1          ETHERNET_802.3    Enabled                  N/A
1    BAD2       N/A              Enabled                  Enabled

RIP/SAP Timer Intervals
Net  IPX net #      SAP Interval(Minutes)  RIP Interval(Minutes)
0    1              1                      1
1    BAD2           1                      1

IPX SAP Filter is: disabled
No IPX SAP Filter records in configuration.
IPX Access Controls are: disabled
No IPX Access Control records in configuration.
IPX config>exit
Config>feature brs 8
Bandwidth Reservation user configuration
Reservation Config>? 9
INTERFACE
ENABLE
DISABLE
ADD-CLASS
DEL-CLASS
CHANGE-CLASS
DEFAULT-CLASS
TAG
UNTAG
ASSIGN
DEASSIGN
LIST
SHOW
CLEAR-BLOCK
EXIT
Reservation Config>interface 1 10
Reservation Config>enable 11
Please restart router for this command to take effect.

:

```

Figure 167 (Part 3 of 7). Scenario 1: 2210B Configuration via the ASCII Console

```

:
Reservation Config>add-class 12
First restart router to activate bandwidth reservation.
Reservation Config>exit
Config>Ctrl+p
*restart 13
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 6 14
Gateway user configuration
Config>feature brs 15
Bandwidth Reservation user configuration
Reservation Config>interface 1 16
Reservation Config>list 17

BANDWIDTH RESERVATION listing from SRAM
network interface number 1
total bandwidth allocated 50%
total classes defined (counting one local and one default) 2

class LOCAL has 10% bandwidth allocated
  no protocols or filters are assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with default priority
    protocol ARP with default priority
    protocol IPX with default priority
    protocol APL with default priority
    protocol AP2 with default priority
    protocol ASRT with default priority

assigned tags:

default class is DEFAULT with priority NORMAL

Reservation Config>change-class 18
class name: [DEFAULT]?
percent bandwidth to reserve : [10]? 10

:

```

Figure 167 (Part 4 of 7). Scenario 1: 2210B Configuration via the ASCII Console

```

:
Reservation Config>add-class 19
class name: [DEFAULT]? ipclass
percent bandwidth to reserve : [10]? 60
Reservation Config>add-class 20
class name: [DEFAULT]? asrtclass
percent bandwidth to reserve : [10]? 20
Reservation Config>list

BANDWIDTH RESERVATION listing from SRAM
network interface number 1
total bandwidth allocated 100%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
  no protocols or filters are assigned to this class.

class DEFAULT has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with default priority
    protocol ARP with default priority
    protocol IPX with default priority
    protocol APL with default priority
    protocol AP2 with default priority
    protocol ASRT with default priority

class IPCLASS has 60% bandwidth allocated
  no protocols or filters are assigned to this class.

class asrtclass has 20% bandwidth allocated
  no protocols or filters are assigned to this class.

assigned tags:

default class is DEFAULT with priority NORMAL

Reservation Config>default-class 21
class name: [DEFAULT]?
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]?
:

```

Figure 167 (Part 5 of 7). Scenario 1: 2210B Configuration via the ASCII Console

```

:
Reservation Config>assign ? 22
IP
ARP
IPX
APL
AP2
ASRT
TUNNELING-IP
SDLC-IP
RLOGIN_IP
TELNET-IP
NETBIOS
SNA
SNMP-IP
MULTICAST-IP
DLSw-IP
TAG1
TAG2
TAG3
TAG4
TAG5
Protocol or filter name [IP]? IP
class name: [DEFAULT]? ipclass
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]? HIGH
Reservation Config>assign ipx DEFAULT low 23
Reservation Config>assign 24
Protocol or filter name [IP]? asrt
class name: [DEFAULT]? asrtclass
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]? high
Reservation Config>assign telnet-ip ipclass normal 25
Reservation Config>assign snmp-ip ipclass urgent 26
Reservation Config>list

BANDWIDTH RESERVATION listing from SRAM
network interface number 1
total bandwidth allocated 100%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
no protocols or filters are assigned to this class.

class DEFAULT has 10% bandwidth allocated
the following protocols and filters are assigned:
protocol ARP with default priority
protocol IPX with priority LOW
protocol APL with default priority
protocol AP2 with default priority
:

```

Figure 167 (Part 6 of 7). Scenario 1: 2210B Configuration via the ASCII Console

```

:
class IPCLASS has 60% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority HIGH
    filter TELNET-IP with priority NORMAL
    filter SNMP-IP with priority URGENT

class asrtclass has 20% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority HIGH

assigned tags:

default class is DEFAULT with priority NORMAL

Reservation Config>exit
Config>Ctrl+p
*restart 27
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 167 (Part 7 of 7). Scenario 1: 2210B Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** List the devices (interfaces) configuration.
- 3** Customization of network 1. This is the serial 1 interface and uses an RS-232 DTE cable.
- 4** Interface 2 is not used in the scenario.
- 5** Customization of the bridging function. Customize 2210B as a transparent bridge on both Ethernet and serial 1 interfaces.
- 6** Customization of the IP protocol. Assign IP addresses to both interfaces. Also, assign internal IP address and enable RIP.
- 7** Customization of the IPX protocol. Enable IPXWAN over the serial 1 link. Assign node ID, router name, network name for both interfaces.
- 8** Access the Bandwidth Reservation feature (BRS).
- 9** This shows you all the possible commands for BRS configuration.

- 10** This is required each time you enter the BRS customization and must be issued before any other command. This command results in the following command to apply to interface 1 only.
- 11** Enable serial 1 for Bandwidth Reservation. You must restart the router for this command to take effect. Otherwise, you will not be allowed to customize Bandwidth Reservation parameters for serial 1.
- 12** This shows you that this command has no effect as we have not yet restarted the router.
- 13** This restarts the router as required.
- 14** Talk to the CONFIG process.
- 15** Access the Bandwidth Reservation feature (BRS).
- 16** This is required each time you enter the BRS customization and before issuing any other command. This command results in the following command to apply to interface 1 (serial 1) only.
- 17** List the BRS configuration.
- 18** Change the DEFAULT class to 10% of the bandwidth.
- 19** Add the IPCLASS class with 60% of the bandwidth.
- 20** Add the ASRTCLASS class with 20% of the bandwidth.
- 21** Set the class by default to class DEFAULT with priority NORMAL. This step is not required as it is the default.
- 22** This shows you all the different protocols, filters and tags that you can assign to a class and a priority. Here we assign IP protocol to the class IPCLASS with priority HIGH.
- 23** Assign IPX protocol to class DEFAULT with priority LOW.
- 24** Assign ASRT protocol to class ASRTCLASS with priority HIGH.
- 25** Assign TELNET-IP filter to class IPCLASS with priority NORMAL.
- 26** Assign SNMP-IP filter to class IPCLASS with priority URGENT.
- 27** Restart the 2210B to get the configuration running.

```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 125 2
  Select CONFIGURATION of Token-Ring line 3
  ENABLE INTERFACE
  MAC ADDRESS = 40002210A001
  Select SPEED
  Select 4
  Select PACKET SIZE
  Select 2052
  Select CABLE TYPE
  Select UTP
  RIF TIMER = 120
  DISABLE END NODE SOURCE ROUTING

Select the data-link protocol of Serial 1 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 1 4
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZ
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select RS-232 DTE
  Select subpanel LCP
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

  :

```

Figure 168 (Part 1 of 5). Scenario 1: 2210A Configuration via the Nways MRS Configuration Program


```

:
  Select CONFIGURATION of Serial 2
    On GENERAL subpanel :
      DISABLE INTERFACE 5

On 2210 Navigation Window :
Select GENERAL panel of IP subdirectory of PROTOCOLS directory

On IP - GENERAL Window :
ENABLE IP 6
  Internal Address = 9.67.46.146

On 2210 Navigation Window :
Select INTERFACES panel of IP subdirectory of PROTOCOLS directory

On IP - INTERFACES Window :
  Select IP ADDRESSES of Token-Ring line
    IP Address = 9.67.46.146
    Subnet Mask = 255.255.255.240
    Select ADD
  Select IP ADDRESSES of Serial 1 line
    IP Address = 9.67.46.132
    Subnet Mask = 255.255.255.240
    Select ADD

On 2210 Navigation Window :
Select GENERAL panel of RIP subdirectory of IP subdirectory of PROTOCOLS directory

On RIP - GENERAL Window :
ENABLE RIP 7

On 2210 Navigation Window :
Select GENERAL panel of IPX subdirectory of PROTOCOLS directory

On IPX - GENERAL Window :
ENABLE IPX 8
  HOST NUMBER = 40002210A002

On 2210 Navigation Window :
Select WAN GLOBAL panel of IPX subdirectory of PROTOCOLS directory

On IPX - WAN GLOBAL Window :
  NODE-ID = 2210A
  ROUTER NAME = routera

On 2210 Navigation Window :
Select INTERFACES panel of IPX subdirectory of PROTOCOLS directory

:

```

Figure 168 (Part 2 of 5). Scenario 1: 2210A Configuration via the Nways MRS Configuration Program

:

On IPX - INTERFACES Window :

ENABLE IPX on Token-Ring line
Select **CONFIGURE** on Token-Ring
 IPX NETWORK NUMBER = **bad1**
 Select FRAMING TYPE
 Select TOKEN-RING MSB
ENABLE IPX on Serial 1 line
Select **CONFIGURE** on Serial 1
 ENABLE WAN
 IPX NETWORK NUMBER = **bad2**

On 2210 Navigation Window :

Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :

ENABLE BRIDGING **9**
DISABLE DLSw

In SOURCE ROUTING BRIDGE box

 BRIDGE NUMBER = 1
 MAXIMUM ARE HOP COUNT = 14
 MAXIMUM STE HOP COUNT = 14
 INTERNAL VIRTUAL SEGMENT = 1
 Select LF BIT INTERPRETATION
 Select EXTENDED
 ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box

ENABLE SR <-> TB CONVERSION
 TB: VIRTUAL SEGMENT = FFF

In TRANSPARENT BRIDGE box

 FILT. DBASE SIZE = 2048
 AGING TIME = 300
 RESOLUTION TIME = 5

On 2210 Navigation Window :

Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :

ENABLE Token-Ring
Select **CONFIGURE** of Token-Ring
 Select INTERFACE SUPPORTS
 Select **SRB**
 Select DUPLICATE FRAMES
 Select STE&TSF
 SEGMENT NUMBER = **FF1**
 MTU UNIT = 4399
 ENABLE STE

:

Figure 168 (Part 3 of 5). Scenario 1: 2210A Configuration via the Nways MRS Configuration Program

```

:
ENABLE SERIAL 1
Select CONFIGURE of Serial 2
  Select INTERFACE SUPPORTS
    Select STB
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = 1
  MTU UNIT = 4399
  ENABLE STE

DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

On 2210 Navigation Window :
Select INTERFACES panel of BRS subdirectory of FEATURES directory

On BRS - INTERFACES Window :
ENABLE BRS on Serial 1 line 10
Select CONFIGURE on Serial 1 line
  On CLASSES subpanel
    Select DEFAULT 40 line
      CLASS NAME = DEFAULT
      BANDWIDTH PERCENT = 10
    Select CHANGE 11
      CLASS NAME = ipclass
      BANDWIDTH PERCENT = 60
    Select ADD 12
      CLASS NAME = asrtclass
      BANDWIDTH PERCENT = 20
    Select ADD 13

Select DEFAULT-CLASS subpanel 14
  Select DEFAULT-CLASS
    Select DEFAULT
  Select DEFAULT-CLASS PRIORITY
    Select NORMAL

Select PROTOCOL subpanel
  On IP protocol line
    Select PRIORITY
      Select HIGH 15
    Select CLASS
      Select ipclass 16
  On IPX protocol line
    Select PRIORITY
      Select LOW 17
    Select CLASS
      Select DEFAULT 18

:

```

Figure 168 (Part 4 of 5). Scenario 1: 2210A Configuration via the Nways MRS Configuration Program

```

:
  On ASRT protocol line
    Select PRIORITY
      Select HIGH 19
    Select CLASS
      Select asrtclass 20

  Select FILTER subpanel
    On TELNET-IP protocol line
      Select PRIORITY
        Select NORMAL 21
      Select CLASS
        Select ipclass 22
    On SNMP-IP protocol line
      Select PRIORITY
        Select URGENT 23
      Select CLASS
        Select ipclass 24

  Nothing to customize on TAG subpanel

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select CREATE ROUTER CONFIGURATION 25

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
  Enter BRSA 26
  Select OK

```

Figure 168 (Part 5 of 5). Scenario 1: 2210A Configuration via the Nways MRS Configuration Program

Notes:

- 1** Start the customization from an empty configuration.
- 2** The 2210 is a Model 125, with token-ring LAN, 4 MB Flash, 8 MB RAM, and without the ISDN BRI adapter.
- 3** Customization of the token-ring interface. Assign a locally administered address, and specify the unshielded (UTP) media for the connector type.
- 4** Customization of serial 1. Nothing has been changed from the default. The RS-232 DTE cable is the default.
- 5** Interface 2 is not used in this scenario.
- 6** Customization of the IP protocol. Assign IP addresses to both interfaces. Also, assign the internal IP address.
- 7** Customization of the RIP protocol.
- 8** Customization of the IPX protocol. Assign a host number, node ID, router name, and network number for both interfaces. Enable IPXWAN over serial 1.

9 Customization of the bridging function. Enable bridging and assign a bridge number of 1. SR<->TB conversion is enabled and the TB virtual segment number is set to FFF. Select SRB for the token-ring interface and assign a LAN segment number FF1 to it. Select STB for the serial 1 interface.

10 Enable the Bandwidth Reservation feature (BRS) for serial 1.

11 Change the DEFAULT class to 10% of the bandwidth.

12 Add the IPCLASS class with 60% of the bandwidth.

13 Add the ASRTCLASS class with 20% of the bandwidth.

14 Set the default to class DEFAULT with priority NORMAL. This is the default.

15 Assign HIGH priority to IP protocol.

16 Assign IPCLASS class to IP protocol.

17 Assign LOW priority to IPX protocol.

18 Assign DEFAULT class to IPX protocol.

19 Assign HIGH priority to ASRT protocol.

20 Assign ASRTCLASS class to ASRT protocol.

21 Assign NORMAL priority to TELNET-IP filter.

22 Assign IPCLASS class to TELNET-IP filter.

23 Assign URGENT priority to SNMP-IP filter.

24 Assign IPCLASS class to SNMP-IP filter.

25 Create the configuration file.

26 This is the name of the configuration file stored on the workstation.

```

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select NEW CONFIGURATION 1

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :
  Select MODEL
  Select MODEL 126 2
  Select CONFIGURATION of Ethernet line 3
  ENABLE INTERFACE
  Select CONNECTOR TYPE
  Select AUTO-CONFIG
  Select IP ENCAPSULATION
  Select ETHERNET

Select the data-link protocol of Serial 1 (PPP by default)
  Select PPP

Select CONFIGURATION of Serial 1 4
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
    Select NRZ
    Select IDLE
    Select FLAG
    Select CLOCKING
    Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
    Select RS-232 DTE
  Select subpanel LCP
    RETRY TIMER = 3000
    CONFIG TRIES = 20
    NAK TRIES = 10
    TERMINATE TRIES = 10
    MAXIMUM RECEIVE UNIT = 2048
  Select subpanel BNCP
    ENABLE MAGIC NUMBER
    DISABLE TINYGRAM COMPRESSION
  Select subpanel IPCP
    DISABLE IP Compression
    Number of Slots = 16
    DISABLE SEND IP ADDRESS
    DISABLE REQUEST IP ADDRESS

```

⋮

Figure 169 (Part 1 of 5). Scenario 1: 2210B Configuration via the Nways MRS Configuration Program

```

:
  Select CONFIGURATION of Serial 2
    On GENERAL subpanel :
      DISABLE INTERFACE 5

On 2210 Navigation Window :
Select GENERAL panel of IP subdirectory of PROTOCOLS directory

On IP - GENERAL Window :
ENABLE IP 6
  Internal Address = 9.67.46.77

On 2210 Navigation Window :
Select INTERFACES panel of IP subdirectory of PROTOCOLS directory

On IP - INTERFACES Window :
  Select IP ADDRESSES of Ethernet line
    IP Address = 9.67.46.77
    Subnet Mask = 255.255.255.240
    Select ADD
  Select IP ADDRESSES of Serial 1 line
    IP Address = 9.67.46.131
    Subnet Mask = 255.255.255.240
    Select ADD

On 2210 Navigation Window :
Select GENERAL panel of RIP subdirectory of IP subdirectory of PROTOCOLS directory

On RIP - GENERAL Window :
ENABLE RIP 7

On 2210 Navigation Window :
Select GENERAL panel of IPX subdirectory of PROTOCOLS directory

On IPX - GENERAL Window :
ENABLE IPX 8
  HOST NUMBER = 40002210B002

On 2210 Navigation Window :
Select WAN GLOBAL panel of IPX subdirectory of PROTOCOLS directory

On IPX - WAN GLOBAL Window :
  NODE-ID = 2210B
  ROUTER NAME = routerb

On 2210 Navigation Window :
Select INTERFACES panel of IPX subdirectory of PROTOCOLS directory

:

```

Figure 169 (Part 2 of 5). Scenario 1: 2210B Configuration via the Nways MRS Configuration Program

:

On IPX - INTERFACES Window :

- ENABLE IPX** on Ethernet line
- Select **CONFIGURE** on Ethernet
 - IPX NETWORK NUMBER = **1**
 - Select FRAMING TYPE
 - Select ETHERNET 802.3
- ENABLE IPX** on Serial 1 line
- Select **CONFIGURE** on Serial 1
 - ENABLE WAN**
 - IPX NETWORK NUMBER = **bad2**

On 2210 Navigation Window :

Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :

- ENABLE BRIDGING** **9**
- DISABLE DLSw

In SOURCE ROUTING BRIDGE box

- BRIDGE NUMBER = 1
- MAXIMUM ARE HOP COUNT = 14
- MAXIMUM STE HOP COUNT = 14
- INTERNAL VIRTUAL SEGMENT = 1
- Select LF BIT INTERPRETATION
- Select EXTENDED
- ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box

- DISABLE SR <-> TB CONVERSION

In TRANSPARENT BRIDGE box

- FILT. DBASE SIZE = 2048
- AGING TIME = 300
- RESOLUTION TIME = 5

On 2210 Navigation Window :

Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :

- ENABLE Ethernet**
- Select CONFIGURE of Ethernet
 - Select INTERFACE SUPPORTS
 - Select **STB**
 - Select DUPLICATE FRAMES
 - Select STE&TSF
 - SEGMENT NUMBER = 1

:

Figure 169 (Part 3 of 5). Scenario 1: 2210B Configuration via the Nways MRS Configuration Program


```

:
ENABLE SERIAL 1
Select CONFIGURE of Serial 2
  Select INTERFACE SUPPORTS
    Select STB
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = 1
  MTU UNIT = 4399
  ENABLE STE

DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

On 2210 Navigation Window :
Select INTERFACES panel of BRS subdirectory of FEATURES directory

On BRS - INTERFACES Window :
ENABLE BRS on Serial 1 line 10
Select CONFIGURE on Serial 1 line
  On CLASSES subpanel
    Select DEFAULT 40 line
      CLASS NAME = DEFAULT
      BANDWIDTH PERCENT = 10
    Select CHANGE 11
      CLASS NAME = ipclass
      BANDWIDTH PERCENT = 60
    Select ADD 12
      CLASS NAME = asrtclass
      BANDWIDTH PERCENT = 20
    Select ADD 13

  Select DEFAULT-CLASS subpanel 14
    Select DEFAULT-CLASS
      Select DEFAULT
      Select DEFAULT-CLASS PRIORITY
      Select NORMAL

  Select PROTOCOL subpanel
    On IP protocol line
      Select PRIORITY
        Select HIGH 15
      Select CLASS
        Select ipclass 16
    On IPX protocol line
      Select PRIORITY
        Select LOW 17
      Select CLASS
        Select DEFAULT 18

:

```

Figure 169 (Part 4 of 5). Scenario 1: 2210B Configuration via the Nways MRS Configuration Program

```

:
    On ASRT protocol line
        Select PRIORITY
            Select HIGH 19
        Select CLASS
            Select asrtclass 20

    Select FILTER subpanel
    On TELNET-IP protocol line
        Select PRIORITY
            Select NORMAL 21
        Select CLASS
            Select ipclass 22
    On SNMP-IP protocol line
        Select PRIORITY
            Select URGENT 23
        Select CLASS
            Select ipclass 24

    Nothing to customize on TAG subpanel

On 2210 Navigation Window :
    Select CONFIGURE from the menu bar
        Select CREATE ROUTER CONFIGURATION 25

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
    Enter BRSB 26
    Select OK

```

Figure 169 (Part 5 of 5). Scenario 1: 2210B Configuration via the Nways MRS Configuration Program

Notes:

- 1** Start the customization from an empty configuration.
- 2** The router is a 2210 Model 126, with Ethernet LAN, 4 MB Flash, 8 MB RAM, and without the ISDN BRI adapter.
- 3** Customization of the Ethernet interface. Assign a connector type of AUTOCONFIG. This will let the IBM 2210 automatically discover the type of connector used.
- 4** Customization of serial 1. Nothing has been changed from the default. The RS-232 DTE cable is the default.
- 5** Interface 2 is not used in this scenario.
- 6** Customization of the IP protocol. Assign IP addresses to both interfaces. Also, assign the internal IP address.
- 7** Customization of the RIP protocol.
- 8** Customization of the IPX protocol. Assign a host number, node ID, router name, and network number for both interfaces. Enable IPXWAN to route IPX over serial 1.

- 9** Customization of the bridging function. Enable bridging and select STB for the Ethernet and serial 1 interfaces.
- 10** Enable the Bandwidth Reservation feature (BRS) for serial 1.
- 11** Change the DEFAULT class to 10% of the bandwidth.
- 12** Add the IPCLASS class with 60% of the bandwidth.
- 13** Add the ASRTCLASS class with 20% of the bandwidth.
- 14** Set the default to class DEFAULT with priority NORMAL. It is already the default.
- 15** Assign HIGH priority to IP protocol.
- 16** Assign IPCLASS class to IP protocol.
- 17** Assign LOW priority to IPX protocol.
- 18** Assign DEFAULT class to IPX protocol.
- 19** Assign HIGH priority to ASRT protocol.
- 20** Assign ASRTCLASS class to ASRT protocol.
- 21** Assign NORMAL priority to TELNET-IP filter.
- 22** Assign IPCLASS class to TELNET-IP filter.
- 23** Assign URGENT priority to SNMP-IP filter.
- 24** Assign IPCLASS class to SNMP-IP filter.
- 25** Create the configuration file.
- 26** This is the name of the configuration file stored on the workstation.

11.4 MAC Filtering (MCF)

This section provides a description of the MAC Filtering (MCF) feature as well as the MAC Filtering configuration commands. A scenario of the MAC Filtering configuration on the 2210 is also provided.

11.4.1 Introduction to MAC Filtering (MCF)

The MAC Filtering feature allows you to specify filters to be applied during the bridging process. These filters are based on the source or the destination MAC address of each bridged packet.

The filters may be applied to one or more interfaces in either direction (input or output).

The MAC Filtering (MCF) is supported for bridged traffic only.

Note

MCF is supported over token-ring, Ethernet and PPP serial link only.

Because Dial-on-Demand is not supported over bridging methods and because MAC Filtering is supported only over bridging, MAC Filtering over a Dial-on-Demand serial interface is not supported.

The action of a filter can be the following:

- INCLUDE

This means to bridge the packets normally.

- EXCLUDE

This means to discard the packets.

- TAG

This means to tag the packets with a number from 1 to 64, in order to apply Bandwidth Reservation (BRS) based on the tag number.

Note: Tagged packets are always forwarded via the bridging function.

Note

Because the TAG action in the MAC Filtering feature is used only for Bandwidth Reservation purposes, and because Bandwidth Reservation is supported only via PPP links, the TAG action should only be used for packets that will be bridged through a PPP link.

Figure 170 on page 567 shows the various actions supported by the MAC Filtering feature.

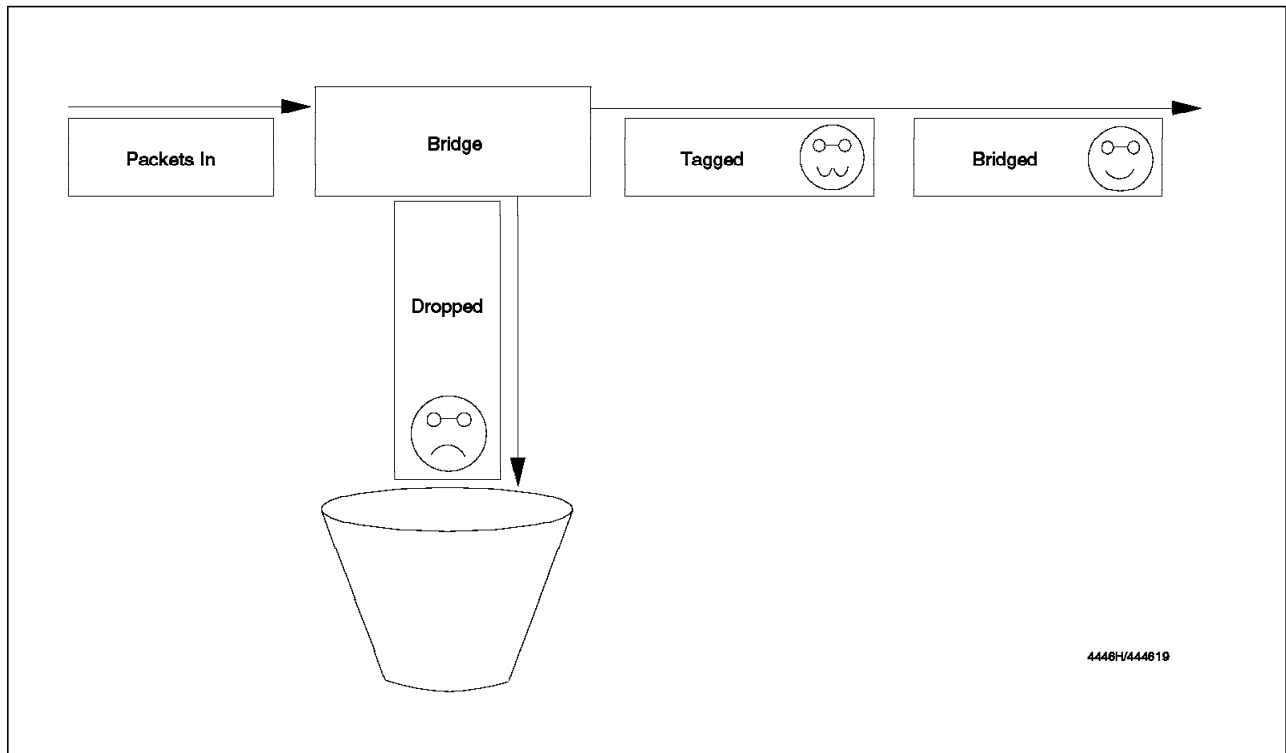


Figure 170. Actions Performed by the MAC Filtering Feature

The following is the description of the terminology used in the MAC Filtering feature:

- A *filter-item* to compare with the source or destination MAC in the packets.
- A *filter-list* is a group of one or more *filter-items*.
- A *filter-list* is attached to one or more *filters*.
- A *filter* is the combination of two parameters:
 - The interface number on which the filter applies
 - The traffic direction on the interface, for which the filter applies (input or output)

Figure 171 on page 568 shows you the MAC Filtering structure.

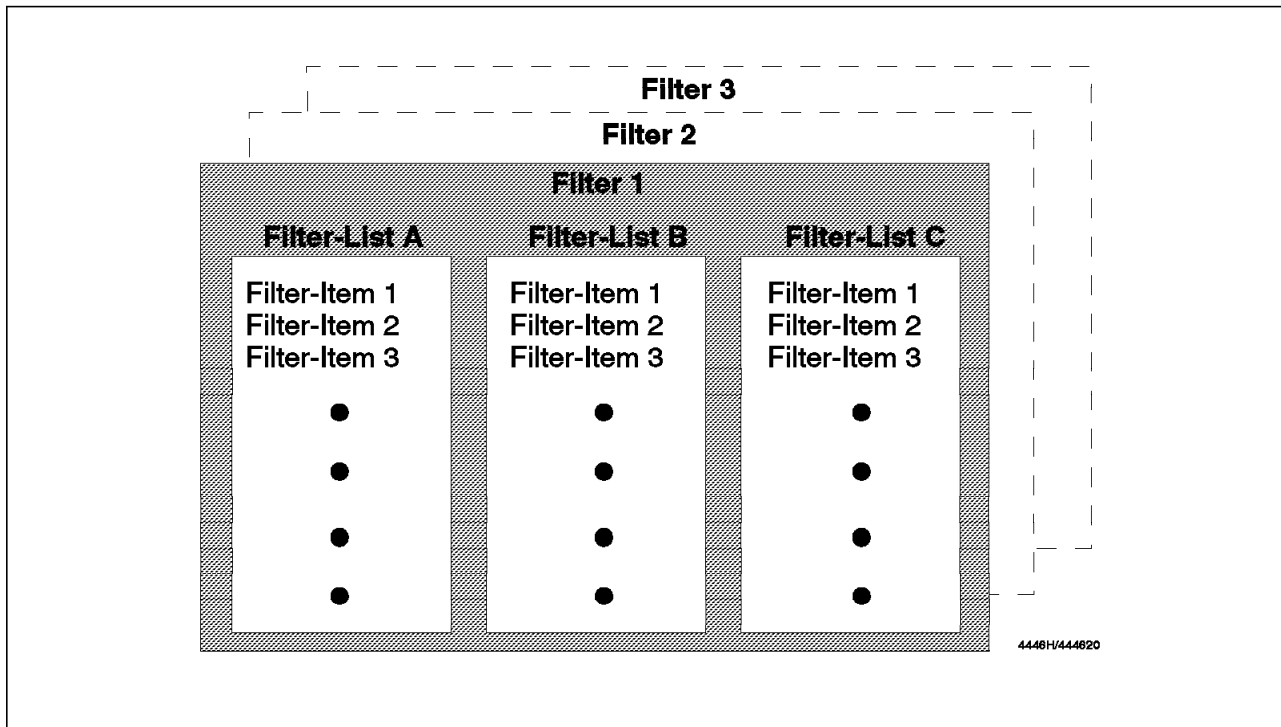


Figure 171. MAC Filtering Structure

The action to perform INCLUDE, EXCLUDE or TAG on a packet is set at the filter-list level containing the filter-item.

If there is no match between the MAC address in a packet and all the filter-items of all the filter-lists attached to a filter, the action performed (INCLUDE, EXCLUDE or TAG) on the packet is the default action set at the filter level.

The order of the filter-items in a filter-list and the order of the filter-lists attached to a filter are very important. The following is a description of how the MAC Filtering process works:

- The MAC Filtering feature compares the MAC address in a packet with the filter-item number 1 in the filter-list number 1.
- If there is no match, the next filter-item (number 2) in the filter-list number 1 is checked. This process continues until the highest filter-item number in the filter-list number 1 has been checked.
- The above process is repeated with the next filter-list (number 2) and will continue until there is either a match with a filter-item or all the filter-items of all the filter-lists have been checked and no match has been found.
- As soon as a filter-item of a filter-list attached to the filter matches the packet's MAC address, the MAC filtering feature performs the action of the filter-list to which the filter-item matching belongs.
- If no filter-item of the filter-lists attached to this filter matches the packet's MAC address, the MAC filtering feature performs the default action of the filter.

Figure 172 on page 569 shows you the MAC Filtering process for a *filter*.

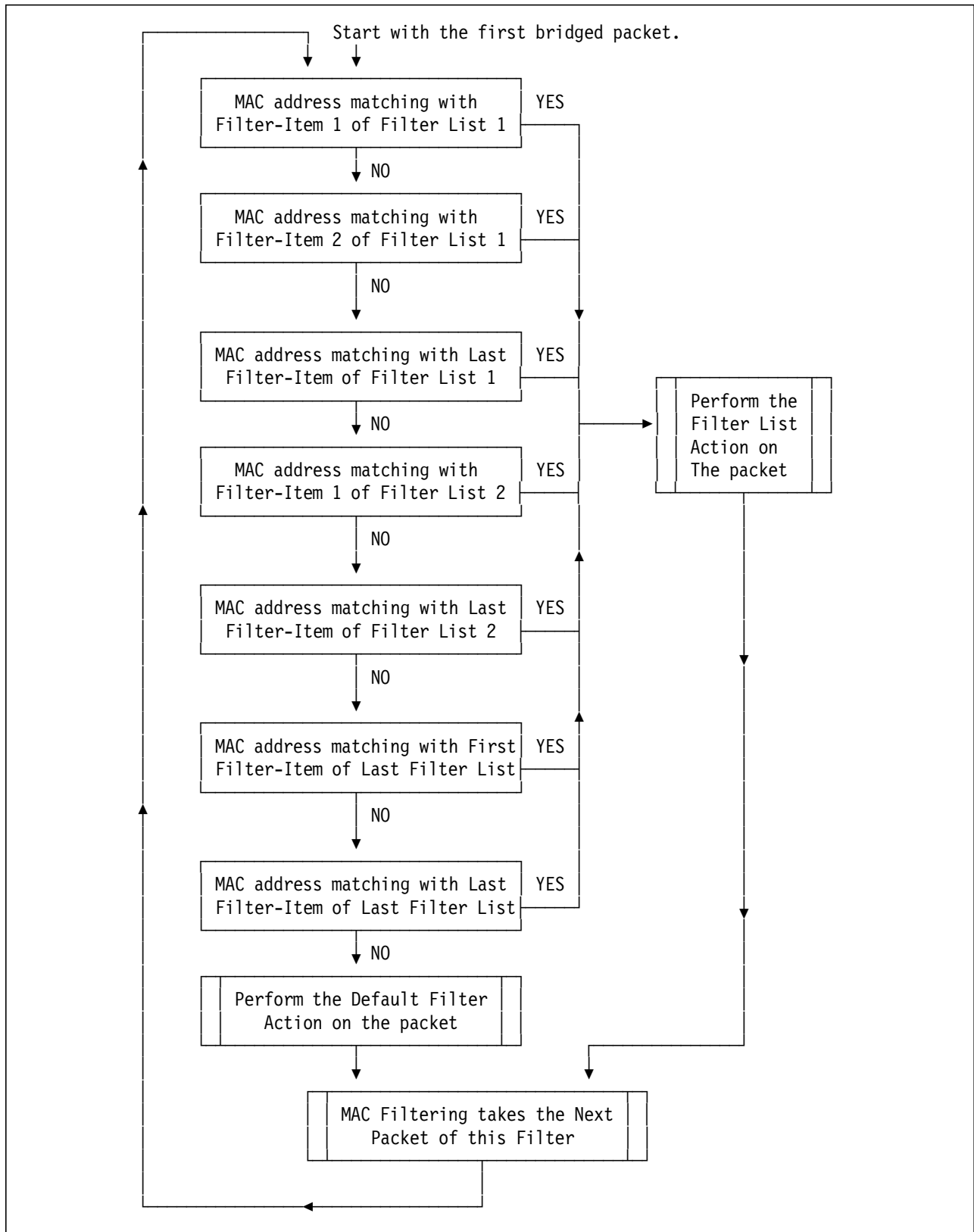


Figure 172. MAC Filtering Process for a Specific Filter

11.4.2 Sliding Window Filter

The sliding window filter is compared to any portion of the frame, as defined by the filter. We can define the portion of the frame that the sliding window is compared to using the offset-value. The offset-value included in the sliding window filter is computed from the beginning of the frame or the beginning of the information field.

To configure the sliding window filter, use the add subcommand of the update command at the Filter filter-list-name config> prompt. To get the Filter filter-list-name config> prompt, enter the following at the Filter config> prompt:

```
update filter-list-name
```

Type:

```
add window mac offset-value hex-data hex-mask  
add window info offset-value hex-data hex-mask
```

For example:

```
add window mac 14 f4f403 fffffff  
add window info 0 f4f403 fffffff
```

11.4.3 MAC Filtering (MCF) Configuration Commands

This section summarizes the MAC Filtering configuration commands available within the CONFIG process of the Nways MRS and within Nways MRS Configuration Program.

To access the MAC Filtering feature you must enter the following command from the CONFIG process:

```
Config>feature mcf
```

For the Nways MRS Configuration Program, select the **General** or the **Details** of the MAC Filter-Lists subdirectory of the MAC Filtering subdirectory of the Features directory or the **Interface** panel of the MAC Filtering subdirectory of the Features directory. Selecting Interfaces panel displays the MAC Filtering window, and selecting the MAC Filter-Lists panel displays the MAC Filter-List window.

Table 72 on page 571 shows the available MAC Filtering commands.

Table 73 on page 571 shows the available MAC Filtering update subcommands.

The *Nways MRS Software User's Guide* covers these commands in detail.

Table 72. MAC Filtering Configuration Commands	
Command	Function
? (Help)	Displays the MAC Filtering commands, or lists subcommand options for specific commands (if available).
Attach	Attaches a <i>filter-list</i> to a <i>filter</i> .
Create	Creates a <i>filter-list</i> or a <i>filter</i> .
Default	Sets the default action for a <i>filter</i> with its specified filter number to EXCLUDE, INCLUDE or TAG.
Delete	Deletes a <i>filter-list</i> with all its <i>filter-items</i> . Also deletes a <i>filter</i> previously created.
Detach	Detaches a <i>filter-list</i> from a <i>filter</i> .
Enable	Enables MAC Filtering entirely or enables a specific <i>filter</i> .
List	Lists a summary of all the <i>filters</i> and <i>filter-lists</i> configured by the user. Also generates a list of attached <i>filter-lists</i> for this <i>filter</i> and all subsequent information for the <i>filter</i> .
Move	Reorders the <i>filter lists</i> attached to a specified <i>filter</i> .
Reinit	Reinitializes the entire MAC Filtering system from an existing configuration without affecting the rest of the router.
Set-cache	Changes the cache size for a filter.
Update	Updates information for a specific <i>filter-list</i> . It brings you to a new prompt with a new menu of appropriate subcommands. Table 73 shows you these new subcommands.
Exit	Exits the MAC Filtering configuration environment and returns to the CONFIG process.

Table 73. MAC Filtering Update Subcommands	
Command	Function
? (Help)	Displays all the Update subcommands.
Add	Adds a <i>filter-item</i> to a <i>filter-list</i> . Adds a hexadecimal number with a hexadecimal mask to compare against the Source or Destination MAC address. Adds an offset-value and a hexadecimal number with a hexadecimal mask as the sliding window filter.
Delete	Deletes a <i>filter-item</i> from a <i>filter-list</i> .
List	Lists all the <i>filter-items</i> configured by the user for a <i>filter-list</i> . You can list either in canonical or non-canonical MAC address format.
Move	Reorders the <i>filter-items</i> attached to a <i>filter list</i> .
Set-action	Sets the action for a <i>filter-list</i> to INCLUDE, EXCLUDE or TAG.
Exit	Exits the MAC Filtering update subcommands environment and returns to MAC Filtering commands.

The following is an example of how to exclude packets with the non-canonical source MAC address of 400000033350 in the INPUT traffic of the token-ring interface:

1. Enable the MAC Filtering. This is done by using the following command:

```
Filter Config>enable all
```

For the Nways MRS Configuration Program, select **Enable MAC Filtering** in the MAC Interfaces window.

2. Create a filter-list with a name you have chosen. Let's call it mylist in this example. This is done by using the following command:

```
Filter Config>create list mylist
```

For the Nways MRS Configuration Program, see the General subpanel of the MAC Filter-List window.

3. Configure this filter-list. You must use the Update command as follows:

```
Filter Config>update mylist
```

The following prompt will be displayed:

```
Filter 'mylist' Config>
```

4. Add filter-items to the filter-list. This is done via the Add command which adds source or destination MAC addresses along with their corresponding *hexadecimal mask* to the filter. The hexadecimal-mask works as follows:

- The comparison between the MAC address of the bridged packet, and the MAC address customized in the filter-item will be done only on the bits where their value is set to B1 in the hexadecimal-mask. For example, to ignore the routed information indicator bit (first bit of the source MAC address in the source-routed bridged packets), you must enter the following hexadecimal-mask:

```
7F:FF:FF:FF:FF:FF.
```

To match the non-canonical MAC address 400000033350 to the source MAC address of the source-routed bridged packet, issue the following command:

```
Filter 'mylist' Config>add source 40:00:00:03:33:50 7f:ff:ff:ff:ff:ff
```

In this case, either 400000033350 or C00000033350 source MAC address will match this filter-item.

For the Nways MRS Configuration Program, use the Filter-Items subpanel of the MAC Filter-List window.

5. All the filter-items that belong to the same filter-list will have the same action. You must assign the action to the filter-list using the Set-action command for the filter-list. In this command, you must set the action that will be performed when one of the the filter-items of this filter-list matches the MAC address in the bridged packets. The specified action can be one of the following:

- INCLUDE
- EXCLUDE
- TAG

To set the EXCLUDE action for all filter-items of the filter-list called mylist, you must issue the following command:

```
Filter 'mylist' Config>set-action exclude
```

For the Nways MRS Configuration Program, use the General subpanel of the MAC Filter-List window.

Note: For the Nways MRS Configuration Program only, the action of the filter-list must be defined when you create the filter-list.

6. Exit the update subcommand configuration process by using the following command:

Filter 'mylist' Config>**exit**

The new prompt will be:

Filter Config>

7. Create a filter to which the filter-list is attached. For example you can create the filter for the INPUT traffic on interface 0, using the following command:

Filter Config>**create filter input 0**

8. Issue a list command to note the filter number assigned to the filter you have just created. This is done by using the following command:

Filter Config>**list all**

For the Nways MRS Configuration Program, the six possible filters are in the MAC Interfaces window.

9. Each of the six possible filters may either be *enabled* or *disabled*. The default is already *enabled*.

To enable/disable a filter, you must refer to the filter number (displayed by the List All command). For example, if the filter number is 1, issue the following command to to enable it:

Filter Config>**enable filter 1**

For the Nways MRS Configuration Program, use the Filter-Item subpanel of the MAC Filter-List window.

10. Attach the filter-list to the filter.

Note: A filter-list could be attached to more than one filter at the same time. Also, you can attach several filter-lists to the same filter.

To attach the filter-list called *mylist* to the filter number 1, created earlier, issue the following command:

Filter Config>**attach mylist 1**

For the Nways MRS Configuration Program, use the Filter-Lists subpanel of the MAC Filtering window.

11. We have now customized the filter to exclude all packets with the non-canonical source MAC address of 400000033350 for INPUT traffic of the token-ring interface.
12. Each filter has a *default action*. The default action applies to every packet that does not match any filter-item of any filter-list attached to this filter. The default-actions can be one of the following:
 - INCLUDE
 - EXCLUDE
 - TAG

For example, we have previously customized the router to exclude all packets with a specific source MAC address in INPUT traffic of interface 0.

To include all other packets of a token-ring interface in INPUT traffic, we must set the default-action of INCLUDE for the filter number 1, using the following command:

```
Filter Config>default include 1
```

For the Nways MRS Configuration Program, use the General subpanel of the MAC Filtering window.

Note

When you set an action for tags, (either a filter-list action or a default-filter action), you must specify the TAG value. This TAG value is a number between 1 and 64, which is also used by the Bandwidth Reservation feature commands.

For example, for a TAG value of 1, customized in the MAC Filtering feature, issue the following BRS command:

```
Reservation Config>tag 1
```

For the Nways MRS Configuration Program, use the TAG subpanel of the corresponding serial configuration of the BRS Interfaces window.

For more information about Bandwidth Reservation, see 11.3, “Bandwidth Reservation (BRS)” on page 530. An example of the filter action of TAG is provided in the following scenario on 11.4.4, “Scenario 2: MAC Filtering (MCF).”

11.4.4 Scenario 2: MAC Filtering (MCF)

In this scenario, we have a 2210 with token-ring interface (2210A) and a 2210 with Ethernet interface (2210B). Both 2210s are linked together using a PPP link with RS-232 modems.

The 2210A is a source route-translational bridge. 2210B is a transparent bridge.

- Interfaces:

2210A token-ring runs at 4 Mbps, and is attached to the LAN using the UTP connector. The MAC address of the token-ring interface on the 2210A is 40002210A001.

2210B Ethernet is attached to the Ethernet LAN using the 10Base-T connector.

- Bridging:

2210A is a source route-translational bridge with SRB on the token-ring interface, and STB on the serial 1 interface. The bridge number of 2210A is 1. The LAN segment number of the 2210A on the token-ring is FFB, and the TB-Domain is seen from SRB Domain as the LAN segment number FFF.

2210B is a transparent bridge with STB on both serial 1 and Ethernet interfaces.

- MAC Filtering (MCF):

- For 2210A INPUT traffic on a token-ring interface the following MAC Filtering is used:

- TAG packets with a non-canonical source address of 400000033350 with the TAG number 1.
- EXCLUDE packets with a non-canonical source address beginning with 40000ABCD1.
- EXCLUDE packets with a non-canonical destination address of C00000000080 (this is the NetBIOS Multicast MAC address).
- INCLUDE all other packets.
- For 2210B OUTPUT traffic on the serial 1 interface the following MAC Filtering is used:
 - EXCLUDE packets with a canonical source address of 08005A6158CF.
 - INCLUDE all other packets.
- Bandwidth Reservation (BRS):

On 2210A, we assign 30% of the bandwidth to the tagged packet with TAG number 1.

For more information about ASRT protocol customization, see 4.4, “Bridging Scenarios and Configurations” on page 138.

To test this configuration, we have the following end users:

- On the token-ring segment of 2210A:
 - End user A1 with a non-canonical MAC address = 400000033350
 - End user A2 with a non-canonical MAC address = 40000ABCD123
 - End user A3, a NetBIOS station
- On the Ethernet segment of 2210B:
 - End user B1 with a canonical MAC address = 08005A415A56
 - End user B2 with a canonical MAC address = 08005A6158CF
 - End user A3, a NetBIOS station

Figure 173 on page 576 shows the configuration of the network used in this scenario.

For the configuration parameters used in this scenario, refer to the following:

- Figure 174 on page 577 shows the 2210A configuration via an ASCII console.
- Figure 175 on page 585 shows the 2210B configuration via an ASCII console.
- Figure 176 on page 589 shows the 2210A configuration via the Nways MRS Configuration Program.
- Figure 177 on page 595 shows the 2210B configuration via the Nways MRS Configuration Program.

In the testing of this scenario:

- OS2PING and TCP/IP PING were successful between end user A1 and B1.
- OS2PING and TCP/IP PING failed between end user A2 and either B1 or B2.
- OS2PING and TCP/IP PING failed between end user B2 and either A1 or A2.

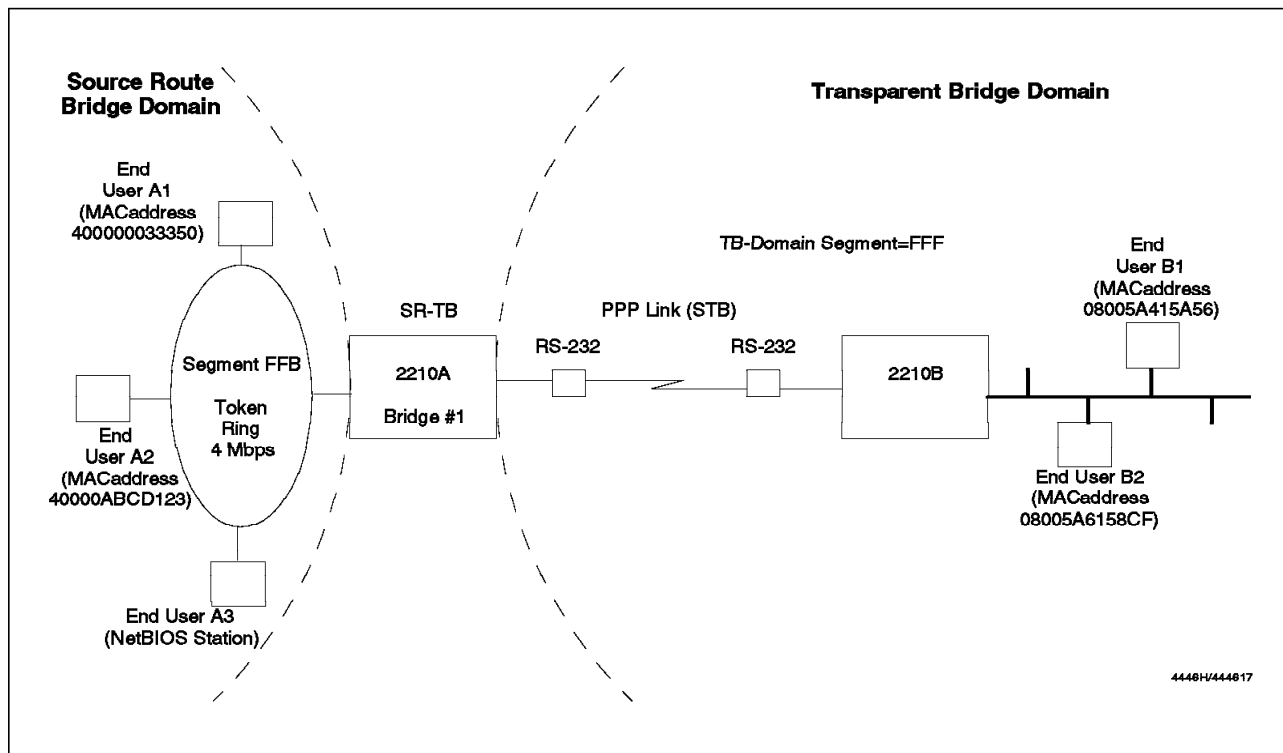


Figure 173. Scenario 2: MAC Filtering (MCF)

```

*
*talk 6 1

Config>network 0 2
Token-Ring interface configuration
TKR config>media unshielded
TKR config>set physical-address 40:00:22:10:A0:01
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                      4 Mb/sec
Media:                      Unshielded

RIF Aging Timer:           120
Source Routing:            Enabled
MAC Address:               40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 3
Point-to-Point user configuration
PPP Config>set hdlc cable rs-232 dte
PPP Config>list hdlc

Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Internal Clock Speed: 0

Transmit Delay Counter: 0
PPP Config>exit
Config>disable interface 2 4
Config>list devices 5
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
(Disabled)
Config>protocol asrt 6
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port 1 2
ASRT config>disable transparent 1
ASRT config>enable source-routing 1
Segment Number for the port in hex(1 - FFF) [1]? FFB
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>enable sr-tb-conversion
TB-Domain Segment Number in hex(1 - FFF) [1]? FFF
TB-Domain's MTU [1470]?

:

```

Figure 174 (Part 1 of 7). Scenario 2: 2210A Configuration via the ASCII Console

```

:
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge:   ENABLED                      Bridge Behaviour: SR<->TB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 1        No. of Source routing segments: 1
SRB: Max ARE Hop cnt: 14              Max STE Hop cnt: 14
SR-TB Conversion: ENABLED  TB-Virtual Segment:0xFFFF  MTU for TB-Domain: 1470
1:N Source Routing:  NOT ACTIVE        Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d on TB ports and IBM-8209 on SR
ports
DLS for the bridge: DISABLED
Number of ports added: 2
Port Number: 1   Interface Number: 0 Port Behaviour: SRB Only
Port Number: 2   Interface Number: 1 Port Behaviour: STB Only

ASRT config>exit
Config>feature mcf 7
MAC Filtering user configuration
Filter Config>list all 8
Filtering: disabled
Filter List                      Action
-----
Filters
-----
Id  Default  State  Ifc  Dir  Cache
--  -
Filter Config>enable all 9
Filter Config>? 10
ATTACH
CREATE
DEFAULT
DELETE
DETACH
DISABLE
ENABLE
LIST
MOVE
REINIT
SET-CACHE
UPDATE
EXIT
Filter Config>create list filtlisttag 11
:

```

Figure 174 (Part 2 of 7). Scenario 2: 2210A Configuration via the ASCII Console


```

:
Filter Config>list all
Filtering: enabled
Filter List                      Action
-----
filtlisttag                      INCLUDE

Filters
-----
Id  Default  State  Ifc  Dir  Cache
--  -
Filter Config>update filtlisttag 12
Filter 'filtlisttag' Config>? 13
ADD
DELETE
LIST
MOVE
SET-ACTION
EXIT
Filter 'filtlisttag' Config>add source 40:00:00:03:33:50 7f:ff:ff:ff:ff:ff 13
Filter 'filtlisttag' Config>list canonical 15
Action: INCLUDE
Id  Type  MAC Address  Mask
--  -
1   SRC   02-00-00-C0-CC-0A  FE-FF-FF-FF-FF-FF
Filter 'filtlisttag' Config>list noncanonical 16
Action: INCLUDE
Id  Type  MAC Address  Mask
--  -
1   SRC   40:00:00:03:33:50  7F:FF:FF:FF:FF:FF
Filter 'filtlisttag' Config>set-action tag 1 17
Filter 'filtlisttag' Config>exit
Filter Config>list all
Filtering: enabled
Filter List                      Action
-----
filtlisttag                      TAG( 1)

Filters
-----
Id  Default  State  Ifc  Dir  Cache
--  -
Filter Config>create filter input 0 18
Filter Config>list all
Filtering: enabled
Filter List                      Action
-----
filtlisttag                      TAG( 1)

:

```

Figure 174 (Part 3 of 7). Scenario 2: 2210A Configuration via the ASCII Console

```

:
Filters
-----
Id   Default  State   Ifc Dir   Cache
--   -
1    INCLUDE  ENABLE  0   INPUT  16
Filter Config>attach filtlisttag 1      19
Filter Config>create list filtlistex    20
Filter Config>update filtlistex         21
Filter 'filtlistex' Config>add source 40:00:0a:bc:d1:00      22
Enter MAC Mask [ffffffffffff]? 7f:ff:ff:ff:ff:00
Filter 'filtlistex' Config>list noncanonical
Action: INCLUDE
Id Type  MAC Address          Mask
-- --
1  SRC   40:00:0A:BC:D1:00    7F:FF:FF:FF:FF:00
Filter 'filtlistex' Config>list canonical
Action: INCLUDE
Id Type  MAC Address          Mask
-- --
1  SRC   02-00-50-3D-8B-00    FE-FF-FF-FF-FF-00
Filter 'filtlistex' Config>set-action exclude                23
Filter 'filtlistex' Config>add destination c0:00:00:00:00:80  24
Enter MAC Mask [ffffffffffff]?
Filter 'filtlistex' Config>list noncanonical
Action: EXCLUDE
Id Type  MAC Address          Mask
-- --
1  SRC   40:00:0A:BC:D1:00    7F:FF:FF:FF:FF:00
2  DST   C0:00:00:00:00:80    FF:FF:FF:FF:FF:FF
Filter 'filtlistex' Config>exit
Filter Config>attach filtlistex 1      25
Filter Config>list all
Filtering: enabled
Filter List          Action
-----
filtlisttag          TAG( 1)
filtlistex           EXCLUDE

Filters
-----
Id   Default  State   Ifc Dir   Cache
--   -
1    INCLUDE  ENABLE  0   INPUT  16
Filter 'filtlistex' Config>exit
Filter Config>exit
:

```

Figure 174 (Part 4 of 7). Scenario 2: 2210A Configuration via the ASCII Console

```

:
Config>feature brs 26
Bandwidth Reservation user configuration
Reservation Config>interface 1
Reservation Config>enable
Please restart router for this command to take effect.
Reservation Config>exit
Config>Ctrl+p
*restart
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
*talk 6
Config>feature brs
Bandwidth Reservation user configuration
Reservation Config>interface 1
Reservation Config>add-class tagclass 30
Reservation Config>tag 1 27
Reservation Config>list all

BANDWIDTH RESERVATION listing from SRAM
network interface number 1
total bandwidth allocated 80%
total classes defined (counting one local and one default) 3

class LOCAL has 10% bandwidth allocated
no protocols or filters are assigned to this class.

class DEFAULT has 40% bandwidth allocated
the following protocols and filters are assigned:
protocol IP with default priority
protocol ARP with default priority
protocol IPX with default priority
protocol APL with default priority
protocol AP2 with default priority
protocol ASRT with default priority

class tagclass has 30% bandwidth allocated
no protocols or filters are assigned to this class.

:

```

Figure 174 (Part 5 of 7). Scenario 2: 2210A Configuration via the ASCII Console

```

:
assigned tags:
  TAG1 represents filter tag 1

default class is DEFAULT with priority NORMAL

Reservation Config>assign TAG1 tagclass high
Reservation Config>list all

BANDWIDTH RESERVATION listing from SRAM
network interface number 1
total bandwidth allocated 80%
total classes defined (counting one local and one default) 3

class LOCAL has 10% bandwidth allocated
  no protocols or filters are assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with default priority
    protocol ARP with default priority
    protocol IPX with default priority
    protocol APL with default priority
    protocol AP2 with default priority
    protocol ASRT with default priority

class tagclass has 30% bandwidth allocated
  the following protocols and filters are assigned:
    filter TAG1 with priority HIGH logically set to tag 1

assigned tags:
  TAG1 represents filter tag 1

default class is DEFAULT with priority NORMAL

Reservation Config>exit
Config>Ctrl+p
*restart
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*

:

```

Figure 174 (Part 6 of 7). Scenario 2: 2210A Configuration via the ASCII Console

```

:
*talk 5 30

+feature mcf
Filter>list all
MAC Filtering: enabled
Id Default  State Ifc  Dir Cache  Hit%  Inc      Exc      Tag
--
1 INCLUDE  ENA   0   IN  16    40.10 164     226     19
Filter>exit
+feature brs
Bandwidth Reservation console
Reservation>interface 1
Reservation>counters

Bandwidth Reservation Counters
Interface 1

Class      Pkt Xmit      Bytes Xmit      Bytes Ovfl
LOCAL      0          0          0
DEFAULT    2147      114745     0
tagclass    37        4144      0
TOTAL      2184      118889     0

Reservation>exit
+Ctrl+p
*

```

Figure 174 (Part 7 of 7). Scenario 2: 2210A Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Customization of network 0. This is the token-ring interface. Specify the unshielded media connector (UTP), and the locally administered address for this interface.
- 3** Customization of network 1. This is the serial 1 interface. Specify the RS-232 DTE cable that is used.
- 4** Interface 2 is not used in this scenario.
- 5** List the devices (interfaces) configuration.
- 6** Customization of the bridging function. Customize a source route - translational bridge with SRB for the token-ring interface and STB for serial 1 interface. Assign the LAN segment numbers and bridge number.
- 7** Access the MAC Filtering (MCF) configuration.
- 8** Lists the MAC Filtering (MCF) configuration.
- 9** Enable the MAC Filtering (MCF) feature.

- 10** This shows all the commands available on the MAC Filtering (MCF) configuration.
- 11** Create the filter-list named FILTLISTTAG.
- 12** Access the FILTLISTTAG filter-list configuration.
- 13** This shows you all the subcommands available on the MAC Filtering (MCF) filter-list configuration.
- 14** Add a filter-item for non-canonical MAC address 400000033350, with mask 7FFFFFFFFFFF to the FILTLISTTAG filter-list.
- 15** List all the filter-items of the FILTLISTTAG filter-list and display the MAC address and the mask in canonical format.
- 16** List all the filter-items of the FILTLISTTAG filter-list and display the MAC address and the mask in non-canonical format.
- 17** Set the action of FILTLISTTAG filter-list to TAG with TAG value number 1.
- 18** Create filter on interface 0 (token-ring interface) for INPUT traffic. The list all command shows that this filter is the assigned the number 1.
- 19** Attach FILTLISTTAG filter-list to the filter number 1.
- 20** Create the filter-list named FILTLISTEX.
- 21** Access the configuration of the FILELISTEX filter-list.
- 22** Add a filter-item for non-canonical source MAC address 40000ABCD100, with mask 7FFFFFFFFF00 to the FILTLISTEX filter-list.
- 23** Set the action of the FILTLISTEX filter-list to EXCLUDE.
- 24** Add a filter-item for non-canonical destination MAC address C00000000080, with mask FFFFFFFFFFFF (the default mask) to the FILTLISTEX filter-list.
- 25** Attach the FILTLISTEX filter-list to the filter number 1.
- 26** Access the Bandwidth Reservation (BRS) feature to configure a bandwidth class named TAGCLASS. Reserve 30% of the bandwidth of serial 1 interface for packets tagged with a TAG value of 1.
- 27** Assign one of the five tags to the TAG value 1. The tag assigned can be seen with the list all command. TAG1 has been assign to TAG value 1.
- 28** Assign TAG1 traffic to the TAGCLASS class with HIGH priority.
- 29** Restart the 2210A to get the configuration running.
- 30** Talk to the gateway operator console and access the MAC Filtering feature (MCF) monitoring to list the actions performed by the filters. Also, access the Bandwidth Reservation feature (BRS) monitoring to list the counters statistic for serial 1.

```

*
*talk 6 1

Config>network 0 2
Ethernet interface configuration
ETH config>list
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 1 3
Point-to-Point user configuration
PPP Config>set hdlc cable rs-232 dte
PPP Config>exit
Config>disable interface 2 4
Config>list devices 5
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
      (Disabled)
Config>protocol asrt 6
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port 1 2
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:  ENABLED                      Bridge Behaviour: STB
Bridge Address: Not Specified By User  Bridge Priority:(dec) 32768, (hex): 8000
Source Routing Bridge Number: 0        No. of Source routing segments: 0
SRB: Max ARE Hop cnt: 0                Max STE Hop cnt: 0
SR-TB Conversion: DISABLED  TB-Virtual Segment:0x0  MTU for TB-Domain: 0
1:N Source Routing:  NOT ACTIVE          Internal-Virtual Segment:0x0
SRB LF-bit interpretation:  EXTENDED  FA <=> GA Conversion: ENABLED
Spanning Tree Protocol Participation: IEEE802.1d
DLS for the bridge:  DISABLED
Number of ports added: 2
Port Number: 1      Interface Number: 0 Port Behaviour: STB Only
Port Number: 2      Interface Number: 1 Port Behaviour: STB Only

ASRT config>exit
Config>feature mcf 7
MAC Filtering user configuration
Filter Config>enable all 8
Filter Config>create list filtlistinc 9
Filter Config>update filtlistinc 10
Filter 'filtlistinc' Config>add source 08005a6158cf 11
Enter MAC Mask [ffffffffffff]?

:

```

Figure 175 (Part 1 of 3). Scenario 2: 2210B Configuration via the ASCII Console

```

:
Filter 'filtlistinc' Config>list canonical 12
Action: INCLUDE
Id Type MAC Address Mask
-- --
1 SRC 08-00-5A-61-58-CF FF-FF-FF-FF-FF-FF
Filter 'filtlistinc' Config>list noncanonical 13
Action: INCLUDE
Id Type MAC Address Mask
-- --
1 SRC 10:00:5A:86:1A&colonF3 FF:FF:FF:FF:FF:FF
Filter 'filtlistinc' Config>set-action exclude 14
Filter 'filtlistinc' Config>exit
Filter Config>? 15
ATTACH
CREATE
DEFAULT
DELETE
DETACH
DISABLE
ENABLE
LIST
MOVE
REINIT
SET-CACHE
UPDATE
EXIT
Filter Config>create filter output 1 16
Filter Config>list all
Filtering: enabled
Filter List Action
-----
filtlistinc EXCLUDE

Filters
-----
Id Default State Ifc Dir Cache
-- --
1 INCLUDE ENABLE 1 OUTPUT 16
Filter Config>attach filtlistinc 1 17
Filter Config>list filter 1 18
Id Default State Ifc Dir Cache
-- --
1 INCLUDE ENABLE 1 OUTPUT 16

Filter List Action
-----
filtlistinc EXCLUDE
Filter Config>exit
:

```

Figure 175 (Part 2 of 3). Scenario 2: 2210B Configuration via the ASCII Console


```
:  
Config>Ctrl+p  
*restart 19  
Are you sure you want to restart the gateway? (Yes or [No]): Yes
```

```
Copyright Notices:  
Copyright 1985-1994 Proteon, Inc.  
Copyright 1984-1987, 1989 by J. Noel Chiappa  
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.
```

```
MOS Operator Control
```

```
*
```

Figure 175 (Part 3 of 3). Scenario 2: 2210B Configuration via the ASCII Console

Notes:

- 1 Talk to the CONFIG process.
- 2 Access the customization of network 0 (Ethernet interface). Issue a list command. No changes are made to the default values.
- 3 Customization of network 1. This is the serial 1 interface. Specify that an RS-232 DTE cable is used.
- 4 Interface 2 is not used in this scenario.
- 5 List the devices (interfaces) customization.
- 6 Customization of the bridging function. Customize transparent bridging for 2210B on both Ethernet and serial 1 interfaces.
- 7 Access to the MAC Filtering feature (MCF).
- 8 Enable the MAC Filtering feature (MCF).
- 9 Create filter-list called FILTLISTINC.
- 10 Access the configuration of the FILTLISTINC filter-list.
- 11 Add a filter-item for canonical MAC address 08005A6158CF, with mask FFFFFFFF to the FILTLISTINC filter-list.
- 12 List all the filter-items of the FILTLISTINC filter-list and display the MAC address and the mask in canonical format .
- 13 List all the filter-items of the FILTLISTINC filter-list and display the MAC address and the mask in non-canonical format.
- 14 Set the action of the FILTLISTINC filter-list to EXCLUDE.
- 15 This shows you all the commands available from the MAC Filtering (MCF) feature configuration.

16 Create the filter for interface 1 (serial 1 interface) for OUTPUT traffic. The list all command shows that this filter is designated as filter number 1.

17 Attach the FILTLISTINC filter-list to the filter number 1.

18 List the filter number 1 customization with all of its attached filter-lists.

19 Restart the 2210B to get the configuration running.

On 2210 Navigation Window :

- Select CONFIGURE from the menu bar
- Select NEW CONFIGURATION **1**

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :

- Select MODEL
- Select **MODEL 125** **2**
- Select CONFIGURATION of Token-Ring line **3**
- ENABLE INTERFACE
- MAC ADDRESS = **40002210A001**
- Select SPEED
- Select 4
- Select PACKET SIZE
- Select 2052
- Select CABLE TYPE
- Select **UTP**
- RIF TIMER = 120
- DISABLE END NODE SOURCE ROUTING

Select the data-link protocol of Serial 1 (PPP by default)

- Select PPP

Select CONFIGURATION of Serial 1 **4**

- On GENERAL subpanel :
- ENABLE INTERFACE
- MAXIMUM TRANSMISSION UNIT = 2048
- Select ENCODING
- Select NRZ
- Select IDLE
- Select FLAG
- Select CLOCKING
- Select EXTERNAL
- CLOCK SPEED = 0
- TRANSMIT DELAY = 0
- Select CABLE TYPE
- Select RS-232 DTE
- Subpanels LCP, BNCP and IPCP not modified

Select CONFIGURATION of Serial 2

- On GENERAL subpanel :
- DISABLE INTERFACE** **5**

On 2210 Navigation Window :

- Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :

- ENABLE BRIDGING** **6**
- DISABLE DLSw

:

Figure 176 (Part 1 of 5). Scenario 2: 2210A Configuration via the Nways MRS Configuration Program

:

In SOURCE ROUTING BRIDGE box

BRIDGE NUMBER = 1
MAXIMUM ARE HOP COUNT = 14
MAXIMUM STE HOP COUNT = 14
INTERNAL VIRTUAL SEGMENT = 1
Select LF BIT INTERPRETATION
Select EXTENDED
ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box

ENABLE SR <-> TB CONVERSION
TB: VIRTUAL SEGMENT = FFF

In TRANSPARENT BRIDGE box

FILT. DBASE SIZE = 2048
AGING TIME = 300
RESOLUTION TIME = 5

On 2210 Navigation Window :

Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :

ENABLE Token-Ring

Select CONFIGURE of Token-Ring

Select INTERFACE SUPPORTS
Select **SRB**
Select DUPLICATE FRAMES
Select STE&TSF
SEGMENT NUMBER = **FFB**
MTU UNIT = 4399
ENABLE STE

ENABLE SERIAL 1

Select CONFIGURE of Serial 2

Select INTERFACE SUPPORTS
Select **STB**
Select DUPLICATE FRAMES
Select STE&TSF
SEGMENT NUMBER = 1
MTU UNIT = 4399
ENABLE STE

DISABLE SERIAL 2

Box CONFIGURE of Serial 2 not customized

:

Figure 176 (Part 2 of 5). Scenario 2: 2210A Configuration via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select MAC FILTER-LISTS panel of MAC FILTERING subdirectory of FEATURES directory

On MAC - FILTER-LIST Window :
  On GENERAL subpanel
    FILTER-LIST NAMES = filtlisttag
    Select ACTION
      Select TAG
      TAG VALUE = 1
      Select ADD 7

    FILTER-LIST NAMES = filtlistex
    Select ACTION
      Select EXCLUDE
      Select ADD 8

  Select filtlisttag Tag 1 line 9

  On FILTER-ITEMS subpanel
    Select MAC ADDRESS TYPE
    Select SOURCE
    Select MAC ADDRESS FORMAT
    Select NONCANONICAL
    MAC ADDRESS = 400000033350
    MAC ADDRESS MASK = 7FFFFFFFFF
    Select ADD inside the FILTER-ITEMS subpanel 10

  Select CHANGE outside the FILTER-ITEMS subpanel 11

  Select filtlistex Exclude line 12

  On FILTER-ITEMS subpanel
    Select MAC ADDRESS TYPE
    Select SOURCE
    Select MAC ADDRESS FORMAT
    Select NONCANONICAL
    MAC ADDRESS = 40000ABCD100
    MAC ADDRESS MASK = 7FFFFFFFFF00
    Select ADD inside the FILTER-ITEMS subpanel 13

    Select MAC ADDRESS TYPE
    Select DESTINATION
    Select MAC ADDRESS FORMAT
    Select NONCANONICAL
    MAC ADDRESS = C00000000080
    MAC ADDRESS MASK = FFFFFFFFFF
    Select ADD inside the FILTER-ITEMS subpanel 14

  Select CHANGE outside the FILTER-ITEMS subpanel 15

:

```

Figure 176 (Part 3 of 5). Scenario 2: 2210A Configuration via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select INTERFACES panel of MAC FILTERING subdirectory of FEATURES directory

On MAC - FILTERING Window :
  Enable MAC Filtering 16
    Select INPUT filter of Token-Ring line 17
      On GENERAL subpanel
        Enable FILTER 18
        CACHE SIZE = 16
        Select DEFAULT ACTION
        Select INCLUDE 19

      On FILTER-ITEMS subpanel
        Select FILTER-LIST NAMES
        Select filtlisttag
        Select ADD 20
        Select FILTER-LIST NAMES
        Select filtlistex
        Select ADD 21

On 2210 Navigation Window :
Select INTERFACES panel of BRS subdirectory of FEATURES directory

On BRS - INTERFACES Window :
  ENABLE BRS on Serial 1 line 22
  Select CONFIGURE on Serial 1 line
    On CLASSES subpanel
      CLASS NAME = tagclass
      BANDWIDTH PERCENT = 30
      Select ADD 23

    On DEFAULT-CLASS subpanel 24
      Select DEFAULT-CLASS
      Select DEFAULT
      Select DEFAULT-CLASS PRIORITY
      Select NORMAL

    On TAG subpanel
      On TAG1 line
        Enable TAG 25
        VALUE = 1 26
        Select PRIORITY
        Select HIGH 27
        Select CLASS
        Select tagclass 28

    Nothing to customize on PROTOCOL and FILTER subpanels

:

```

Figure 176 (Part 4 of 5). Scenario 2: 2210A Configuration via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
    Select CREATE ROUTER CONFIGURATION 29

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
  Enter MCFA 30
  Select OK

```

Figure 176 (Part 5 of 5). Scenario 2: 2210A Configuration via the Nways MRS Configuration Program

Notes:

- 1** Start the customization from an empty configuration.
- 2** The router is a 2210 Model 125, with token-ring LAN, 4 MB Flash, 8 MB RAM, and without the ISDN BRI adapter.
- 3** Customization of the token-ring. Assign locally administered address, and specify the unshielded (UTP) connector is used.
- 4** Customization of serial 1. No changes are made to the default values. Note that the RS-232 DTE cable is the default.
- 5** Interface 2 is not used in this scenario.
- 6** Customization of the bridging function. Enable bridging with the bridge number of 1, and SR<->TB conversion with the TB virtual segment number of FFF. Select SRB for token-ring interface with LAN segment number FFB. Select STB for the serial 1 interface.
- 7** Add a new filter-list named FILTLISTTAG with TAG action (TAG value = 1).
- 8** Add a new filter-list named FILTLISTEX with EXCLUDE action.
- 9** This is required because we will now customize the filter-item of the FILTLISTTAG filter-list.
- 10** Add a new filter-item with a non-canonical source MAC address of 400000033350 and mask of 7FFFFFFFFFFF.
- 11** This is required to add the filter-item to the filter-list previously selected.
- 12** This is required to customize the filter-item of the FILTLISTEX filter-list.
- 13** Add a new filter-item with a non-canonical source MAC address of 40000ABCD00 and mask of 7FFFFFFFFF00.
- 14** Add a new filter-item with a non-canonical destination MAC address of C0000000080 and mask of FFFFFFFFFF.

- 15** This is required to add the two filter-items to the filter-list previously selected.
- 16** Enable the MAC Filtering feature.
- 17** Select the filter corresponding to the INPUT traffic of the token-ring interface.
- 18** Enable this filter.
- 19** Set the default action of this filter to INCLUDE. Packets for which the MAC address does not match any filter-item of any filter-list attached to this filter will be bridged.
- 20** Attach the FILTLISTTAG filter-list to this filter.
- 21** Attach the FILTLISTEX filter-list to this filter.
- 22** Enable the Bandwidth Reservation (BRS) feature for the serial 1 interface.
- 23** Add the TAGCLASS class with 30% of the bandwidth.
- 24** Set the default to class DEFAULT with priority NORMAL. This is the default.
- 25** Enable the TAG1.
- 26** Assign TAG value 1 to TAG1.
- 27** Assign HIGH priority to TAG1.
- 28** Assign TAGCLASS class to TAG1.
- 29** Create the configuration file.
- 30** This is the name of the configuration file stored on the workstation.

On 2210 Navigation Window :

- Select CONFIGURE from the menu bar
- Select NEW CONFIGURATION **1**

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :

- Select MODEL
 - Select **MODEL 126** **2**
- Select CONFIGURATION of Ethernet line **3**
 - ENABLE INTERFACE
 - Select CONNECTOR TYPE
 - Select **AUTO-CONFIG**
 - Select IP ENCAPSULATION
 - Select ETHERNET

Select the data-link protocol of Serial 1 (PPP by default)

- Select PPP

Select CONFIGURATION of Serial 1 **4**

On GENERAL subpanel :

- ENABLE INTERFACE
- MAXIMUM TRANSMISSION UNIT = 2048
- Select ENCODING
 - Select NRZ
- Select IDLE
 - Select FLAG
- Select CLOCKING
 - Select EXTERNAL
- CLOCK SPEED = 0
- TRANSMIT DELAY = 0
- Select CABLE TYPE
 - Select RS-232 DTE

Subpanels LCP, BNCP and IPCP not modified

Select CONFIGURATION of Serial 2

On GENERAL subpanel :

- DISABLE INTERFACE** **5**

:

Figure 177 (Part 1 of 3). Scenario 2: 2210B Configuration via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING      6
DISABLE DLSw

In SOURCE ROUTING BRIDGE box
    BRIDGE NUMBER = 1
    MAXIMUM ARE HOP COUNT = 14
    MAXIMUM STE HOP COUNT = 14
    INTERNAL VIRTUAL SEGMENT = 1
    Select LF BIT INTERPRETATION
    Select EXTENDED
    ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
    DISABLE SR <=> TB CONVERSION

In TRANSPARENT BRIDGE box
    FILT. DBASE SIZE = 2048
    AGING TIME = 300
    RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE Ethernet
Select CONFIGURE of Ethernet
    Select INTERFACE SUPPORTS
    Select STB
    Select DUPLICATE FRAMES
    Select STE&TSF
    SEGMENT NUMBER = 1

ENABLE SERIAL 1
Select CONFIGURE of Serial 2
    Select INTERFACE SUPPORTS
    Select STB
    Select DUPLICATE FRAMES
    Select STE&TSF
    SEGMENT NUMBER = 1
    MTU UNIT = 4399
    ENABLE STE

DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

:

```

Figure 177 (Part 2 of 3). Scenario 2: 2210B Configuration via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select MAC FILTER-LISTS panel of MAC FILTERING subdirectory of FEATURES directory

On MAC - FILTER-LIST Window :
  On GENERAL subpanel
    FILTER-LIST NAMES = filtlistinc
    Select ACTION
      Select EXCLUDE
      Select ADD 7

  On FILTER-ITEMS subpanel
    Select MAC ADDRESS TYPE
    Select SOURCE
    Select MAC ADDRESS FORMAT
    Select CANONICAL
    MAC ADDRESS = 08005A6158CF
    MAC ADDRESS MASK = FFFFFFFFFFFF
    Select ADD inside the FILTER-ITEMS subpanel 8

    Select CHANGE outside the FILTER-ITEMS subpanel 9

On 2210 Navigation Window :
Select INTERFACES panel of MAC FILTERING subdirectory of FEATURES directory

On MAC - FILTERING Window :
  Enable MAC Filtering 10
    Select OUTPUT filter of Serial 1 line 11
      On GENERAL subpanel
        Enable FILTER 12
        CACHE SIZE = 16
        Select DEFAULT ACTION
          Select INCLUDE 13

      On FILTER-ITEMS subpanel
        Select FILTER-LIST NAMES
        Select filtlistinc
        Select ADD 14

On 2210 Navigation Window :
  Select CONFIGURE from the menu bar
  Select CREATE ROUTER CONFIGURATION 15

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
  Enter MCFB 16
  Select OK

```

Figure 177 (Part 3 of 3). Scenario 2: 2210B Configuration via the Nways MRS Configuration Program

Notes:

- 1** Start the customization from an empty configuration.
- 2** The router is a 2210 Model 126, with Ethernet LAN, 4 MB Flash, 8 MB RAM, and without the ISDN BRI adapter.

- 3** Customization of the Ethernet interface. Assign a connector type of AUTOCONFIG. This will let the IBM 2210 to automatically discover the type of connector used.
- 4** Customization of serial 1. Nothing has been changed from the default. Note that RS-232 DTE cable is the default.
- 5** Interface 2 is not used in this scenario.
- 6** Customization of the bridging function. Enable bridging and select STB for the Ethernet serial 1 interfaces.
- 7** Add a new filter-list named FILTLISTINC with EXCLUDE action.
- 8** Add a new filter-item with a canonical source MAC address of 08005A6158CF and mask of FFFFFFFF.
- 9** This is required to add the filter-item to the filter-list selected previously.
- 10** Enable the MAC Filtering feature.
- 11** Select the filter corresponding to the OUTPUT traffic of the serial 1 interface.
- 12** Enable this filter.
- 13** Set the default action of this filter to INCLUDE. Packets for which the MAC address does not match any filter-item of any filter-list attached to this filter will be bridged.
- 14** Attach the FILTLISTINC filter-list to this filter.
- 15** Create the configuration.
- 16** This is the name of the configuration file stored on the workstation.

11.5 WAN Restoral (WRS)

This section provides a description of the WAN Restoral feature and its configuration commands. A scenario of how to configure WAN Restoral on the IBM 2210 is also provided.

11.5.1 Introduction to WAN Restoral (WRS)

The WAN Restoral (WRS) feature, which is also called Dial Backup feature, allows you to back up a primary leased PPP serial link or Permanent Virtual Circuit (PVC) of the frame relay network with a V.25bis or ISDN link.

Note

Backing up of X.25 serial link is not supported. WAN Restoral supports backing up of PPP leased serial link and PVC of the frame relay network.

The WAN Restoral feature is supported over every routed protocol (IP, IPX, Appletalk and DLSw) and for every bridging method, including tunnel bridge.

The backup switched line supported by this feature is over a V.25bis modem or ISDN serial line. For more information about the V.25bis serial interface, see 3.4.23, "The V.25bis Network Interface" on page 96. For more information about the ISDN serial interface, see 3.5, "The ISDN Interface" on page 102.

When the IBM 2210 detects the loss of connectivity on the primary PPP serial link or the PVC of frame relay network, it automatically dials the configured phone number to establish the dial connection via the V.25bis modem or the ISDN interface.

There is only one remote phone number configured in the IBM 2210. This must be the phone number of the same remote IBM 2210 which is reached via the primary link.

When the switchover from the primary link to the backup link occurs due to the failure of the primary link, the whole set of protocols configured on the primary leased PPP serial link or PVC of frame relay will be automatically switched over to the switched V.25bis serial link or ISDN link. All the protocols (IP, IPX, Appletalk, DLSw) and all of the bridging methods will survive the switchover to the switched V.25bis serial link or ISDN link.

When the IBM 2210 detects that the primary link has come back up, it automatically drops the V.25bis or ISDN dial connection and restores all the protocols to use the primary connection.

Figure 178 on page 600 shows the typical configuration of a network using WAN Restoral.

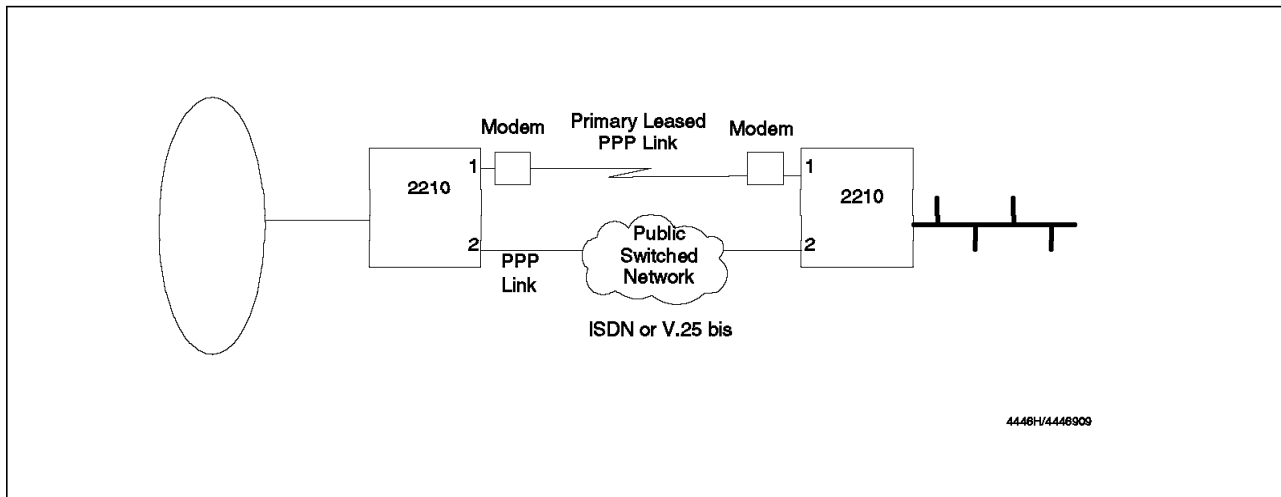


Figure 178. Typical Implementation of WAN Restoral for the Primary Leased PPP Link

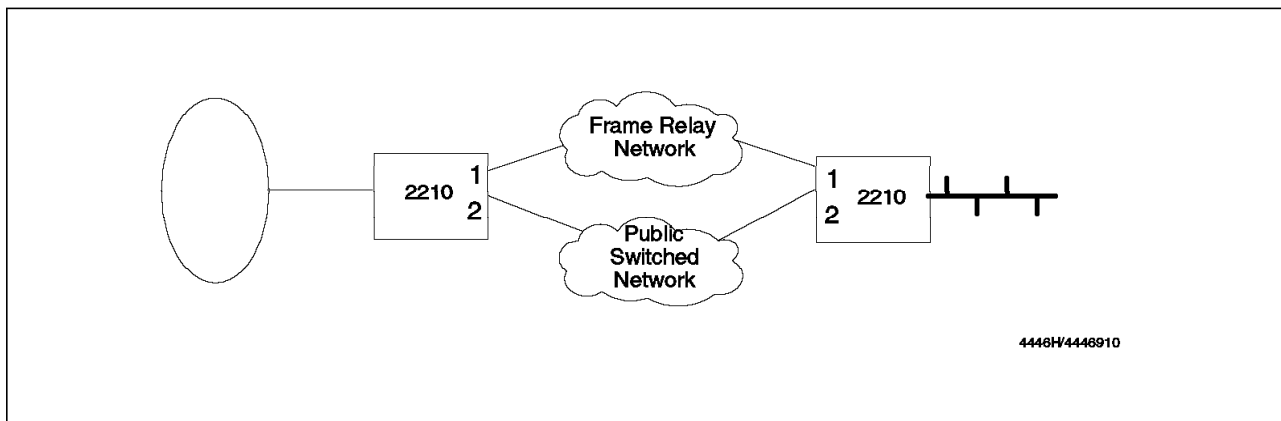


Figure 179. Typical Implementation of WAN Restoral for the Primary PVC of Frame Relay

To be able to use WAN Restoral, both 2210s at each end of the primary link must be customized for WAN Restoral.

To configure a 2210 to use WAN Restoral, you must customize one of its interfaces with PPP link or frame relay, and the other interface as a dial interface using a V.25bis modem with PPP encapsulation method or using ISDN with PPP or frame relay.

11.5.2 WAN Restoral Configuration

This section summarizes the configuration steps needed to customize WAN Restoral within the CONFIG process of the Nways MRS and within the Nways MRS Configuration Program.

This configuration shows the WAN Restoral Configuration on 2210 at one end, and for each parameter it advises you if the command must be different on the 2210 at the other end.

To configure the WAN Restoral feature on an IBM 2210, follow the following steps:

1. Configure three serial interfaces or devices:

- Physical primary interface
- Physical V.25bis or ISDN interface
- Logical secondary (also called dial-circuit) interface

You must also assign names to the remote and local phone numbers.

2. In the V.25bis or ISDN configuration process, configure the serial link.
3. In the circuit configuration process, configure the logical secondary interface.
4. In the WAN Restoral configuration process, configure the WAN Restoral feature.
5. Configure the LAN interface.
6. Configure specific protocols, and assign protocol addresses (IP or IPX) for the primary link only.

Note: No protocol address must be assigned on either the physical V.25bis or ISDN interface.

11.5.2.1 Configuration Commands on CONFIG Process

To configure the WAN Restoral feature on an IBM 2210, you must define three interfaces (also called devices):

- The primary interface (serial physical interface) must be configured with PPP data-link or frame relay data-circuit.
- The V.25bis interface (the other serial physical interface) must be configured with V.25bis data-link. If you want to use the ISDN interface, you can set the data-link protocol for only the dial-circuit interface mapped to it.
- The secondary interface (also called dial-circuit interface) is a logical interface mapped to the other interfaces. It must be configured with PPP data-link or frame relay data-circuit.

We will use an example to demonstrate the steps required. In this example, the primary interface is the interface 1, the V.25bis or ISDN switched interface is the interface #, and the secondary interface is the interface ##.

First of all, you must set the following parameters in the CONFIG process:

- Set the primary link to use the PPP data-link or the frame relay data-circuit. The PPP data-link is the default for each serial link, but you can change it to frame relay. To set the data-link protocol, use the following command:

```
Config>set data-link ppp 1
```

or

```
Config>set data-link fr 1
```

For the Nways MRS Configuration Program, use the corresponding serial line of the Device Interfaces window. To access the Device Interfaces window, select the Interfaces panel of the General subdirectory of the Devices directory.

- Set the V.25bis data-link for the interface #, using the following command:

```
Config>set data-link v25bis #
```

If you want to use the ISDN interface, set the PPP or frame relay data-link for the dial circuit interface ##.

```
Config>set data-link ppp ##
```

or

Config>**set data-link fr ##**

You may use the List Devices command to show the data-link configured for each interface.

For the Nways MRS Configuration Program, use the corresponding serial line of the Device Interfaces window.

- Add a logical dial-circuit using the following command:

Config>**add device dial-circuit**

The interface number assigned to this device dial can be seen by using the List Devices command.

Note: The interface number is always the next interface number available.

For the Nways MRS Configuration Program, use the Dial-Circuits window. To access the Dial-Circuits window, select the Dial-Circuits panel of the General subdirectory of the Devices directory.

- Assign a name to the phone number to be used. One name is assigned to the local phone number and one for the remote one.

For example, to assign the name local-site to the local phone number 12345678, you must issue the following command:

Config>**add v25-bis-address local-site 12345678**

or

Config>**add isdn-address local-site 12345678**

To assign the name remote-site to the remote phone number 87654321, you must issue the following command:

Config>**add v25-bis-address remote-site 87654321**

or

Config>**add isdn-address remote-site 87654321**

Note: The names assigned to the phone numbers must not exceed 23 characters. The phone number must not exceed 20 digits.

You can display the v.25bis or ISDN addresses by using the following command:

Config>**list v25-bis-address**

or

Config>**list isdn-address**

On the 2210 at the other end, the phone number 12345678 should be assigned as to the name of the remote site and the phone number 87654321 should be assigned with the name of the local-site.

For the Nways MRS Configuration Program, use the V.25bis or ISDN Addresses window. To access the V.25bis or ISDN Addresses window, select the V.25bis or ISDN Addresses panel of the General subdirectory of the Devices directory.

11.5.2.2 Configuration Commands on V.25bis Configuration Process

To customize the V.25bis interface, which is interface # in our example, you must use the following command:

1. Access V.25bis interface (#) customization using the following command:

Config>**network #**

After entering the above command, the following prompt will be displayed:

V.25bis Config>

For the Nways MRS Configuration Program, select the corresponding V.25bis serial line of the Devices Interfaces window. To access the Devices Interfaces window, select the Interfaces panel of the General subdirectory of the Devices directory.

2. Define the local phone number of this V.25bis interface using the previously defined name of local-site. To define the local phone number of the V.25bis interface, use the following command:

V.25bis Config>**set local local-site**

For the Nways MRS Configuration Program, use the General subpanel of the corresponding V.25bis serial line in the Devices Interfaces window.

3. Define the number of seconds the IBM 2210 will wait before trying to re-establish a dial-up connection after the previous attempt to establish the dial-up has failed. This time is referred to as the timeout-call-address and can be specified using the following command:

V.25bis Config>**set timeout-call-address 60**

The timeout-call-address must be in the range 0 to 65535, and the default is 0 seconds.

For the Nways MRS Configuration Program, use the General subpanel of the corresponding V.25bis serial line in the Device Interfaces window.

4. Define the maximum number of attempted calls to a remote V.25bis address. This is referred to as the retries-call-address parameter, and can be specified by using the following command:

V.25bis Config>**set retries-call-address 5**

Note: Each attempt will be made after waiting the number of seconds specified by the timeout-call-address parameter.

The retries-call-address must be in the range 0 to 10, and the default is 1 attempt.

For the Nways MRS Configuration Program, use the General subpanel of the corresponding V.25bis serial line in the Device Interfaces window.

5. All the V.25bis interface customization can be displayed by using the following command:

V.25bis Config>**list**

6. Exit V.25bis interface configuration by using the following command:

V.25bis Config>**exit**

After issuing the above command, the following prompt will be displayed:

Config>

For more information about the V.25bis Interface configuration, see 3.4.24, "Configuring V.25bis" on page 100.

11.5.2.3 Configuration Commands on ISDN Configuration Process

To customize the ISDN interface, which is interface # in our example, you must use the following command:

1. Access ISDN interface (#) customization, using the following command:

```
Config>network #
```

After entering the above command, the following prompt will be displayed:

```
ISDN Config>
```

For the Nways MRS Configuration Program, select the corresponding ISDN serial line of the Devices Interfaces window. To access the Devices Interfaces window, select the Interfaces panel of the General subdirectory of the Devices directory.

2. Define the local phone number to of this ISDN interface using the previously defined name of local-site. To define the local phone number of the ISDN interface, use the following command:

```
ISDN Config>set local local-site
```

For the Nways MRS Configuration Program, use the General subpanel of the corresponding ISDN serial line in the Devices Interfaces window.

3. Set the switch type to be connected to this ISDN interface with the following command:

```
ISDN Config>set switch
```

For the Nways MRS Configuration Program, use the Sw Var Parms subpanel of the corresponding ISDN serial line in the Device Interfaces window.

4. Set the network address (telephone number) of the local port with the following command:

```
ISDN Config>set dn0
```

For the Nways MRS Configuration Program, use the Sw Var Parms subpanel of the corresponding ISDN serial line in the Device Interfaces window.

5. Define the number of seconds the IBM 2210 will wait before trying to re-establish a dial-up connection if the previous attempt to establish the dial-up has failed. This time is referred to as the timeout-call-address and can be specified using the following command:

```
ISDN Config>set timeout-call-address
```

The timeout-call-address must be in the range 0 to 65535, and the default is 0 seconds.

For the Nways MRS Configuration Program, use the Sw Var Parms subpanel of the corresponding ISDN serial line in the Device Interfaces window.

6. Define the maximum number of attempted calls to a remote ISDN address. This is referred to as the retries-call-address parameter and can be specified by using the following command:

```
ISDN Config>set retries-call-address 5
```

Note: Each attempt will be made after waiting the number of seconds specified by the timeout-call-address parameter.

The retries-call-address must be in the range 0 to 10, and the default is 1 attempt.

For the Nways MRS Configuration Program, use the Sw Var Parm's subpanel of the corresponding ISDN serial line in the Device Interfaces window.

7. All the ISDN interface customization can be displayed by using the following command:

```
ISDN Config>list
```

8. Exit ISDN interface configuration using the following command:

```
ISDN Config>exit
```

After issuing the above command, the following prompt will be displayed:

```
Config>
```

For more information about the ISDN Interface configuration, see 3.5.4, "ISDN Configuration Steps" on page 105.

11.5.2.4 Configuration Commands for Circuit Configuration Process

As part of the WAN Restoral customization, customize the secondary PPP or frame relay interface. In our example, interface number ## is assigned to the dial-circuit.

1. Access the secondary PPP or frame relay interface, using the following command:

```
Config>network ##
```

After issuing the above command, the following prompt will be displayed:

```
Circuit Config>
```

For the Nways MRS Configuration Program, use the Dial-Circuits window. To access the Dial-Circuits window, select the Dial-Circuits panel of the General subdirectory of the Devices directory.

2. Map this secondary PPP or frame relay interface to the V.25bis or ISDN interface (interface # in our example). To do so, issue the following command:

```
Circuit Config>set net #
```

For the Nways MRS Configuration Program, use the Dial-Circuits window.

3. Specify which end will initiate the call. Note that only one end must initiate the call, while the other end must wait for inbound calls.

To initiate the call from this IBM 2210, issue the following command:

```
Circuit Config>set calls outbound
```

To configure the IBM 2210 waiting for the call, you must issue the following command:

```
Circuit Config>set calls inbound
```

Note: Do not specify the Set Calls Both command at any end.

For the Nways MRS Configuration Program, use the Dial-Circuits window.

4. Specify that this switched link has to stay up, even if there is no data to send (fixed circuit). To do so, issue the following command:

```
Circuit Config>set idle 0
```

For the Nways MRS Configuration Program, use the Dial-Circuits window.

5. Define the remote phone number for this dial-circuit interface, using the previously defined name of *remote-site*. To do so, use the following command:

```
Circuit Config>set destination remote-site
```

For the Nways MRS Configuration Program, use Dial-Circuits window.

6. Specify all the PPP or frame relay parameters for this interface to be the same as the secondary interface. To access the PPP or frame relay parameters of the secondary interface, issue the following command:

```
Circuit Config>encapsulator
```

After issuing the above command, the following prompt will be displayed:

```
PPP Config>
```

or

```
FR Config>
```

You can now display and change the PPP or frame relay parameters of the secondary interface.

To display the current PPP or frame relay parameters of the secondary interface, issue the following command:

```
PPP Config>list all
```

or

```
ISDN Config>list all
```

To exit the PPP configuration of the secondary interface, issue the following command:

```
PPP Config>exit
```

or

```
ISDN Config>exit
```

After issuing the above command, the following prompt will be displayed:

```
Circuit Config>
```

7. You can list all the secondary interface configurations with the List command.
8. To exit the secondary interface configuration, issue the following command:

```
Circuit Config>exit
```

You will be taken back to the CONFIG process, and the prompt becomes:

```
Config>
```

For more information about the circuit interface configuration, see 3.4.23.3, "Dial Circuits" on page 97.

11.5.2.5 Configuration Commands on WAN Restoral Configuration Process

The next task is to customize the WAN Restoral feature using the following steps:

1. Access the WAN Restoral feature configuration, using the following command:

```
Config>feature wrs
```

After issuing the above command, the following prompt will be displayed:

WRS Config>

For the Nways MRS Configuration Program, select the WAN Restoral panel of the WRS subdirectory of the Features directory.

2. Map the secondary interface to the primary interface. To map the secondary interface (interface ## in this example) to the primary interface (interface 1 in this example), issue the following command:

WRS Config>**add secondary-circuit ## 1**

For the Nways MRS Configuration Program, use the WAN Restoral window.

3. Enable the WAN Restoral feature using the following command:

WRS Config>**enable wrs**

For the Nways MRS Configuration Program, use the WRS General window.

4. Enable the secondary PPP or frame relay interface (interface ## in this example), using the following command:

WRS Config>**enable secondary-circuit ##**

For the Nways MRS Configuration Program, use the WAN Restoral window.

5. You can list the WAN Restoral feature configuration by using the following command:

WRS Config>**list all**

6. Exit the WAN Restoral feature, using the following command:

WRS Config>**exit**

Table 74 shows the available WAN Restoral commands. The *Nways MRS Software User's Guide* covers these commands in detail.

Table 74. WAN Restoral Configuration Commands	
Command	Function
? (Help)	Displays the WAN Restoral configuration commands, or lists any parameters associated with that command.
Add	Add a mapping of primary interface to secondary interface.
Disable	Disables WAN Restoral feature or an individual secondary-circuit mapping.
Enable	Enables WAN Restoral feature or an individual secondary-circuit mapping.
List	Lists the WAN Restoral feature configuration.
Remove	Remove a primary to secondary mapping created by add command.
Exit	Exits the WAN Restoral feature configuration process and returns to the CONFIG process.

11.5.3 Scenario 3: WAN Restoral (WRS) Implementation with IP, DLSw and Bridging

In this scenario, we have one 2210 with token-ring interface (2210A) and one 2210 with Ethernet interface (2210B). Both 2210s are linked together by using the following:

1. Leased primary PPP link with V.35 modems on physical interface 1 for both 2210s.
2. Switched Backup PPP link with V.25bis modems on physical interface 2 for both 2210s.

2210A routes IP and DLSw with source route bridging on a token-ring interface 0.

2210B routes IP and DLSw with transparent bridging on Ethernet interface 0.

- Interfaces:

The token-ring interface on 2210A runs at 4 MBps and is attached to the LAN using the UTP connector. It uses the MAC address 40002210A001.

Leased primary serial link is a PPP link over V.35 modems.

Switched backup serial link is a PPP link over V.25bis modems.

The Ethernet interface on 2210B is connected to the LAN using the 10Base-T connector.

- Bridging:

2210A is configured for source route-translational bridging with SRB on the token-ring interface, and STB on the serial 1 interface. The bridge number of 2210A is 1. The LAN segment number of the token-ring is FFB and the TB domain is seen from SRB domain as the LAN segment number FFF. DLSw is enabled at box level.

Note: The bridging function is configured because of the requirements of DLSw.

2210B is configured for transparent bridging on both serial 1 and Ethernet interfaces. DLSw is enabled at box level.

Note: The bridging function is configured because of the requirements of DLSw.

- IP routing:

2210A is an IP router with IP address 9.67.46.146 on its token-ring interface and IP address 9.67.46.132 on its serial 1 interface. Its internal IP address is 9.67.46.146, and RIP is enabled for 2210A.

2210B is an IP router with IP address 9.67.46.77 on its Ethernet interface and IP address 9.67.46.131 on its serial 1 interface. Its internal IP address is 9.67.46.77, and RIP is enabled for 2210B.

- DLSw protocol:

2210B and 2210A are DLSw partners for each other. From 2210s, the DLSw network is seen as segment number FFF.

- WAN Restoral feature:

Dial number of 2210A is 8-352-2184. Dial number of 2210B is 8-352-2186. The call backup will be done from 2210A to 2210B.

For more information about IP protocol customization, see 8.2, “Configuring IP on the IBM 2210” on page 341.

For more information about DLSw protocol customization, see 10.3, “DLSw Configuration on the IBM 2210” on page 453.

For more information about bridging (ASRT) protocol customization, see 4.4, “Bridging Scenarios and Configurations” on page 138.

Figure 180 on page 610 shows the configuration of the network used in this scenario. The customization samples for this scenario are provided as follows:

- Figure 181 on page 611 shows the 2210A configuration via the ASCII console.
- Figure 182 on page 621 shows the 2210B configuration via the ASCII console.
- Figure 183 on page 630 shows the 2210A configuration via the Nways MRS Configuration Program.
- Figure 184 on page 636 shows the 2210B configuration via the Nways MRS Configuration Program.

In this scenario, VTAM host welcome message appears on the end user B station, and the TCP/IP PING command works fine between end user A and end user B. We then logged onto VTAM and issued a continuous PING command. While the PING was in progress, we disconnected the primary link. 2210A established a dial-up connection to 2210B automatically. When testing this scenario, the PING command was not getting any responses for 30 seconds and the VTAM user was in the pending clock for 40 seconds. Then both TCP/IP and SNA/DLSw traffic resumed sending data over the backup line.

Note: In the several tries of the above scenario, the VTAM user was never logged off and it was able to resume data transmission without any need to re-establish the SNA session.

Re-connecting the primary serial interface resulted in the 2210s disconnecting the switched link, and both TCP/IP and SNA/DLSw traffic resumed using the primary link without any loss of PING response or waiting on the part of the SNA session. In other words, switching back to the primary link was completely transparent to both TCP/IP PINGs and the SNA/DLSw user.

Additionally, the following was noticed during our tests:

- Bridging environment

To switch from the failed primary link to the V.25bis link the IBM 2210 suspended the forwarding of the bridged packets for 60 seconds. In switching back to the primary link, the bridging was interrupted for 30 seconds.

- Routing environment

When performing IP and IPX routing, switching from the failed primary link to the V.25bis link resulted in the suspension of the routing functions for 30 to 40 seconds. In switching back to the primary link, the switchover was totally transparent to the routing functions.

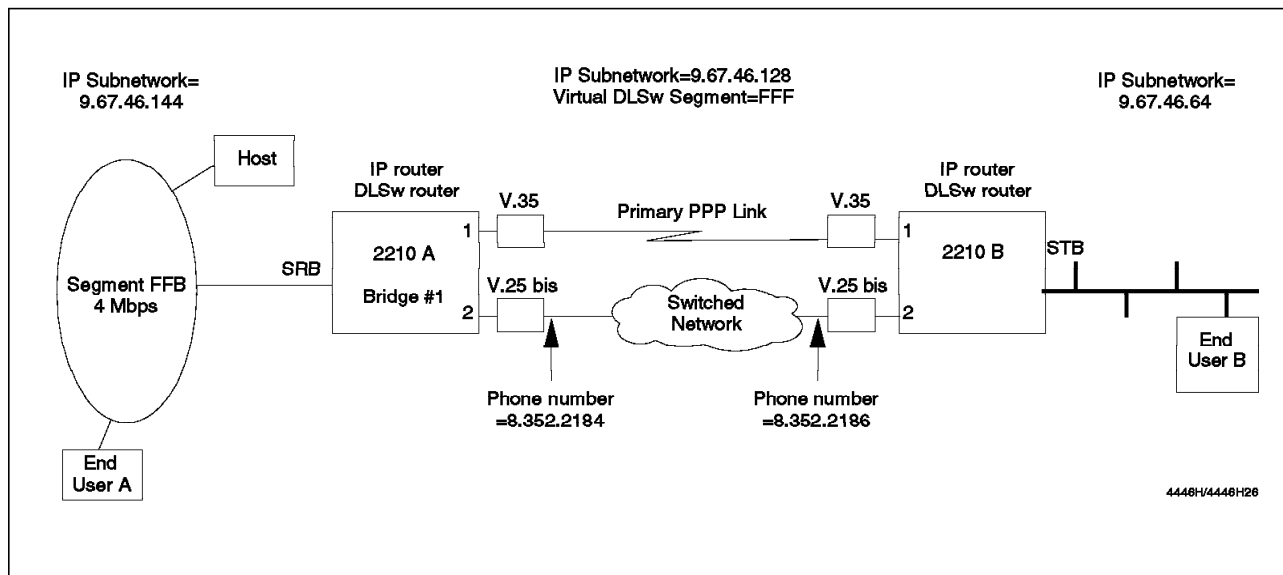


Figure 180. Scenario 3: WAN Restoral (WRS)


```

*
*talk 6 1

Config>add v25-bis-address local-site 8-352-2184 2
Config>add v25-bis-address 3
Assign address name [1-23] chars []? remote-site
Assign network dial address [1-20 digits] []? 8-352-2186
Config>add device dial-circuit 4
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
Config>set data-link v25bis 2 5
Config>list devices 6
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN V.25bis): CSR 81640, CSR2 80E00, vector 92
Ifc 3 (PPP Dial Circuit): CSR 0, vector 0
Config>network 0 7
Token-Ring interface configuration
TKR config>media unshielded
TKR config>set physical-address 40:00:22:10:A0:01
TKR config>list all
Token-Ring configuration:

Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Unshielded

RIF Aging Timer: 120
Source Routing: Enabled
MAC Address: 40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 8
Point-to-Point user configuration
PPP Config>set hdlc cable v35 dte
PPP Config>list all

LCP Parameters
-----
CONFIG Request Tries: 20 CONFIG Nak Tries: 10
Terminate Tries: 10 Retry Timer: 3000

LCP Options
-----
Max Receive Unit: 2048 Magic Number: Yes
Peer to Local (RX) ACCM: A0000
Protocol Field Comp(PFC): No Addr/Cntl Field Comp(ACFC): No

:

```

Figure 181 (Part 1 of 8). Scenario 3: 2210A Configuration via the ASCII Console

```

:
Authentication Options
-----
Authenticate remote using:  none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:      3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit
Config>network 2           9
V.25bis Data Link Configuration
V.25bis Config>list        10
      V.25bis Configuration
Local Network Address Name  = Unassigned

Non-Responding addresses:
Retries                    = 1
Timeout                    = 0 seconds

Call timeouts:
Command Delay              = 0 ms
Connect                    = 60 seconds
Disconnect                  = 2 seconds
V.25bis Config>set local local-site 11
V.25bis Config>set retries-call-address 5 12
V.25bis Config>set timeout-call-address 60 13
V.25bis Config>list
      V.25bis Configuration
Local Network Address Name  = local-site
Local Network Address       = 8-352-2184

:

```

Figure 181 (Part 2 of 8). Scenario 3: 2210A Configuration via the ASCII Console

```

:
Non-Responding addresses:
Retries           = 5
Timeout           = 60 seconds

Call timeouts:
Command Delay     = 0 ms
Connect           = 60 seconds
Disconnect        = 2 seconds
V.25bis Config>exit
Config>network 3 14
Circuit configuration
Circuit Config>list 15

Base net:         0
Destination name:
Outbound calls    allowed
Inbound calls     allowed
Idle timer        = 60 sec
SelfTest Delay Timer = 150 ms

Circuit Config>set net 2 16
Circuit Config>set calls outbound 17
Circuit Config>set idle 0 18
Circuit Config>set destination remote-site 19
Circuit Config>set any_inbound 20
Circuit Config>encapsulator 21
Point-to-Point user configuration
PPP Config>list all 22

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:      3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:      Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):    No   Addr/Cntl Field Comp(ACFC):    No

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:      3000

:

```

Figure 181 (Part 3 of 8). Scenario 3: 2210A Configuration via the ASCII Console

```

:
CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:          Disabled

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Circuit Config>exit
Config>feature wrs             23
WAN Restoral user configuration
WRS Config>add secondary-circuit 3 1 24
WRS Config>enable wrs          25
WRS Config>enable secondary-circuit 26
Secondary interface number [0]? 3
WRS Config>list all           27

WAN Restoral is enabled.

      Primary Interface      Secondary Interface      Restoral
      -----            -----            Enabled
1 - WAN PPP                3 - PPP Dial Circuit          Yes
WRS Config>exit
Config>protocol ip          28
Internet protocol user configuration
IP config>add address 0 9.67.46.146 255.255.255.240
IP config>add address
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.132
Address mask [255.0.0.0]? 255.255.255.240
IP config>enable rip
IP config>set internal IP address 9.67.46.146
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.146      255.255.255.240  Network broadcast,    fill 0
  intf 1  9.67.46.132      255.255.255.240  Network broadcast,    fill 0
  intf 2                                     IP disabled on this interface
Internal IP address: 9.67.46.146

Routing

:

```

Figure 181 (Part 4 of 8). Scenario 3: 2210A Configuration via the ASCII Console

```

:

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0  9.67.46.146      Send net and subnet routes
    intf 1  9.67.46.132      Send net and subnet routes
    intf 2                      IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

EGP: disabled

IP config>exit
Config>protocol asrt 29
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>disable transparent 1
ASRT config>enable source-routing 1
Segment Number for the port in hex(1 - FFF) [1]? ffb
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>enable sr-tb-conversion
TB-Domain Segment Number in hex(1 - FFF) [1]? fff
TB-Domain's MTU [1470]?
ASRT config>enable dls
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:                Enabled                Bridge Behavior: SR<->TB
      +-----+
      ] SOURCE ROUTING INFORMATION ]-----+
      +-----+

Bridge Number:          01                Segments:          1
Max ARE Hop Cnt:        14                Max STE Hop cnt:   14
1:N SRB:                Not Active        Internal Segment: 0x000
LF-bit interpret:       Extended

      +-----+
      ] SR-TB INFORMATION ]-----+
      +-----+

SR-TB Conversion:       Enabled
TB-Virtual Segment:     0xFFF                MTU of TB-Domain: 1470

:

```

Figure 181 (Part 5 of 8). Scenario 3: 2210A Configuration via the ASCII Console

```

:
+-----+
-----] SPANNING TREE PROTOCOL INFORMATION ]-----
+-----+
Bridge Address:      Default      Bridge Priority:  32768/0x8000
STP Participation:   IEEE802.1d on TB ports, IBM-8209 and IBM-SRB proprietary on SR ports
+-----+
-----] TRANSLATION INFORMATION ]-----
+-----+
FA<=>GA Conversion:  Enabled      UB-Encapsulation:  Disabled
DLS for the bridge:  Enabled
+-----+
-----] PORT INFORMATION ]-----
+-----+
Number of ports added: 2
Port:  1      Interface:  0      Behavior:  SRB Only  STP:  Enabled
Port:  2      Interface:  1      Behavior:  STB Only  STP:  Enabled

ASRT config>exit
Config>protocol dls 30
DLSw protocol user configuration
DLSw config>enable dls
DLSw config>set srb fff
DLSw config>list dls
DLSw is                      ENABLED
LLC2 send Disconnect is      ENABLED

SRB Segment number          FFF
Max DLSw sessions           1000
DLSw global memory allotment 153344
LLC per-session memory allotment 8192
SDLC per-session memory allotment 4096

                                No MAC Address set

Database age timer           1200 seconds
Age timer resolution         300 seconds
Max wait timer for ICANREACH 20 seconds
Wait timer for LLC test response 15 seconds
Wait timer for SDLC test response 15 seconds
Join Group Interval          900 seconds
DLSw config>add tcp 9.67.46.77
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive?(E/D)- [D]? E
DLSw config>list tcp
Neighbor      Xmit Bufsize  Max Segsize  Keepalive
9.67.46.77    5120          1024         ENABLED
DLSw config>open-sap 0 00
DLSw config>open-sap 0 04
:

```

Figure 181 (Part 6 of 8). Scenario 3: 2210A Configuration via the ASCII Console

```

:
DLSw config>list open
Interface  SAP
0          0
0          4
DLSw config>exit
Config>Ctrl+p
*restart 31
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 32

+feature wrs 33
WAN Restoral console
WRS>list all

WAN Restoral is enabled with 1 circuit(s) configured

Total restoral attempts =          3 completions =          1
Total packets forwarded =          660

Longest completed restoral period in hrs:min:sec      0:04:07

Primary Interface      Secondary Interface      Restoral
-----
1 PPP/0 - Point to Poi 3 PPP/1 - Point to Poi      Yes

Router primary interface state = Up
Router secondary interface state = Available
Restoral Statistics:

Primary restoral attempts =          3 completions =          1
Restoral packets forwarded =          660
Most recent restoral period in hrs:min:sec      0:04:07

WRS>list all

WAN Restoral is enabled with 1 circuit(s) configured

Total restoral attempts =          3 completions =          1
Total packets forwarded =          970

:

```

Figure 181 (Part 7 of 8). Scenario 3: 2210A Configuration via the ASCII Console

```

:
Longest completed restoral period in hrs:min:sec      0:00:00

Primary Interface      Secondary Interface      Restoral
-----
1 PPP/0 - Point to Poi 3 PPP/1 - Point to Poi      Yes

Router primary interface state = Down
Router secondary interface state = Up
Restoral Statistics:

Primary restoral attempts =          3 completions =          1
Restoral packets forwarded =          970
Most recent restoral period in hrs:min:sec      0:01:54

WRS>exit
+protocol dls      34
Data Link Switching Console
DLSw>list tcp sessions
Group      IP Address      Conn State      Pkts Sent      Pkts Rcvd      Bytes Sent      Bytes Rcvd
-----
1          9.67.46.77      ESTABLISHED          1661          214          164679          19602
DLSw>list dls sessions all
Source      Destination      State      Flags      Dest IP Addr      Id
-----
1 400030000001 04 10005A861AF3 04 CONNECTED          9.67.46.77          13
DLSw>list dls sessions det 13
Source      Destination      State      Flags      Dest IP Addr      Id
-----
0 400030000001 04 10005A861AF3 04 CONNECTED          9.67.46.77          13

Personality:      TARGET
XIDs sent:        4
XIDs rcvd:        5
Datagrams sent:    0
Datagrams rcvd:    0
Info frames sent:  34
Info frames rcvd:  44
RIF:              0E21 FFF1 FFBF 5827 581D C31C 5D10

DLSw>exit
+Ctrl+p
*
```

Figure 181 (Part 8 of 8). Scenario 3: 2210A Configuration via the ASCII Console

Notes:

- 1 Talk to the CONFIG process.
- 2 Assign the name local-site to the 2210A phone number.
- 3 Assign the name remote-site to the 2210B phone number.
- 4 Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 3.

- 5** Set the data-link of interface 2 to V.25bis.
- 6** Lists the devices configuration. Interface 1 is the primary PPP link, interface 2 is the physical switched V.25bis link and interface 3 is the logical dial-circuit with PPP encapsulation method.
- 7** Customization of network 0. This is the token-ring interface. Specify that the unshielded media connector (UTP) is used and enter the locally administered address for this interface.
- 8** Customization of network 1. This is the serial 1 interface. Specify that the V.35 DTE cable is used.
- 9** Customization of network 2. This is the serial 2 interface with V.25bis modems.
- 10** List the interface 2 configuration.
- 11** Assign the phone number to the 2210 using the name defined earlier.
- 12** Set the number of retries for a call in case of no answer.
- 13** Set the number of seconds to wait before a retry.
- 14** Customization of network 3. This is the logical dial-circuit.
- 15** List the interface 3 configuration.
- 16** Set the physical network number on which the calls will be actually performed.
- 17** Allow the outbound calls only. Therefore, in the case of primary PPP link failure, the calls will be done from this 2210.
- 18** Set the idle timer to 0. This will cause the switched connection to stay up even if there is no packet to be sent.
- 19** Set the destination phone number using the name defined earlier.
- 20** Accept any inbound calls.
- 21** Access the link layer protocol that is running on this dial-circuit. The only encapsulation method available is PPP.
- 22** List the PPP link parameters. Defaults are used in this scenario.
- 23** Access the WAN Restoral (WRS) feature configuration.
- 24** Match the secondary dial circuit (interface 3) with the primary PPP leased link (interface 1).
- 25** Enable the WAN Restoral feature.
- 26** Enable the secondary circuit.
- 27** List the WAN Restoral feature configuration.

28 Customization of the IP protocol. Assign an IP address to the token-ring and the PPP link. Also, assign the internal IP address and enable RIP. No IP address must be assigned to the V.25bis interface or the dial-circuit interface. When the backup line is established, the dial-circuit assumes all the characteristics of the protocols customized for the primary PPP link.

29 Customization of the bridging function. Customize source route bridging on the token-ring interface. Assign bridge number and token-ring LAN segment number. Enable bridging and DLSw at the box level. This bridging configuration is required for the DLSw.

30 Customization of the DLSw protocol. Enable DLSw, and set the virtual segment number corresponding to the IP network. Add the IP address of the remote TCP neighbor, and open SAP 00 and 04 for DLSw.

31 Restart the 2210A to get the configuration running.

32 Talk to gateway operator console for monitoring.

33 Access the WAN Restoral feature (WRS) monitoring. First, list the WAN Restoral feature monitoring when the primary PPP link is down and the secondary switched link is up. Then, list the WAN Restoral feature monitoring when the primary PPP link has come back and the secondary switched link has been dropped.

34 Access the DLSw protocol monitoring. List the TCP connection and the SNA/DLSw sessions.

```

*
*talk 6 1

Config>add v25-bis-address local-site 8-352-2186 2
Config>add v25-bis-address remote-site 8-352-2184 3
Config>add device dial-circuit 4
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
Config>set data-link v25bis 2 5
Config>list devices 6
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN V.25bis): CSR 81640, CSR2 80E00, vector 92
Ifc 3 (PPP Dial Circuit): CSR 0, vector 0
Config>network 0 7
Ethernet interface configuration
ETH config>list
Connector type: AUTO-CONFIG
No IPX interface configuration
IP Encapsulation: ETHER

ETH config>exit
Config>network 1 8
Point-to-Point user configuration
PPP Config>set hdlc cable v35 dte
PPP Config>list all

LCP Parameters
-----
CONFIG Request Tries: 20 CONFIG Nak Tries: 10
Terminate Tries: 10 Retry Timer: 3000

LCP Options
-----
Max Receive Unit: 2048 Magic Number: Yes
Peer to Local (RX) ACCM: A0000
Protocol Field Comp(PFC): No Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using: none
Identify self as: ibm

NCP Parameters
-----
CONFIG Request Tries: 20 CONFIG Nak Tries: 10
Terminate Tries: 10 Retry Timer: 3000

:

```

Figure 182 (Part 1 of 7). Scenario 3: 2210B Configuration via the ASCII Console

```

:
CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit
Config>network 2           9
V.25bis Data Link Configuration
V.25bis Config>list        10
      V.25bis Configuration
Local Network Address Name  = Unassigned

Non-Responding addresses:
Retries                    = 1
Timeout                    = 0 seconds

Call timeouts:
Command Delay              = 0 ms
Connect                    = 60 seconds
Disconnect                 = 2 seconds
V.25bis Config>set local local-site 11
V.25bis Config>set retries-call-address 5 12
V.25bis Config>set timeout-call-address 60 13
V.25bis Config>list
      V.25bis Configuration
Local Network Address Name  = local-site
Local Network Address       = 8-352-2186

Non-Responding addresses:
Retries                    = 5
Timeout                    = 60 seconds

Call timeouts:
Command Delay              = 0 ms
Connect                    = 60 seconds
Disconnect                 = 2 seconds
V.25bis Config>exit
:

```

Figure 182 (Part 2 of 7). Scenario 3: 2210B Configuration via the ASCII Console

```

:
Config>network 3      14
Circuit configuration
Circuit Config>list   15

Base net:      0
Destination name:
Outbound calls    allowed
Inbound calls     allowed
Idle timer       = 60 sec
SelfTest Delay Timer = 150 ms

Circuit Config>set net 2      16
Circuit Config>set destination remote-site  17
Circuit Config>set calls inbound  18
Circuit Config>set idle 0      19
Circuit Config>set any_inbound  20
Circuit Config>list

Base net:      2
Destination name:  remote-site
Inbound calls    allowed
Idle timer       = 0 (fixed circuit)
SelfTest Delay Timer = 150 ms

Circuit Config>encapsulator  21
Point-to-Point user configuration
PPP Config>list all  22

LCP Parameters
-----
CONFIG Request Tries:      20    CONFIG Nak Tries:      10
Terminate Tries:          10    Retry Timer:      3000

LCP Options
-----
Max Receive Unit:      2048    Magic Number:      Yes
Peer to Local (RX) ACCM:  A0000
Protocol Field Comp(PFC):  No    Addr/Cntl Field Comp(ACFC):  No

Authentication Options
-----
Authenticate remote using:  none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20    CONFIG Nak Tries:      10
Terminate Tries:          10    Retry Timer:      3000

:

```

Figure 182 (Part 3 of 7). Scenario 3: 2210B Configuration via the ASCII Console

```

:
CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:          Disabled

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Circuit Config>exit
Config>protocol ip             23
Internet protocol user configuration
IP config>add address 0 9.67.46.77 255.255.255.240
IP config>add address 1 9.67.46.131 255.255.255.240
IP config>set internal IP address 9.67.46.77
IP config>enable rip
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0   9.67.46.77      255.255.255.240  Network broadcast,   fill 0
  intf 1   9.67.46.131    255.255.255.240  Network broadcast,   fill 0
  intf 2                                     IP disabled on this interface
  intf 3                                     IP disabled on this interface
Internal IP address: 9.67.46.77

Routing
Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
Per-interface address flags:
  intf 0   9.67.46.77      Send net and subnet routes
  intf 1   9.67.46.131    Send net and subnet routes
  intf 2                                     IP & RIP are disabled on this interface
  intf 3                                     IP & RIP are disabled on this interface

:

```

Figure 182 (Part 4 of 7). Scenario 3: 2210B Configuration via the ASCII Console

```

:
Accept RIP updates always for:
[NONE]

EGP: disabled

IP config>exit
Config>protocol dls 24
DLSw protocol user configuration
DLSw config>enable dls
DLSw config>set srb fff
DLSw config>list dls
DLSw is                               ENABLED
LLC2 send Disconnect is              ENABLED

SRB Segment number                   FFF
Max DLSw sessions                    1000
DLSw global memory allotment         153344
LLC per-session memory allotment     8192
SDLC per-session memory allotment    4096

                                     No MAC Address set

Database age timer                   1200 seconds
Age timer resolution                 300 seconds
Max wait timer for ICANREACH         20 seconds
Wait timer for LLC test response     15 seconds
Wait timer for SDLC test response    15 seconds
Join Group Interval                  900 seconds
DLSw config>add tcp 9.67.46.146
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive?(E/D)- [D]? E
DLSw config>list tcp
Neighbor      Xmit Bufsize   Max Segsize   Keepalive
9.67.46.146   5120          1024         ENABLED
DLSw config>open-sap 0 00
DLSw config>open-sap 0 04
DLSw config>list open
Interface  SAP
0          0
0          4
DLSw config>exit
Config>protocol asrt 25
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>enable dls
ASRT config>list bridge

:

```

Figure 182 (Part 5 of 7). Scenario 3: 2210B Configuration via the ASCII Console

```

:
Source Routing Transparent Bridge Configuration
=====

Bridge: Enabled Bridge Behavior: STB
+-----+
-----] SOURCE ROUTING INFORMATION ]-----
+-----+

Bridge Number: N/A Segments: 0
Max ARE Hop Cnt: 00 Max STE Hop cnt: 00
1:N SRB: Not Active Internal Segment: 0x000
LF-bit interpret: Extended
+-----+
-----] SR-TB INFORMATION ]-----
+-----+

SR-TB Conversion: Disabled
TB-Virtual Segment: 0x000 MTU of TB-Domain: 0
+-----+
-----] SPANNING TREE PROTOCOL INFORMATION ]-----
+-----+

Bridge Address: Default Bridge Priority: 32768/0x8000
STP Participation: IEEE802.1d
+-----+
-----] TRANSLATION INFORMATION ]-----
+-----+

FA<=>GA Conversion: Enabled UB-Encapsulation: Disabled
DLS for the bridge: Enabled
+-----+
-----] PORT INFORMATION ]-----
+-----+

Number of ports added: 2
Port: 1 Interface: 0 Behavior: STB Only STP: Enabled
Port: 2 Interface: 1 Behavior: STB Only STP: Enabled

ASRT config>exit
Config>feature wrs 26
WAN Restoral user configuration
WRS Config>add secondary-circuit 3 1 27
WRS Config>enable wrs 28
WRS Config>enable secondary-circuit 29
Secondary interface number [0]? 3
WRS Config>enable secondary-circuit 3
WRS Config>list 30

WAN Restoral is enabled.

Primary Interface Secondary Interface Restoral
-----
1 - WAN PPP 3 - PPP Dial Circuit Yes
WRS Config>exit
Config>Ctrl+p

:

```

Figure 182 (Part 6 of 7). Scenario 3: 2210B Configuration via the ASCII Console


```

:
*restart 31
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
*talk 5

+protocol dls 32
Data Link Switching Console
DLSw>list tcp sessions
  Group      IP Address  Conn State  Pkts Sent  Pkts Rcvd  Bytes Sent  Bytes Rcvd
-----
1           9.67.46.146 ESTABLISHED      188        1606        19579        159423
DLSw>list dls sessions all
  Source      Destination      State      Flags      Dest IP Addr      Id
-----
1 10005A861AF3 04 400030000001 04 CONNECTED      9.67.46.146      487
DLSw>list dls sessions det 487
  Source      Destination
State      Flags      Dest IP Addr      Id
-----
0 10005A861AF3 04 400030000001 04 CONNECTED      9.67.46.146      487

  Personality:      ORIGINATOR
  XIDs sent:        5
  XIDs rcvd:        4
  Datagrams sent:    0
  Datagrams rcvd:    0
  Info frames sent:  44
  Info frames rcvd:  34
  RIF:

DLSw>exit
+Ctrl+p
*

```

Figure 182 (Part 7 of 7). Scenario 3: 2210B Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Assign the name local-site to the 2210B phone number.
- 3** Assign the name remote-site to the 2210A phone number.
- 4** Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 3.

- 5** Set the data-link of interface 2 to V.25bis.
- 6** Lists the devices configuration. Interface 1 is the primary PPP link, interface 2 is the physical switched V.25bis link and interface 3 is the logical dial-circuit with the PPP encapsulation method.
- 7** Customization of network 0. List the Ethernet interface. There is nothing to change.
- 8** Customization of network 1. This is the serial 1 interface. Specify that a V.35 DTE cable is used.
- 9** Customization of network 2. This is the serial 2 interface with V.25bis modems.
- 10** List the interface 2 configuration.
- 11** Set the local phone number referring to the v25-bis-address name defined earlier.
- 12** Set the number of retries for a call in case of no answer.
- 13** Set the number of seconds to wait before a retry.
- 14** Customization of network 3. This is the logical dial-circuit.
- 15** List the interface 3 configuration.
- 16** Set the physical network number on which the calls will be actually performed (V.25bis interface 2).
- 17** Set the destination phone number using the name defined earlier.
- 18** Allow the INBOUND calls only. Therefore, in case of a primary PPP link failure, 2210B will wait for the call from 2210A.
- 19** Set the idle timer to 0. The switched connection will stay up even if there are no packets to send.
- 20** Accept any inbound calls.
- 21** Access the link layer protocol that is running on the dial-circuit. The only encapsulation method available is PPP.
- 22** List the PPP link parameters. Defaults are used in this scenario.
- 23** Customization of the IP protocol. Assign IP address to the Ethernet and PPP link. Also, assign the internal IP address and enable RIP. The IP address for the serial interfaces must be added only to the primary interface. No IP address must be assigned to the V.25bis interface or the dial-circuit interface. When a backup line is established, it assumes all the characteristics of the primary PPP link.
- 24** Customization of the DLSw protocol. Enable DLSw and set the virtual segment number corresponding to the IP network. Add the IP address of the remote TCP neighbor, and open SAP 00 and 04 for DLSw.

- 25** Customization of the bridging function. Transparent bridging is already enabled by default for the Ethernet interface. Enable bridge and DLSw at the box level. This bridging configuration is required because of the requirements of DLSw.
- 26** Access the WAN Restoral (WRS) feature configuration.
- 27** Match the secondary dial-circuit (interface 3) with the primary PPP leased link (interface 1).
- 28** Enable the WAN Restoral feature.
- 29** Enable the secondary-circuit.
- 30** List the WAN Restoral feature configuration.
- 31** Restart the 2210B to get the configuration running.
- 32** Access the DLSw protocol monitoring. List the TCP connection and the SNA/DLSw sessions.

On 2210 Navigation Window :

- Select CONFIGURE from the menu bar
- Select NEW CONFIGURATION **1**

Select V.25bis
ADDRESSES panel of GENERAL subdirectory of DEVICES directory.

On V25bis ADDRESSES Window :

- ADDRESS NAME = **local-site**
- ADDRESS NUMBER = **8-352-2184**
- Select **ADD** **2**

- ADDRESS NAME = **remote-site**
- ADDRESS NUMBER = **8-352-2186**
- Select **ADD** **3**

Select V25bis SECONDARY CIRCUITS panel of GENERAL subdirectory of DEVICES directory.

On SECONDARY CIRCUITS Window:

- Select V25bis NETWORK NUMBER
- Select **2** **4**
- Select CALLS
- Select **OUTBOUND** **5**
- IDLE TIMER = **0** **6**
- SELF TEST DELAY TIMER = 150
- Select DESTINATION ADDRESS NAME
- Select **remote-site** **7**
- Select DESTINATION INBOUND ADDRESS NAME
- Select **local-site** **8**
- Select **ANY INBOUND**
- Select **ADD** **9**

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window:

- Select MODEL
- Select **MODEL 125** **10**
- Select CONFIGURATION of Token-Ring line **11**
- ENABLE INTERFACE
- MAC ADDRESS = **40002210A001**
- Select SPEED
- Select 4
- Select PACKET SIZE
- Select 2052
- Select CABLE TYPE
- Select **UTP**
- RIF TIMER = 120
- DISABLE END NODE SOURCE ROUTING

Select the data-link protocol of Serial 1 (PPP by default)

- Select PPP

:

Figure 183 (Part 1 of 5). Scenario 3: 2210A Configuration via the Nways MRS Configuration Program

```

:
Select CONFIGURATION of Serial 1 12
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
      Select NRZ
    Select IDLE
      Select FLAG
    Select CLOCKING
      Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
      Select V.35 DTE
    Subpanels LCP, BNCP and IPCP not modified

Select the data-link protocol of Serial 2 (PPP by default)
  Select V.25bis 13

Select CONFIGURATION of Serial 2
  On GENERAL subpanel :
    ENABLE INTERFACE 14
    RETRIES = 5
    TIMEOUT = 60
    Select LOCAL NETWORK ADDRESS NAME
      Select local-site 15
    COMMAND DELAY = 0
    CONNECT = 60
    DISCONNECT = 2

On 2210 Navigation Window :
Select GENERAL panel of IP subdirectory of PROTOCOLS directory

On IP - GENERAL Window :
ENABLE IP 16
Internal Address = 9.67.46.146

On 2210 Navigation Window :
Select INTERFACES panel of IP subdirectory of PROTOCOLS directory

On IP - INTERFACES Window :
  Select IP ADDRESSES of Token-Ring line
    IP Address = 9.67.46.146
    Subnet Mask = 255.255.255.240
    Select ADD
  Select IP ADDRESSES of Serial 1 line
    IP Address = 9.67.46.132
    Subnet Mask = 255.255.255.240
    Select ADD
  Do NOT customize IP ADDRESS for Serial 2 line

:

```

Figure 183 (Part 2 of 5). Scenario 3: 2210A Configuration via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select GENERAL panel of RIP subdirectory of IP subdirectory of PROTOCOLS directory

On RIP - GENERAL Window :
ENABLE RIP 17

On 2210 Navigation Window :
Select GENERAL panel DLSw subdirectory of PROTOCOL directory.

On DLSw GENERAL window :
ENABLE DLSw 18
SRB SEGMENT = FFF 19
MAXIMUM DLSw SESSIONS = 150
DLSw MAC ADDRESS = 0
ADDRESS DATABASE AGE = 1200
ADDRESS AGING INTERVAL = 300
ICANREACH WAIT TIMEOUT = 20
LLC TEST TIMEOUT = 15
SDLC TEST TIMEOUT = 15
GROUP JOIN INTERVAL = 900
ENABLE LLC DISCONNECT
DLSw MEMORY ALLOTMENT = 153344
LLC SESSION MEMORY ALLOTMENT = 8192
SDLC SESSION MEMORY ALLOTMENT = 4096

On 2210 Navigation Window :
Select TCP CONNECTIONS panel DLSw subdirectory of PROTOCOL directory.

On DLSw TCP CONNECTIONS window :
DLSw NEIGHBOR IP ADDRESS = 9.67.46.77 20
TRANSMIT BUFFER SIZE = 5120
MAXIMUM SEGMENT SIZE = 1024
ENABLE KEEPALIVE

On 2210 Navigation Window :
Select INTERFACES panel DLSw subdirectory of PROTOCOL directory.

On DLSw INTERFACES window :
Select CONFIGURE box of Token-Ring line
Verify SAP 00 and 04 are listed. 21

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 22
ENABLE DLSw 23

:

```

Figure 183 (Part 3 of 5). Scenario 3: 2210A Configuration via the Nways MRS Configuration Program

```

:
In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 1
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 1
  Select LF BIT INTERPRETATION
    Select EXTENDED
  ENABLE FA-GA

In SOURCE ROUTING TRANSPARENT BRIDGE box
  DISABLE SR <--> TB CONVERSION

In TRANSPARENT BRIDGE box
  FILT. DBASE SIZE = 2048
  AGING TIME = 300
  RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE Token-Ring
Select CONFIGURE of Token-Ring
  Select INTERFACE SUPPORTS
    Select SRB
    Select DUPLICATE FRAMES
    Select STE&TSF
    SEGMENT NUMBER = FFB 24
    MTU UNIT = 4399
    ENABLE STE

  DISABLE SERIAL 1
  Box CONFIGURE of Serial 1 not customized

  DISABLE SERIAL 2
  Box CONFIGURE of Serial 2 not customized

Select WRS CIRCUIT panel of WRS subdirectory of FEATURES directory.

On WRS GENERAL Window :
ENABLE WRS 25
ENABLE WRS SECONDARY CIRCUIT 26
Select SECONDARY INTERFACE NUMBER
  Select 3 27
Select PRIMARY INTERFACE NUMBER
  Select 1 28

:

```

Figure 183 (Part 4 of 5). Scenario 3: 2210A Configuration via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
    Select CONFIGURE from the menu bar
        Select CREATE ROUTER CONFIGURATION 29

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
    Enter W RSA 30
    Select OK

```

Figure 183 (Part 5 of 5). Scenario 3: 2210A Configuration via the Nways MRS Configuration Program

Notes:

- 1** Start the customization from an empty configuration.
- 2** Assign the name local site to phone number 301-2184. This is the local phone number of 2210A.
- 3** Assign the name remote site to phone number 301-2186. This is the phone number of the remote 2210B.
- 4** Map the secondary circuit to the V.25bis interface 2.
- 5** The backup call will be performed by 2210A. The 2210B must specify Inbound for this parameter.
- 6** The idle timer must be set to 0 to keep up the switched link even if there is no packet to send over it.
- 7** This is the name of the phone number to call in case of a primary link failure.
- 8** This is the name of the destination address from the remote site's point of view.
- 9** This adds the secondary circuit. You can see in the list at the top of the window that the interface number for this secondary circuit is 3.
- 10** The router is a 2210 Model 125, with token-ring LAN, 4 MB Flash, 8 MB RAM, and without an ISDN BRI adapter.
- 11** Customization of the token-ring interface. Assign a locally administered address, and specify the unshielded (UTP) connector used.
- 12** Customization of serial 1. Nothing has been changed from the default. The RS-232 DTE cable is already the default.
- 13** Specify the V.25bis data-link for the interface 2.
- 14** The V.25bis interface is already enabled by default.
- 15** This is the name of the local phone number.
- 16** Customization of the IP protocol. Assign IP addresses to the Ethernet and the PPP link interface. Also, assign the internal IP address.

17 Customization of the RIP protocol. Enable RIP.

18 Enable DLSw.

19 This is the virtual segment number used for DLSw. It must be the same on every DLSw partner.

20 This is the remote TCP neighbor address, also called the DLSw partner.

21 By default SAP 00 and SAP 04 are already open on the LAN interface.

22 Customization of the bridging function. Enable bridging at the box level.

23 Enable DLSw at the box level.

24 Select SRB for a token-ring interface with LAN Segment number FF1.

25 Enable the WAN Restoral feature.

26 Enable the secondary circuit.

27 Set the secondary interface as logical interface number 3. It is already the default.

28 Set the primary interface as physical interface number 1.

29 Create the configuration file.

30 This is the name of the configuration file stored in the workstation.

On 2210 Navigation Window :

- Select CONFIGURE from the menu bar
- Select NEW CONFIGURATION **1**

Select V25bis ADDRESSES panel of GENERAL subdirectory of DEVICES directory.

On V25bis ADDRESSES Window :

- ADDRESS NAME = **local-site**
- ADDRESS NUMBER = **8-352-2186**
- Select **ADD** **2**

- ADDRESS NAME = **remote-site**
- ADDRESS NUMBER = **8-352-2184**
- Select **ADD** **3**

Select V25bis SECONDARY CIRCUITS panel of GENERAL subdirectory of DEVICES directory.

On SECONDARY CIRCUITS Window:

- Select V25bis NETWORK NUMBER
- Select **2** **4**
- Select CALLS
- Select **INBOUND** **5**
- IDLE TIMER = **0** **6**
- SELF TEST DELAY TIMER = 150
- Select DESTINATION ADDRESS NAME
- Select **remote-site** **7**
- Select DESTINATION INBOUND ADDRESS NAME
- Select **local-site** **8**
- Select **ANY INBOUND**
- Select **ADD** **9**

Select INTERFACES panel of DEVICES directory

On DEVICE INTERFACES Window :

- Select MODEL
- Select **MODEL 126** **10**
- Select CONFIGURATION of Ethernet line **11**
- ENABLE INTERFACE
- Select CONNECTOR TYPE
- Select **AUTO-CONFIG**
- Select IP ENCAPSULATION
- Select ETHERNET

- Select the data-link protocol of Serial 1 (PPP by default)
- Select PPP

:

Figure 184 (Part 1 of 4). Scenario 3: 2210B Configuration via the Nways MRS Configuration Program

```

:
Select CONFIGURATION of Serial 1 12
  On GENERAL subpanel :
    ENABLE INTERFACE
    MAXIMUM TRANSMISSION UNIT = 2048
    Select ENCODING
      Select NRZ
    Select IDLE
      Select FLAG
    Select CLOCKING
      Select EXTERNAL
    CLOCK SPEED = 0
    TRANSMIT DELAY = 0
    Select CABLE TYPE
      Select V.35 DTE
    Subpanels LCP, BNCP and IPCP not modified

Select the data-link protocol of Serial 2 (PPP by default)
  Select V.25bis 13

Select CONFIGURATION of Serial 2
  On GENERAL subpanel :
    ENABLE INTERFACE 14
    RETRIES = 5
    TIMEOUT = 60
    Select LOCAL NETWORK ADDRESS NAME
      Select local-site 15
    COMMAND DELAY = 0
    CONNECT = 60
    DISCONNECT = 2

On 2210 Navigation Window :
Select GENERAL panel of IP subdirectory of PROTOCOLS directory

On IP - GENERAL Window :
ENABLE IP 16
Internal Address = 9.67.46.77

On 2210 Navigation Window :
Select INTERFACES panel of IP subdirectory of PROTOCOLS directory

On IP - INTERFACES Window :
  Select IP ADDRESSES of Ethernet line
    IP Address = 9.67.46.77
    Subnet Mask = 255.255.255.240
    Select ADD
  Select IP ADDRESSES of Serial 1 line
    IP Address = 9.67.46.131
    Subnet Mask = 255.255.255.240
    Select ADD
  Do NOT customize IP ADDRESS for Serial 2 line

:

```

Figure 184 (Part 2 of 4). Scenario 3: 2210B Configuration via the Nways MRS Configuration Program

```

:
On 2210 Navigation Window :
Select GENERAL panel of RIP subdirectory of IP subdirectory of PROTOCOLS directory

On RIP - GENERAL Window :
ENABLE RIP 17

On 2210 Navigation Window :
Select GENERAL panel DLSw subdirectory of PROTOCOL directory.

On DLSw GENERAL window :
ENABLE DLSw 18
SRB SEGMENT = FFF 19
MAXIMUM DLSw SESSIONS = 150
DLSw MAC ADDRESS = 0
ADDRESS DATABASE AGE = 1200
ADDRESS AGING INTERVAL = 300
ICANREACH WAIT TIMEOUT = 20
LLC TEST TIMEOUT = 15
SDLC TEST TIMEOUT = 15
GROUP JOIN INTERVAL = 900
ENABLE LLC DISCONNECT
DLSw MEMORY ALLOTMENT = 153344
LLC SESSION MEMORY ALLOTMENT = 8192
SDLC SESSION MEMORY ALLOTMENT = 4096

On 2210 Navigation Window :
Select TCP CONNECTIONS panel DLSw subdirectory of PROTOCOL directory.

On DLSw TCP CONNECTIONS window :
DLSw NEIGHBOR IP ADDRESS = 9.67.46.146 20
TRANSMIT BUFFER SIZE = 5120
MAXIMUM SEGMENT SIZE = 1024
ENABLE KEEPALIVE

On 2210 Navigation Window :
Select INTERFACES panel DLSw subdirectory of PROTOCOL directory.

On DLSw INTERFACES window :
Select CONFIGURE box of Ethernet line
Verify SAP 00 and 04 are listed. 21

On 2210 Navigation Window :
Select BRIDGING - GENERAL panel of BRIDGING directory

On BRIDGING - GENERAL Window :
ENABLE BRIDGING 22
ENABLE DLSw 23
:

```

Figure 184 (Part 3 of 4). Scenario 3: 2210B Configuration via the Nways MRS Configuration Program

```

:
In SOURCE ROUTING BRIDGE box
  BRIDGE NUMBER = 1
  MAXIMUM ARE HOP COUNT = 14
  MAXIMUM STE HOP COUNT = 14
  INTERNAL VIRTUAL SEGMENT = 1
  Select LF BIT INTERPRETATION
    Select EXTENDED
  ENABLE FA-GA 24

In SOURCE ROUTING TRANSPARENT BRIDGE box
  DISABLE SR <--> TB CONVERSION

In TRANSPARENT BRIDGE box
  FILT. DBASE SIZE = 2048
  AGING TIME = 300
  RESOLUTION TIME = 5

On 2210 Navigation Window :
Select INTERFACES panel of INTERFACES subdirectory of BRIDGING directory

On BRIDGING - INTERFACES Window :
ENABLE Ethernet
Select CONFIGURE of Ethernet
  Select INTERFACE SUPPORTS
    Select STB 25
  Select DUPLICATE FRAMES
    Select STE&TSF
  SEGMENT NUMBER = 1

DISABLE SERIAL 1
Box CONFIGURE of Serial 1 not customized

DISABLE SERIAL 2
Box CONFIGURE of Serial 2 not customized

Select WRS CIRCUIT panel of WRS subdirectory of FEATURES directory.

On WRS GENERAL Window :
ENABLE WRS 26
ENABLE WRS SECONDARY CIRCUIT 27
Select SECONDARY INTERFACE NUMBER
  Select 3 28
Select PRIMARY INTERFACE NUMBER
  Select 1 29

On 2210 Navigation Window :
Select CONFIGURE from the menu bar
  Select CREATE ROUTER CONFIGURATION 30

On FILE NAME FOR CONFIGURATION DATA,PLEASE? window :
Enter WRSB 31
Select OK

```

Figure 184 (Part 4 of 4). Scenario 3: 2210B Configuration via the Nways MRS Configuration Program

Notes:

- 1** Start the customization from an empty configuration.
- 2** Assign the name local site to phone number 301-2186. This is the local phone number of 2210B.
- 3** Assign the name remote site to phone number 301-2184. This is the phone number of the remote 2210A.
- 4** Map the secondary circuit to the V.25bis interface 2.
- 5** 2210B will receive the backup calls. The 2210A must specify Outbound for this parameter.
- 6** The idle timer must be set to 0 to keep up the switched link up even if there is no packet to send over it.
- 7** This is the name of the phone number to call in case of a primary link failure.
- 8** This is the name of the destination address from the remote site's point of view.
- 9** Add the secondary circuit. You can see in the list at the top of the window that the interface number for this secondary circuit is 3.
- 10** The router is a 2210 Model 126, with Ethernet LAN, 4MB Flash, 8MB RAM, and without an ISDN BRI adapter.
- 11** Customization of the Ethernet interface. Specify AUTOCONFIG for the connector type. This will let the IBM 2210 automatically discover the type of connector used.
- 12** Customization of serial 1. Nothing has been changed from the default.
- 13** Specify the V.25bis data-link for the interface 2.
- 14** The V.25bis interface is already enabled by default.
- 15** This is the name of the local phone number.
- 16** Customization of the IP protocol. Assign IP addresses to the Ethernet and the PPP link interfaces. Also, assign the internal IP address.
- 17** Customization of the RIP protocol. Enable RIP.
- 18** Enable DLSw.
- 19** This is the virtual segment number used for DLSw. It must be the same on every DLSw partner.
- 20** This is the remote TCP neighbor address, also called the DLSw partner.

- 21** By default SAP 00 and SAP 04 are already open on the LAN interface.
- 22** Customization of the bridging function. Enable bridging at the box level.
- 23** Enable DLSw at the box level.
- 24** Having FA-GA mapping enabled is a requirement when you do DLSw with Ethernet. This is the default.
- 25** Select STB for the Ethernet interface.
- 26** Enable the WAN Restoral feature.
- 27** Enable the secondary circuit.
- 28** Set the secondary interface as logical interface number 3. It is the default.
- 29** Set the primary interface as physical interface number 1.
- 30** Create the configuration file.
- 31** This is the name of the configuration file stored on the workstation.

11.5.4 Scenario 4: WAN Restoral (WRS) Implementation with IP, DLSw and Bridging using ISDN

In this scenario, we have one 2210 with token-ring interface (2210A) and one 2210 with Ethernet interface (2210B). Both 2210s are linked together using the following:

1. Leased primary PPP link with V.35 modems on physical interface 1 for both 2210s.
2. Backup PPP link over the ISDN on physical interface 3 for both 2210s.

2210A routes IP and DLSw with source route bridging on a token-ring interface 0.

2210B routes IP and DLSw with transparent bridging on Ethernet interface 0.

- Interfaces:

The token-ring interface on 2210A runs at 4 MBps and is attached to the LAN using the UTP connector. It uses the MAC address 40002210A001.

Leased primary serial link is a PPP link over V.35 modems.

Backup serial link is a PPP link over ISDN.

The Ethernet interface on 2210B is connected to the LAN using the 10Base-T connector.

- Bridging:

2210A is configured for source route-translational bridging with SRB on the token-ring interface, and STB on the serial 1 interface. The bridge number of 2210A is 1. The LAN segment number of the token-ring is FFB and the TB-Domain is seen from SRB Domain as the LAN segment number FFF. DLSw is enabled at box level.

Note: The bridging function is configured because of the requirements of DLSw.

2210B is configured for transparent bridging on both serial 1 and Ethernet interfaces. DLSw is enabled at box level.

Note: The bridging function is configured because of the requirements of DLSw.

- IP routing:

2210A is an IP router with IP address 9.67.46.146 on its token-ring interface and IP address 9.67.46.132 on its serial 1 interface. Its internal IP address is 9.67.46.146, and RIP is enabled for 2210A.

2210B is an IP router with IP address 9.67.46.77 on its Ethernet interface and IP address 9.67.46.131 on its serial 1 interface. Its internal IP address is 9.67.46.77, and RIP is enabled for 2210B.

- DLSw protocol:

2210B and 2210A are DLSw partners for each other. From 2210s, the DLSw network is seen as segment number FFF.

- WAN Restoral feature:

Dial number of 2210A is 8-352-2184. Dial number of 2210B is 8-352-2186. The call backup will be done from 2210A to 2210B.

For more information about IP protocol customization, see 8.2, “Configuring IP on the IBM 2210” on page 341.

For more information about DLSw protocol customization, see 10.3, “DLSw Configuration on the IBM 2210” on page 453.

For more information about bridging (ASRT) protocol customization, see 4.4, “Bridging Scenarios and Configurations” on page 138.

Figure 185 on page 643 shows the configuration of the network used in this scenario. The customization samples for this scenario are provided as follows:

- Figure 186 on page 644 shows the 2210A configuration via the ASCII console.
- Figure 187 on page 655 shows the 2210B configuration via the ASCII console.

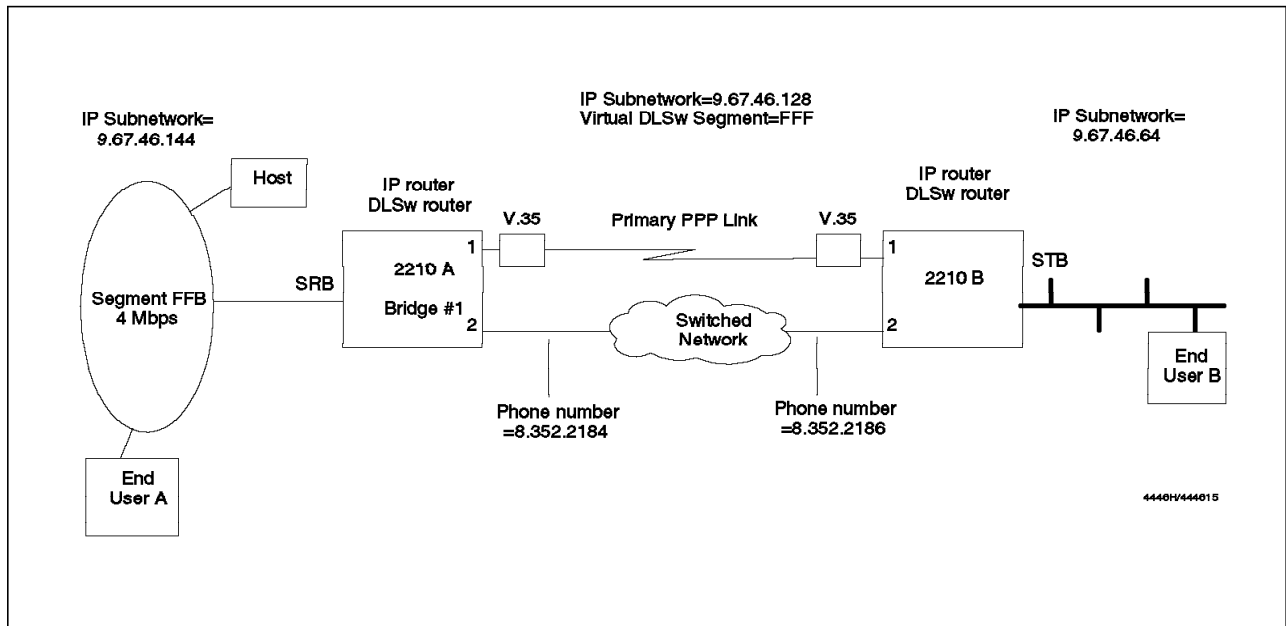


Figure 185. Scenario 4: WAN Restoral (WRS) Using ISDN

```

*
*talk 6 1

Config>add isdn
Assign address name [1-23] chars []? local-site 2
Assign network dial address [1-25 digits] []? 8-352-2184 2
Assign network subdial address [0-20 digits] []? 2
Config>add isdn
Assign address name [1-23] chars []? remote-site 3
Assign network dial address [1-25 digits] []? 8-352-2186 3
Assign network subdial address [0-20 digits] []? 3
Config>add device dial-circuit 4
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Config>set data-link ppp 4 5
Config>list isdn-address 6

Address assigned name      Network Address  Network Subaddress
-----
local-site                 8-352-2184
remote-site                8-352-2186
Config>list devices 7
Ifc 0   Token Ring                CSR 6000000, vector 28
Ifc 1   WAN PPP                   CSR 81620, CSR2 80D00, vector 93
Ifc 2   WAN PPP                   CSR 81640, CSR2 80E00, vector 92
Ifc 3   ISDN Basic                CSR 0, vector 0
Ifc 4   PPP Dial Circuit           CSR 0, vector 0
Config>network 0 8
Token-Ring interface configuration
TKR config>media unshielded
TKR config>set physical-address 40:00:22:10:A0:01
TKR config>list all
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                      4 Mb/sec
Media:                      Unshielded

RIF Aging Timer:           120
Source Routing:             Enabled
MAC Address:                40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 1 9
Point-to-Point user configuration
PPP Config>set hdlc cable v35 dte

:

```

Figure 186 (Part 1 of 9). Scenario 4: 2210A Configuration via the ASCII Console

```

:
PPP Config>list all

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):      No     Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using: none
Identify self as:             ibm

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:          Disabled

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Config>network 3               10
ISDN user configuration
ISDN Config>list               11
ISDN Configuration

Local Network Address Name      = Unassigned
Local Network Address:Subaddress = Unassigned

:

```

Figure 186 (Part 2 of 9). Scenario 4: 2210A Configuration via the ASCII Console

```

:
Maximum frame size in bytes      = 2048
Outbound call address Timeout    = 180 Retries = 2
Switch Variant                   = Net 3
Multipoint Selection             = Point-to-Point
TEI                              = Automatic
PS1 detect                      = Disabled
No circuit address accounting information being kept
ISDN Config>set local-address-name
Assign local address name []? local-site 13
ISDN Config>set switch
Switch-Variant-Model [NET3]? net3 14
ISDN Config>set dn0
Enter DNO (Directory-Number-0) []? 8-352-2184 15
ISDN Config>set retries-call-address 5 16
ISDN Config>set timeout-call-address 60 17
ISDN Config>list 12
ISDN Configuration

Local Network Address Name      = local-site
Local Network Address:Subaddress = 8-352-2184:

Maximum frame size in bytes      = 2048
Outbound call address Timeout    = 60 Retries = 5
Switch Variant                   = Net 3
DNO (Directory Number 0)        = 8-352-2184
Multipoint Selection             = Point-to-Point
TEI                              = Automatic
PS1 detect                      = Disabled
No circuit address accounting information being kept
ISDN Config>exit
Config>network 4 18
Circuit configuration
Circuit config: 4>list 19

Base net                        = 0
Destination name                =
Circuit priority                = 8

Outbound calls                  = allowed
Idle timer                      = 60 sec
SelfTest Delay Timer            = 150 ms

Circuit Config: 4>set net 3 20
Circuit Config: 4>set calls outbound 21
Circuit Config: 4>set idle
Idle timer (seconds, 0 means always active) [60]? 0 22
Circuit Config: 4>set destination remote-site 23
:

```

Figure 186 (Part 3 of 9). Scenario 4: 2210A Configuration via the ASCII Console

```

:
Circuit Config: 4>list 24

Base net                = 3
Destination name        = remote-site
Circuit priority        = 8

Outbound calls          = allowed
Idle timer              = 0 (fixed circuit)
SelfTest Delay Timer    = 150 ms

Circuit Config: 4>encapsulator 25
Point-to-Point user configuration
PPP Config>list all 26

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:      3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:      Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):    No   Addr/Cntl Field Comp(ACFC):    No

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:      3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

:

```

Figure 186 (Part 4 of 9). Scenario 4: 2210A Configuration via the ASCII Console

```

:
IPCP Options
-----
IPCP Compression:          None
IP Address:      Don't Send or Request
PPP Config>exit
Circuit config:  4>exit
Config>feature wrs      27
Feature name or number [WAN Restoral System]?
WAN Restoral user configuration
WRS Config>add secondary-circuit 4 1      28
WRS Config>enable wrs      29
WRS Config>enable secondary-circuit      30
Secondary interface number [0]? 4
WRS Config>list all      31

WAN Restoral is enabled.
Default Stabilization Time:      0 seconds
Default First Stabilization Time: 0 seconds

      Primary Interface      Secondary Interface      Secondary
      -----      -----      -----
1 - WAN PPP      4 - PPP Dial Circuit      Yes
[No Primary-Alternate pairs defined]
WRS Config>exit
Config>protocol ip      32
Internet protocol user configuration
IP config>add address 0 9.67.46.146 255.255.255.240
IP config>add address
Which net is this address for [0]? 1
New address [0.0.0.0]? 9.67.46.132
Address mask [255.0.0.0]? 255.255.255.240
IP config>enable rip
IP config>set internal IP address 9.67.46.146
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.146      255.255.255.240  Network broadcast,    fill 0
  intf 1  9.67.46.132      255.255.255.240  Network broadcast,    fill 0
  intf 2                                IP disabled on this interface
Internal IP address: 9.67.46.146

Routing

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled

:

```

Figure 186 (Part 5 of 9). Scenario 4: 2210A Configuration via the ASCII Console

```

:
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0   9.67.46.146      Send net and subnet routes
    intf 1   9.67.46.132      Send net and subnet routes
    intf 2                                IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

EGP: disabled

IP config>exit
Config>protocol asrt 33
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>disable transparent 1
ASRT config>enable source-routing 1
Segment Number for the port in hex(1 - FFF) [1]? ffb
Bridge number in hex (1 - 9, A - F) [1]? 1
ASRT config>enable sr-tb-conversion
TB-Domain Segment Number in hex(1 - FFF) [1]? fff
TB-Domain's MTU [1470]?
ASRT config>enable dls
ASRT config>list bridge

          Source Routing Transparent Bridge Configuration
          =====

Bridge:           Enabled           Bridge Behavior: SR<->TB
-----+-----+
-----] SOURCE ROUTING INFORMATION ]-----
-----+-----+
Bridge Number:    01                 Segments:          1
Max ARE Hop Cnt:  14                 Max STE Hop cnt:   14
1:N SRB:          Not Active         Internal Segment:  0x000
LF-bit interpret: Extended
-----+-----+
-----] SR-TB INFORMATION ]-----
-----+-----+
SR-TB Conversion: Enabled
TB-Virtual Segment: 0xFF             MTU of TB-Domain: 1470

:

```

Figure 186 (Part 6 of 9). Scenario 4: 2210A Configuration via the ASCII Console

```

:
+-----+
-----] SPANNING TREE PROTOCOL INFORMATION ]-----
+-----+
Bridge Address:      Default      Bridge Priority: 32768/0x8000
STP Participation:   IEEE802.1d on TB ports, IBM-8209 and IBM-SRB proprietary on SR ports
+-----+
-----] TRANSLATION INFORMATION ]-----
+-----+
FA<=>GA Conversion:  Enabled      UB-Encapsulation: Disabled
DLS for the bridge: Enabled
+-----+
-----] PORT INFORMATION ]-----
+-----+
Number of ports added: 2
Port: 1      Interface: 0      Behavior: SRB Only  STP: Enabled
Port: 2      Interface: 1      Behavior: STB Only  STP: Enabled

ASRT config>exit
Config>protocol dls 34
DLSw protocol user configuration
DLSw config>enable dls
DLSw config>set srb fff
DLSw config>list dls
DLSw is                      ENABLED
LLC2 send Disconnect is      ENABLED

SRB Segment number          FFF
Max DLSw sessions           1000
DLSw global memory allotment 153344
LLC per-session memory allotment 8192
SDLC per-session memory allotment 4096

                               No MAC Address set

Database age timer           1200 seconds
Age timer resolution         300 seconds
Max wait timer for ICANREACH 20 seconds
Wait timer for LLC test response 15 seconds
Wait timer for SDLC test response 15 seconds
Join Group Interval          900 seconds
DLSw config>add tcp 9.67.46.77
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive?(E/D)- [D]? E
DLSw config>list tcp
Neighbor      Xmit Bufsize  Max Segsize  Keepalive
9.67.46.77    5120          1024         ENABLED
DLSw config>open-sap 0 00
DLSw config>open-sap 0 04
:

```

Figure 186 (Part 7 of 9). Scenario 4: 2210A Configuration via the ASCII Console


```

:
DLSw config>list open
Interface  SAP
0          0
0          4
DLSw config>exit
Config>Ctrl+p
*restart 35
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*talk 5 36

+feature wrs 37
WAN Restoral console
WRS>list all

WAN Restoral is enabled with 1 circuit(s) configured

Total restoral attempts =          3 completions =          1
Total packets forwarded =          660

Longest completed restoral period in hrs:min:sec      0:04:07

Primary Interface      Secondary Interface      Restoral
-----
1 PPP/0 - Point to Poi 3 PPP/1 - Point to Poi      Yes

Router primary interface state = Up
Router secondary interface state = Available
Restoral Statistics:

Primary restoral attempts =          3 completions =          1
Restoral packets forwarded =          660
Most recent restoral period in hrs:min:sec      0:04:07

WRS>list all

WAN Restoral is enabled with 1 circuit(s) configured

Total restoral attempts =          3 completions =          1
Total packets forwarded =          970

:

```

Figure 186 (Part 8 of 9). Scenario 4: 2210A Configuration via the ASCII Console

```

:
Longest completed restoral period in hrs:min:sec      0:00:00

Primary Interface      Secondary Interface      Restoral
-----
1 PPP/0 - Point to Poi 3 PPP/1 - Point to Poi      Yes

Router primary interface state = Down
Router secondary interface state = Up
Restoral Statistics:

Primary restoral attempts =      3 completions =      1
Restoral packets forwarded =      970
Most recent restoral period in hrs:min:sec      0:01:54

WRS>exit
+protocol dls      38
Data Link Switching Console
DLSw>list tcp sessions
Group      IP Address      Conn State      Pkts Sent      Pkts Rcvd      Bytes Sent      Bytes Rcvd
-----
1          9.67.46.77      ESTABLISHED      1661           214           164679          19602
DLSw>list dls sessions all
Source      Destination      State      Flags      Dest IP Addr      Id
-----
1 400030000001 04 10005A861AF3 04 CONNECTED      9.67.46.77      13
DLSw>list dls sessions det 13
Source      Destination      State      Flags      Dest IP Addr      Id
-----
0 400030000001 04 10005A861AF3 04 CONNECTED      9.67.46.77      13

Personality:      TARGET
XIDs sent:      4
XIDs rcvd:      5
Datagrams sent:      0
Datagrams rcvd:      0
Info frames sent:      34
Info frames rcvd:      44
RIF:      0E21 FFF1 FFBF 5827 581D C31C 5D10

DLSw>exit
+Ctrl+p
*
```

Figure 186 (Part 9 of 9). Scenario 4: 2210A Configuration via the ASCII Console

Notes:

- 1 Talk to the CONFIG process.
- 2 Assign the name local-site to the 2210A phone number.
- 3 Assign the name remote-site to the 2210B phone number.
- 4 Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 4.

- 5** Set the data-link of interface 4 to PPP.
- 6** List the ISDN address.
- 7** List the devices configuration. Interface 1 is the primary PPP link, interface 3 is the physical ISDN link and interface 4 is the logical dial-circuit with PPP encapsulation method.
- 8** Customization of network 0. This is the token-ring interface. Specify that the unshielded media connector (UTP) is used and enter the locally administered address for this interface.
- 9** Customization of network 1. This is the serial 1 interface. Specify that the V.35 DTE cable is used.
- 10** Customization of network 3. This is the ISDN interface.
- 11** List the interface 3 configuration.
- 12** Assign the phone number to the 2210 using the name defined earlier.
- 13** Set the switch type.
- 14** If you set the switch-variant to NET3, VN3, DMS250 or AUS, set the directory number of the local port. Set the network dial address (telephone number) of the local port.
- 15** Set the number of retries for a call in case of no answer.
- 16** Set the number of seconds to wait before a retry.
- 17** List the ISDN configuration.
- 18** Customization of network 4. This is the logical dial-circuit.
- 19** List the interface 4 configuration.
- 20** Set the physical network number on which the calls will be actually performed.
- 21** Allow the outbound calls only. Therefore, in the case of primary PPP link failure, the calls will be done from this 2210.
- 22** Set the idle timer to 0. This will cause the switched connection to stay up even if there is no packet to be sent.
- 23** Set the destination phone number using the name defined earlier.
- 24** List the circuit configuration.
- 25** Access the link layer protocol that is running on this dial-circuit. The encapsulation method is PPP in this scenario.
- 26** List the PPP link parameters. Defaults are used in this scenario.
- 27** Access the WAN Restoral (WRS) feature configuration.

- 28** Match the secondary dial circuit (interface 4) with the primary PPP leased link (interface 1).
- 29** Enable the WAN Restoral feature.
- 40** Enable the secondary circuit.
- 31** List the WAN Restoral feature configuration.
- 32** Customization of the IP protocol. Assign an IP address to the token-ring and the PPP link. Also, assign the internal IP address and enable RIP. No IP address must be assigned to the V.25bis interface or the dial-circuit interface. When a backup line is established, the dial-circuit assumes all the characteristics of the protocols customized for the primary PPP link.
- 33** Customization of the bridging function. Customize source route bridging on the token-ring interface. Assign bridge number and token-ring LAN segment number. Enable bridging and DLSw at the box level. This bridging configuration is required for the DLSw.
- 34** Customization of the DLSw protocol. Enable DLSw, and set the virtual segment number corresponding to the IP network. Add the IP address of the remote TCP neighbor, and open SAP 00 and 04 for DLSw.
- 35** Restart the 2210A to get the configuration running.
- 36** Talk to gateway operator console for monitoring.
- 37** Access the WAN Restoral feature (WRS) monitoring. First, list the WAN Restoral feature monitoring when the primary PPP link is down and the secondary switched link is up. Then, list the WAN Restoral feature monitoring when the primary PPP link has returned and the secondary switched link has been dropped.
- 38** Access the DLSw protocol monitoring. List the TCP connection and the SNA/DLSw sessions.

```

*
*talk 6 1

Config>add isdn
Assign address name [1-23] chars []? local-site 2
Assign network dial address [1-25 digits] []? 8-352-2186 2
Assign network subdial address [0-20 digits] []? 2
Config>add isdn
Assign address name [1-23] chars []? remote-site 3
Assign network dial address [1-25 digits] []? 8-352-2184 3
Assign network subdial address [0-20 digits] []? 3
Config>add device dial-circuit 4
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Config>set data-link ppp 4 5
Config>list isdn-address 6

Address assigned name      Network Address
-----
local-site                 8-352-2186
remote-site                8-352-2184
Config>list devices 7
Ifc 0   Token Ring                CSR 6000000, vector 28
Ifc 1   WAN PPP                   CSR 81620, CSR2 80D00, vector 93
Ifc 2   WAN PPP                   CSR 81640, CSR2 80E00, vector 92
Ifc 3   ISDN Basic                CSR 0, vector 0
Ifc 4   PPP Dial Circuit           CSR 0, vector 0
Config>network 0 8
Ethernet interface configuration
ETH config>list
Connector type:             AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:          ETHER

ETH config>exit
Config>network 1 9
Point-to-Point user configuration
PPP Config>set hdlc cable v35 dte
PPP Config>list all

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):    No   Addr/Cntl Field Comp(ACFC): No

:

```

Figure 187 (Part 1 of 8). Scenario 4: 2210B Configuration via the ASCII Console

```

:
Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:      3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit
Config>network 3           10
ISDN Data Link Configuration
ISDN Config>list           11
    ISDN Configuration

Local Network Address Name      = Unassigned
Local Network Address:Subaddress = Unassigned

Maximum frame size in bytes     = 2048
Outbound call address Timeout   = 180 Retries = 2
Switch Variant                  = Net 3
Multipoint Selection            = Point-to-Point
TEI                             = Automatic
PS1 detect                      = Disabled
No circuit address accounting information being kept
ISDN Config>set local-address-name
Assign local address name []? local-site 12
ISDN Config>set switch
Switch-Variant-Model [NET3]? net3 13
ISDN Config>set dn0
Enter DNO (Directory-Number-0) []? 8-352-2186 14
ISDN Config>set retries-call-address 5 15
ISDN Config>set timeout-call-address 60 16

:

```

Figure 187 (Part 2 of 8). Scenario 4: 2210B Configuration via the ASCII Console

```

:
ISDN Config>list 17
    ISDN Configuration

Local Network Address Name      = local-site
Local Network Address:Subaddress = 8-352-2186:

Maximum frame size in bytes     = 2048
Outbound call address Timeout   = 60 Retries = 5
Switch Variant                  = Net 3
DNO (Directory Number 0)       = 8-352-2186
Multipoint Selection            = Point-to-Point
TEI                             = Automatic
PS1 detect                      = Disabled
No circuit address accounting information being kept
ISDN Config>exit
Config>network 4 18
Circuit configuration
Circuit Config: 4>list 19

Base net                        = 0
Destination name                =
Circuit priority                = 8

Outbound calls                  = allowed
Idle timer                     = 60 sec
SelfTest Delay Timer           = 150 ms

Circuit Config: 4>set net 3 20
Circuit Config: 4>set calls inbound 21
Circuit Config: 4>set idle
Idle timer (seconds, 0 means always active) [60]? 0 22
Circuit Config: 4>set destination remote-site 23
Circuit Config: 4>set any_inbound 24
Circuit Config: 4>list 25

Base net                        = 3
Destination name                = remote-site
Circuit priority                = 8

Inbound calls                   = allowed
Inbound dst name                = * ANY *
Idle timer                     = 0 (fixed circuit)
SelfTest Delay Timer           = 150 ms

Circuit Config: 4>encapsulator 26
Point-to-Point user configuration
PPP Config>list all 27

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:            3000

:

```

Figure 187 (Part 3 of 8). Scenario 4: 2210B Configuration via the ASCII Console

```

:

LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:   A0000
Protocol Field Comp(PFC):   No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20     CONFIG Nak Tries:      10
Terminate Tries:          10     Retry Timer:            3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit
Circuit Config: 4>exit
Config>feature wrs        28
Feature name or number [WAN Restoral System]?
WAN Restoral user configuration
WRS Config>add secondary-circuit 4 1    29
WRS Config>enable wrs                30
WRS Config>enable secondary-circuit    31
Secondary interface number [0]? 4
WRS Config>list all                32

WAN Restoral is enabled.
Default Stabilization Time:      0 seconds
Default First Stabilization Time: 0 seconds

:

```

Figure 187 (Part 4 of 8). Scenario 4: 2210B Configuration via the ASCII Console


```

:

```

Primary Interface	Secondary Interface	Secondary Enabled
1 - WAN PPP	4 - PPP Dial Circuit	Yes

```

[No Primary-Alternate pairs defined]
WRS Config>exit
Config>protocol ip 33
Internet protocol user configuration
IP config>add address 0 9.67.46.77 255.255.255.240
IP config>add address 1 9.67.46.131 255.255.255.240
IP config>set internal IP address 9.67.46.77
IP config>enable rip
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.77      255.255.255.240  Network broadcast,    fill 0
  intf 1  9.67.46.131    255.255.255.240  Network broadcast,    fill 0
  intf 2                                IP disabled on this interface
  intf 3                                IP disabled on this interface
Internal IP address: 9.67.46.77

Routing
Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
    intf 0  9.67.46.77      Send net and subnet routes
    intf 1  9.67.46.131    Send net and subnet routes
    intf 2                                IP & RIP are disabled on this interface
    intf 3                                IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

EGP: disabled

IP config>exit
Config>protocol asrt 34
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>enable dls
:

```

Figure 187 (Part 5 of 8). Scenario 4: 2210B Configuration via the ASCII Console

```

:
ASRT config>list bridge

Source Routing Transparent Bridge Configuration
=====

Bridge: Enabled Bridge Behavior: STB
+-----+
-----] SOURCE ROUTING INFORMATION ]-----
+-----+

Bridge Number: N/A Segments: 0
Max ARE Hop Cnt: 00 Max STE Hop cnt: 00
1:N SRB: Not Active Internal Segment: 0x000
LF-bit interpret: Extended
+-----+
-----] SR-TB INFORMATION ]-----
+-----+

SR-TB Conversion: Disabled
TB-Virtual Segment: 0x000 MTU of TB-Domain: 0
+-----+
-----] SPANNING TREE PROTOCOL INFORMATION ]-----
+-----+

Bridge Address: Default Bridge Priority: 32768/0x8000
STP Participation: IEEE802.1d
+-----+
-----] TRANSLATION INFORMATION ]-----
+-----+

FA<=>GA Conversion: Enabled UB-Encapsulation: Disabled
DLS for the bridge: Enabled
+-----+
-----] PORT INFORMATION ]-----
+-----+

Number of ports added: 2
Port: 1 Interface: 0 Behavior: STB Only STP: Enabled
Port: 2 Interface: 1 Behavior: STB Only STP: Enabled

ASRT config>exit
Config>protocol dls 35
DLSw protocol user configuration
DLSw config>enable dls
DLSw config>set srb fff
DLSw config>list dls
DLSw is ENABLED
LLC2 send Disconnect is ENABLED

:

```

Figure 187 (Part 6 of 8). Scenario 4: 2210B Configuration via the ASCII Console

```

:
SRB Segment number          FFF
Max DLSw sessions           1000
DLSw global memory allotment 153344
LLC per-session memory allotment 8192
SDLC per-session memory allotment 4096

                                No MAC Address set

Database age timer           1200 seconds
Age timer resolution         300 seconds
Max wait timer for ICANREACH 20 seconds
Wait timer for LLC test response 15 seconds
Wait timer for SDLC test response 15 seconds
Join Group Interval          900 seconds
DLSw config>add tcp 9.67.46.146
Transmit Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive?(E/D)- [D]? E
DLSw config>list tcp
Neighbor      Xmit Bufsize  Max Segsize  Keepalive
9.67.46.146   5120          1024         ENABLED
DLSw config>open-sap 0 00
DLSw config>open-sap 0 04
DLSw config>list open
Interface  SAP
0          0
0          4
DLSw config>exit
Config>Ctrl+p
*restart 36
Are you sure you want to restart the gateway? (Yes or [No]): Yes

```

```

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

```

```

MOS Operator Control

```

```

*
*talk 5 37

```

```

+protocol dls 38
Data Link Switching Console

```

```

:

```

Figure 187 (Part 7 of 8). Scenario 4: 2210B Configuration via the ASCII Console

```

:
DLSw>list tcp sessions
  Group      IP Address      Conn State  Pkts Sent  Pkts Rcvd  Bytes Sent  Bytes Rcvd
-----
1           9.67.46.146  ESTABLISHED      188      1606      19579      159423
DLSw>list dls sessions all
      Source      Destination      State      Flags      Dest IP Addr      Id
-----
1 10005A861AF3 04 400030000001 04 CONNECTED      9.67.46.146      487
DLSw>list dls sessions det 487
      Source      Destination
State      Flags      Dest IP Addr      Id
-----
0 10005A861AF3 04 400030000001 04 CONNECTED      9.67.46.146      487

  Personality:    ORIGINATOR
  XIDs sent:      5
  XIDs rcvd:      4
  Datagrams sent: 0
  Datagrams rcvd: 0
  Info frames sent: 44
  Info frames rcvd: 34
  RIF:
DLSw>exit
+Ctrl+p
*
```

Figure 187 (Part 8 of 8). Scenario 4: 2210B Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Assign the name local-site to the 2210B phone number.
- 3** Assign the name remote-site to the 2210A phone number.
- 4** Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 4.
- 5** Set the data-link of interface 4 to PPP.
- 6** List the ISDN address.
- 7** List the devices configuration. Interface 1 is the primary PPP link, interface 3 is the physical ISDN link and interface 4 is the logical dial-circuit with the PPP encapsulation method.
- 8** Customization of network 0. List the Ethernet interface. There is nothing to change.
- 9** Customization of network 1. This is the serial 1 interface. Specify that a V.35 DTE cable is used.
- 10** Customization of network 3. This is the ISDN interface.

- 11** List the interface 3 configuration.
- 12** Assign the phone number to the 2210 using the name defined earlier.
- 13** Set the switch type.
- 14** If you set the switch-variant to NET3, VN3, DMS250 or AUS, set the directory number of the local port. Set the network dial address (telephone number) of the local port.
- 15** Set the number of retries for a call in case of no answer.
- 16** Set the number of seconds to wait before a retry.
- 17** List the ISDN configuration.
- 18** Customization of network 4. This is the logical dial-circuit.
- 19** List the interface 4 configuration.
- 20** Set the physical network number on which the calls will be actually performed.
- 21** Allow the inbound calls only. Therefore, in case of a primary PPP link failure, 2210B will wait for the call from 2210A.
- 22** Set the idle timer to 0. The switched connection will stay up even if there are no packets to send.
- 23** Set the destination phone number using the name defined earlier.
- 24** Accept any inbound calls.
- 25** List the circuit configuration.
- 26** Access the link layer protocol that is running on the dial-circuit.
- 27** List the PPP link parameters. Defaults are used in this scenario.
- 28** Access the WAN Restoral (WRS) feature configuration.
- 29** Match the secondary dial-circuit (interface 4) with the primary PPP leased link (interface 1).
- 30** Enable the WAN Restoral feature.
- 31** Enable the secondary-circuit.
- 32** List the WAN Restoral feature configuration.
- 33** Customization of the IP protocol. Assign IP address to the Ethernet and the PPP link. Also, assign the internal IP address and enable RIP. The IP address for the serial interfaces must be added only to the primary interface. No IP address must be assigned to the V.25bis interface or the dial-circuit interface. When a backup line is established, it assumes all the characteristics of the primary PPP link.

34 Customization of the bridging function. Transparent bridging is already enabled by default for the Ethernet interface. Enable bridge and DLSw at the box level. This bridging configuration is required because of the requirements of DLSw.

35 Customization of the DLSw protocol. Enable DLSw and set the virtual segment number corresponding to the IP network. Add the IP address of the remote TCP neighbor, and open SAP 00 and 04 for DLSw.

36 Restart the 2210B to get the configuration running.

37 Talk to gateway operator console for monitoring.

38 Access the DLSw protocol monitoring. List the TCP connection and the SNA/DLSw sessions.

11.6 WAN Reroute Feature

This section describes the WAN Reroute function implemented in the IBM 2210. The WAN Reroute function provides the possibility to route the traffic, at a predefined link, when the normal leased line fails.

This subchapter includes the following sections.

- WAN Reroute implementation in the IBM 2210
- WAN Reroute configuring commands
- WAN Reroute scenarios and configuration

11.7 WAN Reroute Implementation in the IBM 2210

The WAN Reroute function is an enhancement to the IBM 2210 Multiprotocol Routing Services (MRS) software. It allows the activation of an alternate network interface when a primary interface fails. WAN Reroute is more flexible than the standard WAN Restoral feature (WRS) currently provided because the alternate link may have a different termination point other than the primary link. It uses the dynamic routing abilities of the different routing protocols (IP RIP, IP OSPF, IPX RIP, etc.) or bridging protocols to find alternate paths through the two new network topologies.

WAN Reroute is not a new MRS feature. It constitutes enhancements to the following functional areas:

- WAN Restoral feature
- Frame relay support
- Dial Circuit support

To support WAN Reroute, WRS can now be configured for the type of backup to be performed when the primary link fails.

Prior to WAN Reroute, the user specified a secondary interface (dial circuit) to use when the primary interface failed. The primary interface had to be configured to use the Point-to-Point Protocol (PPP) as the network layer protocol. When the primary interface failed, the entire PPP configuration for the primary interface was moved to the secondary interface. Both ends of the primary PPP link were configured for WRS with one end of the dial circuit configured to initiate a backup call and the other end configured to accept a backup call.

A new stabilization period configuration parameter has also been added. It allows the user to specify the amount of time a reactivated primary interface must be up before its associated secondary or alternate interface is deactivated. This configuration option is useful when PPP links and frame relay PVCs are oscillating between an active and inactive state.

11.8 Frame Relay Enhancements

Frame relay Permanent Virtual Circuits (PVCs) now have a new *required* attribute, which indicates that the PVC must be active for the interface to be considered up. When the interface is first enabled, it will not be reported as up to the protocols configured for it until all required PVCs are active. If a required PVC is reported as inactive by LMI while the interface is up, the interface will be reported as down.

Frame relay interfaces have a new option to control the status of the interface when there are no active PVCs. When this option is selected, the interface will be reported as down when there are no active PVCs on the interface.

When is a primary interface up or down?

The up or down state of a serial interface can be influenced by several factors. The first factor is the physical state on the interface with respect to modem signals. An interface is either enabled or disabled based on these signals:

Cable type	Signals required for enabled interface
=====	=====
X.21	Indication
V.35	CTS, DSR, DCD
V.36	CTS, DSR, DCD
RS232/V.24	CTS, DSR, DCD

The IBM 2210 continuously monitors the modem signals. When it detects the fact that at least one of the required signals is not present, it gives the interface 5 seconds to recover. If all of the required signals are not present within 5 seconds, the interface is considered disabled. Once an interface is disabled, a link self-test is attempted after a 5-second lapse. If the self-test fails, another is attempted 5-seconds later. If the self-test completes, the interface is enabled. An interface must be enabled before it can be up.

A serial interface configured for PPP is up when the physical interface is enabled and the PPP Link Control Protocol (LCP) has placed the link in opened state. Prior to the opened state, the interface is down.

The state of frame relay interfaces may be influenced by the Frame Relay Local Management Interface (LMI). If LMI is disabled for the interface, the state of the interface is determined by its physical state: up if it is enabled and down if it is not. If LMI is enabled, it will determine the state of the interface.

Before LMI reports the interface as up, it must be able to successfully send and receive management packets on that interface. LMI uses two parameters, N2 and N3, to determine if it is successful. N2 is the error threshold for management events and N3 is the number of events that are monitored in the event window. If there are N2 management errors in N3 management events, the interface is considered down. The values used for N2 and N3 are configurable and default to 3 and 4, respectively.

Once LMI has verified that it can send and receive management packets, the state of the interface may also be influenced by the state of its PVCs. There is a new configuration option that allows the user to have the interface reported as

down when there are no active PVCs on that interface. The user may also configure PVCs as required. If a required PVC is not active, the interface will be down.

For a frame relay interface enabled for LMI to be up, the following conditions must be met:

1. There must be less than N2 errors in N3 LMI events.
2. If active PVCs are monitored, there must be at least one active PVC.
3. If required PVCs are configured, at least one of them must be active.

A final factor that can influence that state of an interface is an optionally configured stabilization period. This is the amount of time that a previously down interface must be up before the WAN Restoral function is informed of the fact that it is up. This configuration option is useful when PPP links and frame relay PVCs are oscillating between an active and inactive state.

11.9 WAN Reroute Commands

All the WAN Reroute commands can be found under the WAN Restoral feature.

<i>Table 75. Process Description</i>	
Command	Function
?(help)	Lists the commands or actions associated with the specific command
Enable	Enables the alternate or secondary circuit or WRS
Disable	Disables the alternate or secondary circuit or WRS
List	Lists the WRS configuration
ADD	Adds alternate and secondary circuits
REMOVE	Removes alternate secondary circuits
SET	Sets the stabilizations periods
EXIT	Returns to previous prompt

11.9.1 Scenario 5: WAN Reroute Implementation

2210A and 2210B are configured for IP and DLSw and have the DLC partner and the internal 2210 address of the token-ring side. 2210C is only configured as an IP router. The routing protocol used is RIP.

In this scenario the three 2210s are connected with PPP links and 2210A is the hub router. At the 2210B token-ring side there is a workstation running SNA and using DLSw to connect to a 3745 connected at the 2210A ring. Link D is the primary link and link E is the alternate (backup link) for the link E. 2210C is configured as a normal V.25bis circuit; it cannot be an alternate link as it is in 2210B.

At the same time trying to have the Link F as primary and Link E as alternate in 2210C will result in an invalid configuration. An alternate link will not answer to an incoming call. If Link F must have backup as primary, a new alternate link must be defined.

The scenario for this configuration is when link D breaks (the connection). 2210B will wait for X seconds (X=50 in our scenario); if the link is still down, 2210B will call 2210C and set up the backup link configured for WAN Reroute. The traffic will then flow from 2210B over link E to 2210C and up to 2210A.

If you have a routing protocol that sends routing updates, you will need to disable the dial circuits or make it a DOD (Dial-on-Demand) circuit. The routing protocol will establish connection each time an update is sent and this will be avoided when the dial circuit is disabled.

The feature will keep monitoring the broken link. When the primary link is OK, the alternate link will drop and the traffic will flow over the primary link. All these events take place without losing the current session.

When running DLSw you should not have the serial link (the one defined as primary link) as the internal address and DLSw partner. If the modem fails, the IP address at that interface will also disappear, which means that the TCP connection cannot be set up and no SNA NB traffic can flow. In this case the token-ring IP addresses are the internal and DLSw partner addresses.

One configuration was made with frame relay instead of the PPP link between 2210A and 2210B.

To have the IBM 7855 modem work as expected, we only did a factory reset, that is, we returned the modem to its factory setup. This can be accomplished by referring to page 4-4 of the *IBM 7855 Guide to Operation*, GA33-0160-01.

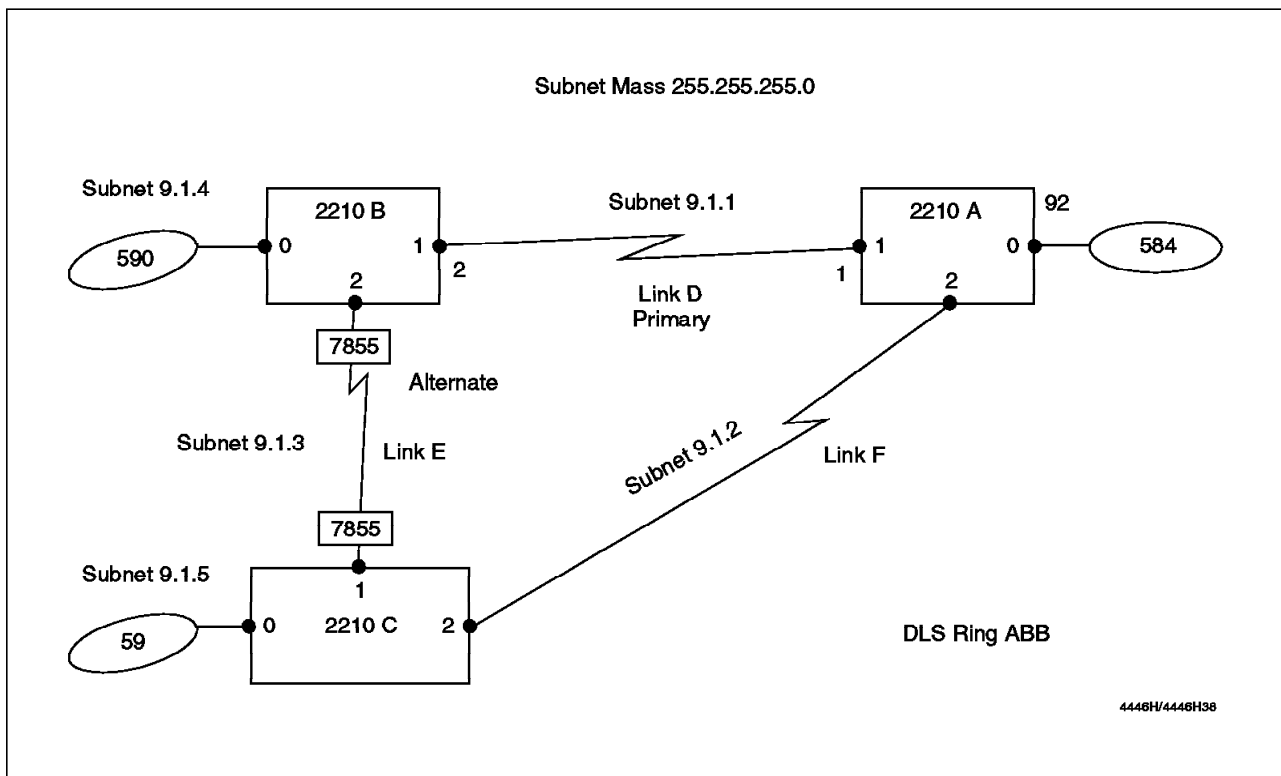


Figure 188. Scenario 5: WAN Reroute

```

*talk 6
Config>add v25-bis-address
Assign address name [1-23] chars []? remote
Assign network dial address [1-30 digits] []? 13440
Config>add v25-bis-address
Assign address name [1-23] chars []? local
Assign network dial address [1-30 digits] []? 13435
Config>list v25-bis-address

Address assigned name      Network Address
-----
local                      13435  1
remote                    13440

Config>set data-link v25bis
Interface Number [0]? 2
Config>add device dial-circuit
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters  2
Config>network 2
V.25bis Data Link Configuration
V25bis Config>set local-address-name
Local network address name [] ? local
V25bis Config>set timeout
Timeout-no-answer (0-65535 Seconds, 0 means no timeout) [0]? 30
V25bis Config>list
    V.25bis Configuration
Local Network Address Name   = local
Local Network Address        = 13435

Non-Responding addresses:
Retries                      = 1
Timeout                      = 30 seconds

Call timeouts:
Command Delay                = 0 ms
Connect                      = 60 seconds
Disconnect                   = 2 seconds

Cable type                   = RS-232 DTE
V25bis Config>exit
Config>network 3
Circuit configuration
Circuit Config>set net
Base net for this circuit [0]? 2
Circuit Config>set destination
Assign destination address name ? remote
Circuit Config>set idle 20
Circuit Config>encapsulator
Point-to-Point user configuration

:

```

Figure 189 (Part 1 of 4). Scenario 5: WAN Reroute and the V.25bis Configuration at 2210B

```

:
PPP Config>list all      22

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):    No   Addr/Cntl Field Comp(ACFC):    No

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit
Config>protocol
Protocol name or number [IP]? IP
Internet protocol user configuration
IP config>add address
Which net is this address for [0]? 3  3
New address [0.0.0.0]? 9.1.3.1
Address mask [255.0.0.0]? 255.255.255.0
IP config>exit
Config>disable interface  4
Interface number [0]? 3

:

```

Figure 189 (Part 2 of 4). Scenario 5: WAN Reroute and the V.25bis Configuration at 2210B

```

:
Config>feature wrs
WAN Restoral user configuration
WRS Config>add alternate-circuit
Alternate interface number [0]? 3 5
Primary interface number [0]? 1
WRS Config>set first-stab 6
Primary interface number [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default) [- 1]? 40
WRS Config>set stab stab 6
Primary interface number [0]? 1
Primary stabilization time (0 - 3600 seconds, -1 = default) [-1]? 40
WRS Config>set default first-stab 6
Default first primary stabilization time (0 - 3600 seconds) [20]? 50
WRS Config>list

WAN Restoral is DISABLED.
Default Stabilization Time: 0 seconds
Default First Stabilization Time: 50 seconds

No Primary-Secondary pairs defined

```

Primary Interface	Alternate Interface	Alternate Enabled	1st Stab	Subseq Stab
1 - WAN PPP	3 - PPP Dial Circuit	No	40	40

```

WRS Config>enable alternate 7
Alternate interface number [0]? 3
WRS Config>list

WAN Restoral is DISABLED. 8
Default Stabilization Time: 0 seconds
Default First Stabilization Time: 50 seconds

[No Primary-Secondary pairs defined]

```

Primary Interface	Alternate Interface	Alternate Enabled	1st Stab	Subseq Stab
1 - WAN PPP	3 - PPP Dial Circuit	Yes	40	40

```

WRS Config>enable wrs 8
WRS Config>list

WAN Restoral is enabled.
Default Stabilization Time: 0 seconds
Default First Stabilization Time: 50 seconds

No Primary-Secondary pairs defined

```

Primary Interface	Alternate Interface	Alternate Enabled	1st Stab	Subseq Stab
1 - WAN PPP	3 - PPP Dial Circuit	Yes	40	40

```

WRS Config>exit
:

```

Figure 189 (Part 3 of 4). Scenario 5: WAN Reroute and the V.25bis Configuration at 2210B

```

:
Config>Ctrl+p
*restart
Are you sure you want to restart the gateway? (Yes or No): yes

Copyright Notices:
Copyright 1985-1995 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 189 (Part 4 of 4). Scenario 5: WAN Reroute and the V.25bis Configuration at 2210B

- 1** The V.25bis must have telephone numbers configured for both local and remote sides.
- 2** The interface number depends on how many interfaces this box supports; the dial-circuits starts after the interface numbering.
- 3** Add the IP address to the dial-circuit, not to the V.25bis interface.
- 4** Disabling the dial-circuit means that the routing protocol cannot send any updates and the link is only used as a WAN Reroute link.
- 5** The only specification needed for WAN Reroute is to tell which link is the primary (Link D) and which is the alternate link (Link E). In this case, the alternate link is number 3, which is the dial-circuit.
- 6** Set the default first stabilization period means that all defined primary links will have the same stabilization period. The set first stabilization period is for a specific interface and overrides the default setting. The set stabilization period means that you set the subsequent stabilization time for a specific interface and default stabilization time means that you set stabilization on all the primary interfaces.
- 7** The alternate interface must be enabled
- 8** The feature WRS must be enabled.

The same V.25bis configuration was applied to 2210C, but with a different IP address and local/remote telephone numbers were swapped. The WAN Reroute configuration should not be applied.

11.9.2 Scenario 6: WAN Reroute Implementation Using ISDN

2210A and 2210B are configured for IP and DLSw and have the DLC partner and the internal 2210 address of the token-ring side. 2210C is only configured as an IP router. The routing protocol used is RIP.

In this scenario the three 2210s are connected with PPP links and the 2210A is the hub router. At the 2210B token-ring side there is a workstation running SNA,

using DLSw to connect to a 3745 connected at the 2210A ring. Link D is the primary link and Link E is the alternate (backup link) for Link E. The 2210C is configured as a normal V.25bis circuit; it cannot be an alternate link as it is in the 2210B.

At the same time trying to have Link F as primary and Link E as alternate in 2210C will result in an invalid configuration. An alternate link will not answer to an incoming call. If Link F must have backup as primary, a new alternate link must be defined.

The scenario for this configuration is when Link D breaks the connection 2210B will wait for X seconds (X=50 in our scenario). If the link is still down, 2210B will call 2210C and set up the backup link configured for WAN Reroute. The traffic will then flow from 2210B over Link E to 2210C and up to 2210A.

If you have a routing protocol that sends routing updates, you will need to disable the dial-circuits or make it a DOD (Dial-On-Demand) circuit. The routing protocol will establish connection each time an update is sent and this will be avoided when the dial-circuit is disabled.

The feature will keep monitoring the broken link. When the primary link is OK, the alternate link will drop and the traffic will flow over the primary link. All of these events take place without losing the current session.

When running DLSw you should not have the serial link (the one defined as primary link) as the internal address and DLSw partner. If the modem fails, the IP address at that interface will also disappear, which means that the TCP connection cannot be set up and no SNA NB traffic can flow. In this case the token-ring IP addresses are the internal and DLSw partner addresses.

One configuration was made with frame relay instead of the PPP link between the 2210A and 2210B.

To have the IBM 7855 modem working as expected we only did a factory reset, that is, we returned the modem to its factory setup. This can be accomplished by referring to page 4-4 of the *IBM 7855 Guide to Operation*, GA33-0160-01.

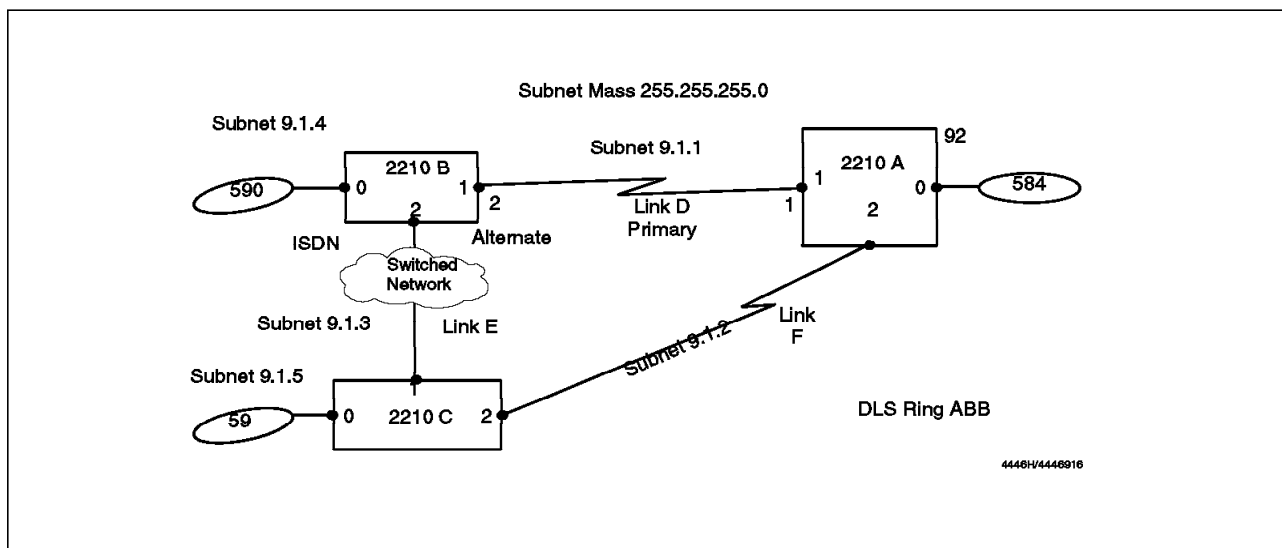


Figure 190. Scenario 6: WAN Reroute Using ISDN

```

*talk 6 1
Config>add isdn
Assign address name [1-23] chars []? local 2
Assign network dial address [1-25 digits] []? 13435 2
Assign network subdial address [0-20 digits] []? 2
Config>add isdn
Assign address name [1-23] chars []? remote 3
Assign network dial address [1-25 digits] []? 13440 3
Assign network subdial address [0-20 digits] []? 3
Config>add device dial-circuit 4
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Config>set data-link ppp
Interface Number [0]? 4 5
Config>list isdn-address 6

Address assigned name      Network Address  Network Subaddress
-----
local                      13435
remote                    13440

Config>network 3 7
ISDN user configuration
ISDN Config>list 8
ISDN Configuration

Local Network Address Name      = Unassigned
Local Network Address:Subaddress = Unassigned

Maximum frame size in bytes      = 2048
Outbound call address Timeout    = 180 Retries = 2
Switch Variant                   = NET 3
Multipoint Selection = Point-to-Point
TEI = Automatic
PS1 detect = Disabled
No circuit address accounting information being kept
ISDN Config>set local-address-name
Assign local address name []? local 9
ISDN Config>set switch
Switch-Variant-Model [NET3]? net3 10
ISDN Config>set dn0
Enter DNO (Directory-Number-0) []? 13435 11
ISDN Config>set retries-call-address 5 12
ISDN Config>set timeout-call-address 60 13

:

```

Figure 191 (Part 1 of 4). Scenario 6: WAN Reroute and the ISDN Configuration at 2210B


```

:
ISDN Config>list 14
ISDN Configuration

Local Network Address Name      = local-site
Local Network Address:Subaddress = 13435:

Maximum frame size in bytes     = 2048
Outbound call address Timeout   = 60 Retries = 5
Switch Variant                  = NET 3
DNO (Directory Number 0)       = 13435
Multipoint Selection = Point-to-Point
TEI = Automatic
PS1 detect = Disabled
No circuit address accounting information being kept
ISDN Config>exit
Config>network 4 15
Circuit configuration
Circuit config: 4>list 16

Base net                        = 0
Destination name                =
Circuit priority                = 8

Outbound calls                  = allowed
Idle timer                      = 60 sec
SelfTest Delay Timer            = 150 ms

Circuit Config: 4>set net
Base net for this circuit [0]? 3 17
Circuit Config: 4>set calls outbound 18
Circuit Config: 4>set idle 0 19
Circuit Config: 4>set destination
Assign destination address name ? remote 20
Circuit Config: 4>list 21

Base net                        = 3
Destination name                = remote
Circuit priority                = 8

Outbound calls                  = allowed
Idle timer                      = 0 (fixed circuit)
SelfTest Delay Timer            = 150 ms

Circuit Config: 4>encapsulator 22
Point-to-Point user configuration
PPP Config>list all 23

LCP Parameters
-----
CONFIG Request Tries:           20   CONFIG Nak Tries:           10
Terminate Tries:                10   Retry Timer:              3000

:

```

Figure 191 (Part 2 of 4). Scenario 6: WAN Reroute and the ISDN Configuration at 2210B

```

:
LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:   A0000
Protocol Field Comp(PFC):   No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20    CONFIG Nak Tries:      10
Terminate Tries:          10    Retry Timer:           3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit
Circuit config: 4>exit
Config>feature wrs        24
WAN Restoral user configuration
WRS Config>add alternate-circuit
Alternate interface number [0]? 4    25
Primary interface number [0]? 1    25
Changing alternate interface for primary 1
WRS Config>set first-stabilization 26
Primary interface number [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default) [- 1]? 40
WRS Config>set stabilization      26
Primary interface number [0]? 1
Primary stabilization time (0 - 3600 seconds, -1 = default) [-1]? 40
WRS Config>set default first-stabilization 26
Default first primary stabilization time (0 - 3600 seconds) [20]? 50
WRS Config>enable alternate      27
Alternate interface number [0]? 3

:

```

Figure 191 (Part 3 of 4). Scenario 6: WAN Reroute and the ISDN Configuration at 2210B

```

:
WRS Config>enable wrs      28
WRS Config>list            29

WAN Restoral is enabled.
Default Stabilization Time:      0 seconds
Default First Stabilization Time: 50 seconds

[No Primary-Secondary pairs defined]

Primary Interface  Alternate Interface  Alt.   1st  Subseq TOD Revert Back
Enabled  Stab  Stab  Start  Stop
-----
1 - WAN PPP      4 - PPP Dial Circuit  Yes    40   40   Not Set  Not Set

WRS Config>exit
Config>protocol
Protocol name or number [IP]? IP      30
Internet protocol user configuration
IP config>add address
Which net is this address for [0]? 3
New address [0.0.0.0]? 9.1.3.1
Address mask [255.0.0.0]? 255.255.255.0
IP config>exit
Config>disable interface
Interface number [0]? 4              31
Config>Ctrl+p
*restart      32
Are you sure you want to restart the gateway? (Yes or No): yes

Copyright Notices:
Copyright 1985-1995 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 191 (Part 4 of 4). Scenario 6: WAN Reroute and the ISDN Configuration at 2210B

- 1 Talk to the CONFIG process.
- 2 Assign the name *local* to the 2210B phone number.
- 3 Assign the name *remote* to the 2210C phone number.
- 4 Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 4. The interface number depends on how many interfaces this box supports; the dial-circuits start after the interface numbering.
- 5 Set the data-link of interface 4 to PPP.
- 6 List the ISDN address.

- 7** Customization of network 3. This is the ISDN interface.
- 8** List the interface 3 configuration.
- 9** Assign the phone number to the 2210 using the name defined earlier.
- 10** Set the switch type.
- 11** If you set the switch-variant to NET3, VN3, DMS250 or AUS, set the directory number of the local port. Set the network dial address (telephone number) of the local port.
- 12** Set the number of retries for a call in case of no answer.
- 13** Set the number of seconds to wait before a retry.
- 14** List the ISDN configuration.
- 15** Customization of network 4. This is the logical dial-circuit.
- 16** List the interface 4 configuration.
- 17** Set the physical network number on which the calls will be actually performed.
- 18** Allow the outbound calls only. Therefore, in case of a primary PPP link failure, the calls will be done from this 2210.
- 19** Set the idle timer to 0. This will cause the switched connection to stay up even if there is no packet to be sent.
- 20** Set the destination phone number using the name defined earlier.
- 21** List the circuit configuration.
- 22** Access the link layer protocol that is running on this dial-circuit. The encapsulation method is PPP in this scenario.
- 23** List the PPP link parameters. Defaults are used in this scenario.
- 24** Access the WAN Restoral (WRS) feature configuration.
- 25** The only needed specification for WAN Reroute is to tell which link is the primary (Link D) and which is the alternate link (Link E). In this case, the alternate link is number 4, which is the dial-circuit.
- 26** Set the default first stabilization period means that all defined primary links will have the same stabilization period. The set first stabilization period is for a specific interface and overrides the default setting. The set stabilization period means that you set the subsequent stabilization time for a specific interface and default stabilization time means that you set stabilization on all the primary interfaces.
- 27** The alternate interface must be enabled.
- 28** Enable the WAN Restoral feature.
- 29** List the WAN Restoral feature configuration.

30 Customization of the IP protocol. Assign an IP address to the token-ring and the PPP link. Also, assign the internal IP address and enable RIP. No IP address must be assigned to the V.25bis interface or the dial-circuit interface. When a backup line is established, the dial-circuit assumes all the characteristics of the protocols customized for the primary PPP link.

31 Disabling the dial-circuit means that the routing protocol cannot send any updates and the link is only used as an WAN Reroute link.

The same ISDN configuration was applied to 2210C, but with a different IP address, and local/remote telephone numbers were swapped. The WAN Reroute configuration should not be applied.

```

*
*talk 6

Config>set data-link frame-relay
Interface Number 0? 1
Config>network 1
frame relay user configuration
FR Config>add ?
PERMANENT-VIRTUAL-CIRCUIT
PROTOCOL-ADDRESS
FR Config>add permanent-Virtual-circuit
Circuit number [16]? 495
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name ? test
Is circuit required for interface operation? [N] Yes 1
FR Config>add protocol
Protocol name or number [IP]?
IP Address [0.0.0.0]? 9.1.1.1
Circuit number [16]? 495
FR Config>list all

```

Frame Relay HDLC Configuration

```

Encoding      = NRZ IDLE          = Flag
Clocking      = External
Cable type    = V.35 DCE
Line access rate bps =      0
Interface MTU in bytes =      2048
Transmit delay =      0

```

Frame Relay Configuration

```

LMI enabled = Yes LMI DLCI      = 0
LMI type    = ANSI LMI Orphans OK = Yes

Protocol broadcast = Yes Congestion monitoring = Yes
Emulate multicast = Yes CIR monitoring          = No

PVCs P1 allowed   = 64 CIR monitor adjustment = 1
Timer T1 seconds  = 10 Counter N1 increments  = 6
LMI N2 error threshold = 3 LMI N3 error threshold window = 4
MIR % of CIR      = 25 IR % Increment          = 12
IR % Decrement    = 25 DECnet length field     = no

Interface down if no PVCs = No 2

Maximum PVCs allowable = 64
Total PVCs configured  = 2

```

:

Figure 192 (Part 1 of 2). Scenario 6: WAN Reroute over Frame Relay Configuration at 2210B

```

:
      Circuit      Circuit      Circuit      CIR      Burst      Excess
      Name        Number      Type        in bps    Size       Burst
-----
test          495      *Permanent  64000    64000      0

      Frame Relay Protocol Address Translations

      Protocol Type      Protocol Address      Circuit Number
      -----
      IP                  9.1.1.1                  495
FR Config>exit
Config>Ctrl+p
*restart
Are you sure you want to restart the gateway? (Yes or No): yes

Copyright Notices:
Copyright 1985-1995 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 192 (Part 2 of 2). Scenario 6: WAN Reroute over Frame Relay Configuration at 2210B

1 This required parameter means that if this PVC is down then the primary link is down and a call at the alternate link should be initiated.

2 If all PVCs are down, the alternate link should be used.

11.9.3 Additional Configuration for 2210B and 2210C

***talk 6**

Config>**protocol**

Protocol name or number [IP]

IP config>**add route** **1**

IP destination [0.0.0.0]? **9.24.104.0**

Address mask [0.0.0.0]? **255.255.255.0**

Via gateway at [0.0.0.0]? **9.1.3.1**

Cost [1]? **3**

IP config>**list route**

route to 9.24.104.0,255.255.255.0 via 9.1.3.1, cost 3

IP config>**exit**

Config>**Ctrl+p**

***restart**

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

Copyright Notices:

Copyright 1985-1995 Proteon, Inc.

Copyright 1984-1987, 1989 by J. Noel Chiappa

Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*

Figure 193. WAN Reroute Adding a Static Route at 2210B

1 This static route is needed in 2210B since the 2210C will not send out any routes to 2210B. When the primary link fails 2210B will lose all routes and will need to know to which interface the packets should be routed.

***talk 6**

Config>**protocol**

Protocol name or number [IP]?

IP config>**disable route sending**

Set for which interface address [0.0.0.0]? **9.1.3.1**

IP config>**list protocol**

BOOTP forwarding: disabled

Directed broadcasts: enabled

ARP Subnet routing: disabled

RFC925 routing: disabled

OSPF: disabled

Per-packet-multipath: disabled

RIP: enabled

RIP default origination: disabled

Per-interface address flags:

intf 0	9.1.5.1	Send net and subnet routes
		Receive No Dynamic host routes
intf 1	9.1.2.2	Send net and subnet routes
		Receive No Dynamic host routes
intf 2		IP & RIP are disabled on this interface
intf 3	9.1.3.1	Send no routes 1
		Receive No Dynamic host routes

Accept RIP updates always for:

NONE

EGP: disabled

***restart**

Figure 194. Scenario 6: WAN Reroute Disabling Sending Route Updates 2210C

1 If sending routes were enabled on this interface (dial circuit) the dial would connect the other side each time a routing update is sent.

11.10 Dial-on-Demand

This section provides a description of the Dial-on-Demand facility. It shows the Dial-on-Demand configuration commands, and provides an example scenario of the Dial-on-Demand configuration.

11.10.1 Introduction to Dial-on-Demand

The Dial-on-Demand facility is designed for remote sites that do not need to be connected to the central site all the time, but only when there is some data to be sent.

When the IBM 2210 detects that a packet needs to be sent over the switched network to a remote IBM 2210, it automatically dials the customized phone number to establish the dial connection via the V.25bis or ISDN interface.

You could customize several phone numbers in the IBM 2210, and map each remote phone number to a specific protocol address (IP or IPX address). However, note that there can only be one connection to a remote site at any single point in time. This means that if there is already a connection to a remote

site, you cannot send any packets to another remote site. In this case, you must wait until the first connection has been terminated before trying to reach the second remote site.

To use the Dial-on-Demand facility, you must configure all the parameters of the desired protocol (IP or IPX) on the corresponding virtual dial-circuits and not on the physical V.25bis or ISDN interface.

When the IBM 2210 detects that no more packets are required to be sent over the switched interface for a certain lapse of time (idle timer), the switched line is automatically dropped and the V.25bis or ISDN interface becomes available.

Note that when you customize a serial interface as a dial interface using V.25bis modem with PPP encapsulation method, the other physical serial interface can be used for anything else at the same time. Also, both 2210s at each end of the primary serial link must be customized for Dial-on-Demand.

Note

It is recommended that you allow only one site to issue outbound calls, and the other site should allow inbound calls only. This will prevent dial collision in case both sides want to call each other at the same time. However, this is not a requirement and you can enable both sides for both Inbound and Outbound calls. In this case, you must be aware that if the IBM 2210s want to call each other at the same time, the V.25bis modems will loop with DIALING, then BUSY, then DIALING, then BUSY, etc. This will be repeated until one side decides to no longer send data to the other side. Then the switched link will be activated from the other side.

For IP routing over Dial-on-Demand, it is recommended that you customize static routes. This prevents the IBM 2210 from establishing the connection for each routing table update which is sent by the dynamic routing protocols.

If there is DLSw customization over a Dial-on-Demand circuit, be sure to not enable the Keepalives parameter. Enabling this parameter to verify that the remote DLSw partner is alive, by sending the keep-alive messages to them, would result in the dial-up connection to remain active permanently.

IPX does not provide static routing. Therefore, you are advised to specify large RIP and SAP update intervals to ensure that the Dial-on-Demand circuits are not frequently established as a result of the frequent RIP and SAP messages in an IPX environment. If you are using IPX, configure it for low-frequency updates or change updates so that it sends broadcast message at specified intervals, when there is data to send, or if there is a problem. You should also enable IPX Keepalive filtering, which prevents keepalive and serialization packets from continually activating a dial-on-demand link.

Note

Dial-on-Demand cannot be used to provide additional bandwidth over a switched serial interface in case of over-utilization of the bandwidth of a primary leased serial interface.

The Dial-on-Demand facility is only supported over the following:

- TCP/IP (including DLSw and Tunnel Bridge)

- IPX protocol

Note

Dial-on-Demand is not supported for any bridging methods, except for the tunnel bridge method, which is actually using IP protocol over the serial links.

The Dial-on-Demand is supported over a switched V.25bis PPP serial link, an ISDN PPP link and a frame relay link over ISDN. For more information about the V.25bis serial interface, see 3.4.23, "The V.25bis Network Interface" on page 96.

Figure 195 shows you a typical drawing of a Dial-on-Demand network.

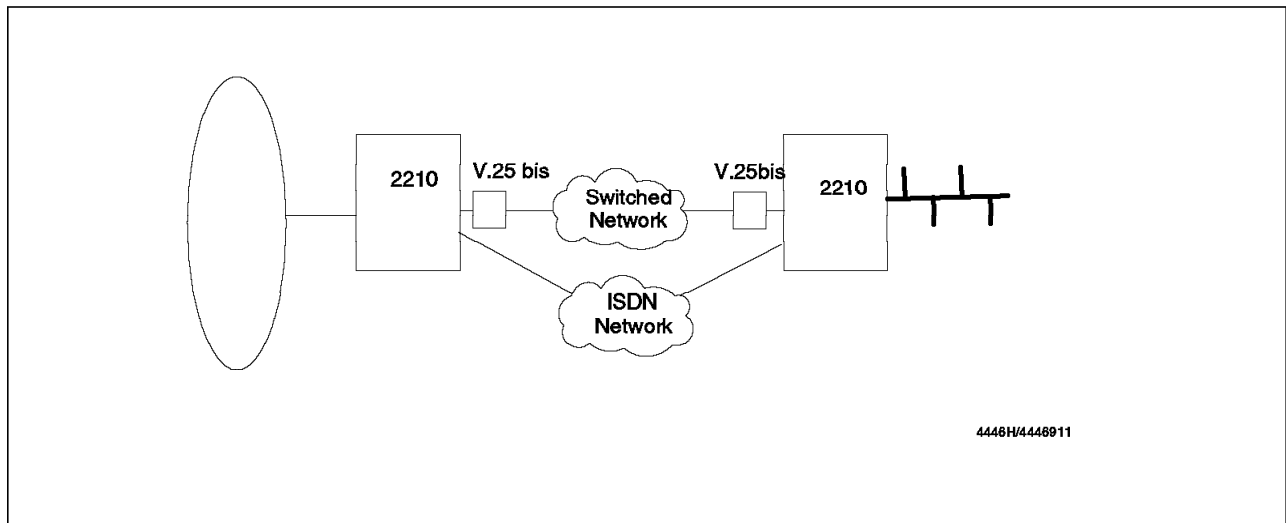


Figure 195. Typical Implementation of Dial-on-Demand

11.10.2 Dial-on-Demand Configuration Commands

This section summarizes the configuration commands needed to customize Dial-on-Demand using the CONFIG process of the Nways MRS.

Note

The Dial-on-Demand configuration with the Nways MRS Configuration Program is not supported, because you cannot assign a protocol address (IP or IPX) to a dial-circuit interface via the Nways MRS Configuration Program. See APAR NA01134.

The following is a summary of the tasks that must be performed to configure a 2210 to use the Dial-on-Demand feature. When necessary, you will be advised if different configuration tasks must be performed at the other end.

To configure the Dial-on-Demand facility on a IBM 2210, perform the following steps:

1. Configure two serial interfaces or devices (physical switched V.25bis serial interface or ISDN interface and logical dial-circuit serial interface) and assign names to the remote and local phone numbers.
2. In the V.25bis or ISDN configuration process, configure the serial link.

3. In the Circuit configuration process, configure the logical interface.
4. Configure the LAN interface.
5. Configure specific protocols, and assign protocol addresses (IP or IPX) for Dial-on-Demand link on the logical dial-circuits only. No protocol address must be assigned on the physical V.25bis or ISDN interface.

11.10.2.1 Configuration Commands on the CONFIG Process

To configure the Dial-on-Demand facility on an IBM 2210, you must first define the following two interfaces (also called devices):

- The V.25bis or ISDN interface

One of the two physical interfaces must be configured with a V.25bis data-link. If you want to use ISDN interface, you can set the data-link protocol only for the dial-circuit interface mapped to it.

- The dial-circuit interface

This is a logical interface mapped to the V.25bis or ISDN physical interface. It is configured with a PPP data-link. For ISDN dial-circuits, you can configure a frame relay frame. Several dial-circuit interfaces can be customized and mapped to the same V.25bis or ISDN physical interface.

Once the two interfaces have been defined, you must customize them for the Dial-on-Demand feature. To show you how to define the interfaces and customize them for the Dial-on-Demand feature, we will use the example in which the V.25bis or ISDN interface is the interface # and the dial-circuit interface is the interface ##. The following is a summary of the tasks that must be performed:

1. Set the V.25bis data-link for the interface # using the following command:

```
Config>set data-link v25bis #
```

If you want to use the ISDN interface, set the PPP or frame relay data-link for the dial circuit interface ##.

```
Config>set data-link ppp ##
```

```
Config>set data-link fr ##
```

You can use the List Devices command to show the data-link configured for each interface.

2. Add a logical dial-circuit interface which is logically mapped to the V.25bis physical serial interface. To do so, you must issue the following command:

```
Config>add device dial-circuit
```

The interface number assigned to this dial-circuit can be displayed using the List Devices command.

Note: More than one dial-circuit interface can be added.

3. Assign a name to each local and remote phone numbers to be used.

For example, to assign the name local site to the local phone number 12345678, you must issue the following command:

```
Config>add v25-bis-address local-site 12345678
```

or

```
Config>add isdn-address local-site 12345678
```

To assign the name remote site to the phone number 87654321, you must issue the following command:

```
Config>add v25-bis-address remote-site 87654321
```

or

```
Config>add isdn-address remote-site 87654321
```

The name assigned must not exceed 23 characters, and the phone number must not exceed 20 digits.

You can display the names assigned to the phone numbers by using the List v25-bis-address command.

Note: On the 2210 at the other end, phone number 12345678 should be assigned with the name remote site, and phone number 87654321 should be assigned with name local site to be consistent.

11.10.2.2 Configuration Commands on V.25bis Configuration Process

Once the interfaces have been defined, you must customize the V.25bis interface (interface 2 in this example). To do so, you must perform the following steps:

1. Access V.25bis interface (#) customization, using the following command:

```
Config>network #
```

After issuing the above command, the following prompt will be displayed:

```
V.25bis Config>
```

2. Define the phone number assigned to the local end of the V.25bis interface using the previously defined name of local site. You can do so, using the following command:

```
V.25bis Config>set local local-site
```

3. Define the number of seconds the IBM 2210 will wait before retrying to establish a dial-up connection if the previous attempt to establish the dial-up connection fails. This time is referred to as the *timeout-call-address* and can be specified using the following command:

```
V.25bis Config>set timeout-call-address 60
```

The timeout-call-address must be in the range 0 to 65535, and the default is 0 seconds.

4. Define the maximum number of attempted calls to a remote V.25bis address. This is referred to as the *retries-call-address* parameter and can be specified using the following command:

```
V.25bis Config>set retries-call-address 5
```

Note: Each attempt will be made after waiting the number of seconds specified by the timeout-call-address command.

The *retries-call-address* must be in the range 0 to 10, and the default is 1 attempt.

5. The V.25bis interface customization can be displayed using List command.
6. Exit the V.25bis interface configuration, using the following command:

```
V.25bis Config>exit
```

For more information about the V.25bis Interface configuration, see 3.4.24, "Configuring V.25bis" on page 100.

11.10.2.3 Configuration Commands on ISDN Configuration Process

Once the interfaces have been defined, you must customize the ISDN interface (interface # in this example). To do so, you must perform the following steps:

1. Access ISDN interface (#) customization, using the following command:

```
Config>network #
```

After issuing the above command, the following prompt will be displayed:

```
ISDN Config>
```

2. Define the phone number assigned to the local end of the ISDN interface using the previously defined name of local site. You can do so, using the following command:

```
ISDN Config>set local local-site
```

3. Define the number of seconds the IBM 2210 will wait before retrying to establish a dial-up connection if the previous attempt to establish the dial-up connection fails. This time is referred to as the *timeout-call-address* and can be specified by using the following command:

```
ISDN Config>set timeout-call-address 60
```

The timeout-call-address must be in the range 0 to 65535, and the default is 0 seconds.

4. Define the maximum number of attempted calls to a remote ISDN address. This is referred to as the *retries-call-address* parameter and can be specified using the following command:

```
ISDN Config>set retries-call-address 5
```

Note: Each attempt will be made after waiting the number of seconds specified by the timeout-call-address command.

The *retries-call-address* must be in the range 0 to 10, and the default is 1 attempt.

5. The ISDN interface customization can be displayed using List command.
6. Exit the ISDN interface configuration, using the following command:

```
ISDN Config>exit
```

For more information about the ISDN Interface configuration, see 3.5.4, "ISDN Configuration Steps" on page 105.

11.10.2.4 Configuration Commands on Circuit Configuration Process

The next task in our example is to to customize the dial-circuit interface (interface ##). To do so, you must perform the following steps:

1. Access the dial-circuit interface, using the following command:

```
Config>network ##
```

After issuing the above command, the following prompt will be displayed:

```
Circuit Config>
```

2. Map this dial-circuit interface to the V.25bis or ISDN interface (interface # in our example). To do so, issue the following command:

```
Circuit Config>set net #
```

3. Specify if the IBM 2210 is allowed to initiate outbound calls only, to receive inbound calls only or both inbound and outbound calls.

You must issue the following command for the IBM 2210 that will initiate the call:

```
Circuit Config>set calls outbound
```

You must issue the following command for the IBM 2210 that will wait for the call:

```
Circuit Config>set calls inbound
```

To allow the IBM 2210 to be able to both initiate and wait for the calls, you must issue the following command:

```
Circuit Config>set calls both
```

4. Specify that this switched link has to be disconnected after no data has been sent for a period of, say, 30 seconds. To do so, you must issue the following command:

```
Circuit Config>set idle 30
```

5. Define the remote phone number of the dial-circuit interface, using the previously defined name of remote site. To do so, use the following command:

```
Circuit Config>set destination remote-site
```

6. Specify the PPP or frame relay parameters to be used on the dial-up circuit. To access the PPP or frame relay parameters, issue the following command:

```
Circuit Config>encapsulator
```

After issuing the above command, the following prompt will be displayed:

```
PPP Config>
```

or

```
FR Config>
```

You can now change the PPP or frame relay parameters if required.

You can list all the PPP or frame relay parameters of the dial-circuit using the List All command.

To exit the PPP configuration of the secondary interface, issue the following command:

```
PPP Config>exit
```

or

```
FR Config>exit
```

7. You can now display the configuration of the dial-circuit by using the List command.

8. Exit the dial-circuit configuration, using the following command:

```
Circuit Config>exit
```

Note: More than one dial-circuit interface may be defined in your router.

For more information about the Circuit Interface configuration, see 3.4.23.3, "Dial Circuits" on page 97.

11.10.3 Scenario 7: Dial-on-Demand Implementation over IP

In this scenario, we have one 2210 with a token-ring interface (2210A) and one 2210 with an Ethernet interface (2210B). Both 2210s are linked together using a switched PPP link with V.25bis modems on interface 2 for both 2210s.

2210A and 2210B are both IP routers.

- Interfaces:

The token-ring interface on 2210A runs at 4 MBps, and is connected to the LAN using the UTP connector. It uses the MAC address 40002210A001.

Ethernet interface on the 2210B is connected to the LAN using the 10Base-T connector.

The switched serial link (PPP link over V.25bis modems) is interface 2 for both 2210s.

Interface 1 is not used in either of the 2210s.

- IP routing:

2210A is an IP router with an IP address 9.67.46.146 on its token-ring interface and an IP address of 9.67.46.132 on its serial 1 interface. 2210A has a static route to reach the 9.67.46.64 subnetwork with a subnetmask of 255.255.255.240 via the 9.67.46.131 router.

2210B is an IP router with an IP address of 9.67.46.77 on its Ethernet interface and an IP address of 9.67.46.131 on its serial 1 interface. 2210B has a static route to reach the 9.67.46.144 subnetwork with a subnetmask of 255.255.255.240 via the 9.67.46.132 router.

- Dial-on-Demand:

The dial number of 2210A is 8-352-2184. The dial number of 2210B is 8-352-2186. The call could be initiated from both 2210s.

For more information about IP protocol customization, see 8.2, "Configuring IP on the IBM 2210" on page 341. Figure 196 on page 691 shows the configuration of the network used in this scenario.

The following figures provide the customization samples that are used in this scenario:

- Figure 197 on page 692 shows the 2210A configuration via the ASCII console.
- Figure 198 on page 697 shows the 2210B configuration via the ASCII console.

In testing this scenario, both TCP/IP PING and TFTP file transfers between end user A and end user B were successful. The switched link is established as soon as one of the IBM 2210s has some data to send to the other IBM 2210.

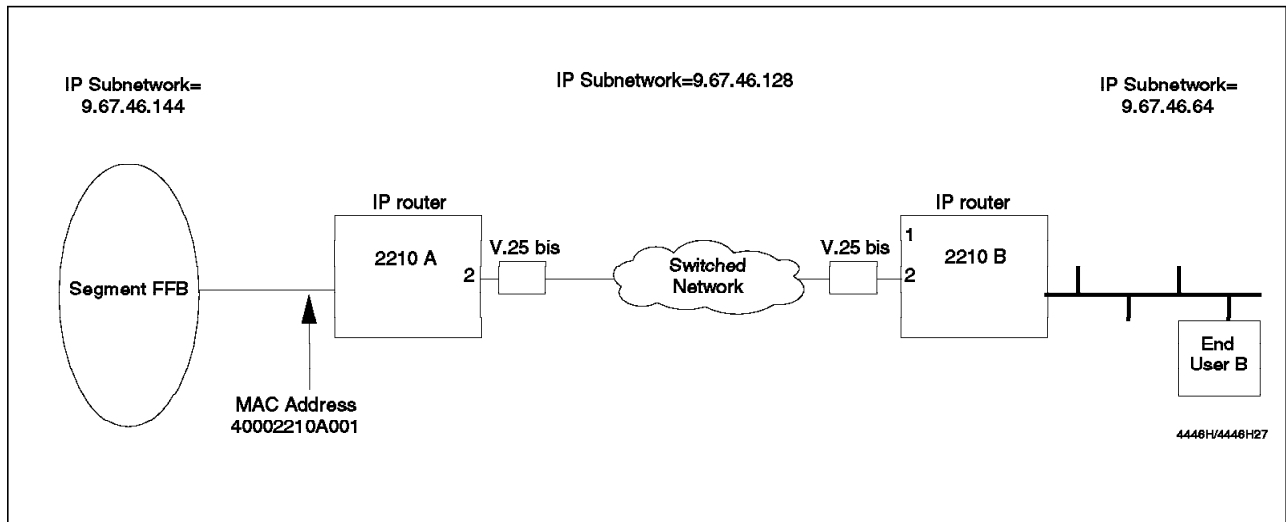


Figure 196. Scenario 7: Dial-on-Demand

```

*
*talk 6 1

Config>disable interface 1 2
Config>set data-link v25bis 2 3
Config>add v25-bis-address local-site 8-352-2184 4
Config>add v25-bis-address remote-site 8-352-2186 5
Config>add device dial-circuit 6
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
Config>list v25-bis-address 7

Address assigned name      Network Address
-----
local-site                 8-352-2184
remote-site                8-352-2186
Config>list devices 8
Ifc 0 (Token Ring): CSR 6000000, vector 28
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
      (Disabled)
Ifc 2 (WAN V.25bis): CSR 81640, CSR2 80E00, vector 92
Ifc 3 (PPP Dial Circuit): CSR 0, vector 0
Config>network 0 9
Token-Ring interface configuration
TKR config>media unshielded
TKR config>set physical-address 40:00:22:10:a0:01
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                     4 Mb/sec
Media:                     Unshielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:               40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 2 10
V.25bis Data Link Configuration
V.25bis Config>set local local-site 11
V.25bis Config>set timeout-call-address 60 12
V.25bis Config>set retries-call-address 5 13

:

```

Figure 197 (Part 1 of 4). Scenario 7: 2210A Configuration via the ASCII Console

```

:
V.25bis Config>list 14
    V.25bis Configuration
Local Network Address Name    = local-site
Local Network Address        = 8-352-2184

Non-Responding addresses:
Retries                      = 5
Timeout                      = 60 seconds

Call timeouts:
Command Delay                = 0 ms
Connect                      = 60 seconds
Disconnect                   = 2 seconds
V.25bis Config>exit
Config>network 3 15
Circuit configuration
Circuit Config>set net 2 16
Circuit Config>list 17

Base net:                    2
Destination name:
Outbound calls               allowed
Inbound calls                allowed
Idle timer                   = 60 sec
SelfTest Delay Timer = 150 ms

Circuit Config>set destination remote-site 18
Circuit Config>set idle 30 19
Circuit Config>list

Base net:                    2
Destination name:            remote-site
Outbound calls               allowed
Inbound calls                allowed
Idle timer                   = 30 sec
SelfTest Delay Timer = 150 ms

Circuit Config>encapsulator 20
Point-to-Point user configuration
PPP Config>list all 21

LCP Parameters
-----
CONFIG Request Tries:        20    CONFIG Nak Tries:        10
Terminate Tries:            10    Retry Timer:          3000

:

```

Figure 197 (Part 2 of 4). Scenario 7: 2210A Configuration via the ASCII Console

```

:
LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:   A0000
Protocol Field Comp(PFC):   No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20    CONFIG Nak Tries:      10
Terminate Tries:          10    Retry Timer:           3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit
Circuit Config>exit
Config>protocol ip 22
Internet protocol user configuration
IP config>add address 0 9.67.46.146 255.255.255.240
IP config>add address 3 9.67.46.132 255.255.255.240 23
IP config>add route 24
IP destination [0.0.0.0]? 9.67.46.64
Address mask [0.0.0.0]? 255.255.255.240
Via gateway at [0.0.0.0]? 9.67.46.131
Cost [1]?
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.146      255.255.255.240 Network broadcast,   fill 0
  intf 1                                     IP disabled on this interface
  intf 2                                     IP disabled on this interface
  intf 3  9.67.46.132      255.255.255.240 Network broadcast,   fill 0
:

```

Figure 197 (Part 3 of 4). Scenario 7: 2210A Configuration via the ASCII Console

```

:
Routing
route to 9.67.46.64,255.255.255.240 via 9.67.46.131, cost 1

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled

IP config>exit
Config>Ctrl+p
*restart 25
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 197 (Part 4 of 4). Scenario 7: 2210A Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Disable interface serial 1 which is not used in this scenario.
- 3** Set the data-link of interface 2 to V.25bis.
- 4** Assign the name local site to the 2210A phone number.
- 5** Assign the name remote site to the 2210B phone number.
- 6** Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 3.
- 7** List the customized V.25-bis-addresses.
- 8** Lists the devices configuration. Interface 1 is disabled, interface 2 is the physical switched V.25bis link, and interface 3 is the logical dial-circuit with PPP encapsulation.

- 9** Customization of network 0. This is the token-ring interface. Specify that the UTP connector is used and define the locally administered address for this interface.
- 10** Customization of network 2. This is the serial 2 interface with V.25bis modems.
- 11** Set the local phone number, using the name defined earlier.
- 12** Set the number of seconds to wait before a retry.
- 13** Set the number of retries for a call in case of no answer.
- 14** List the interface 2 configuration.
- 15** Customization of network 3. This is the logical dial-circuit.
- 16** Set the physical network number on which the calls will be actually performed.
- 17** List the interface 3 configuration.
- 18** Set the destination phone number, using the name defined earlier.
- 19** Set the idle timer to 30. The switched connection will be dropped if there are no frames to be sent for 30 seconds.
- 20** Access the link layer protocol that is running on this dial-circuit. The only encapsulation method available is PPP.
- 21** List the PPP link parameters. Use the default settings.
- 22** Customization of the IP protocol. Assign IP addresses to interfaces.
- 23** The IP address for the serial interfaces must be added only to the logical dial-circuit interface. No IP address must be assigned to the V.25bis interface.
- 24** Add a static route to reach the 9.67.46.64 subnetwork with a subnet mask of 255.255.255.240 via the router 9.67.46.131.
- 25** Restart the 2210A to get the configuration running.

```

*
*talk 6 1

Config>add v25-bis-address local-site 8-352-2186 2
Config>add v25-bis-address remote-site 8-352-2184 3
Config>list v25-bis address 4

Address assigned name      Network Address
-----
local-site                 8-352-2186
remote-site                8-352-2184
Config>list devices
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
Ifc 2 (WAN PPP): CSR 81640, CSR2 80E00, vector 92
Config>disable interface 1 5
Config>set data-link v25bis 2 6
Config>add device dial-circuit 7
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
Config>list devices 8
Ifc 0 (Ethernet): CSR 81600, CSR2 80C00, vector 94
Ifc 1 (WAN PPP): CSR 81620, CSR2 80D00, vector 93
(Disabled)
Ifc 2 (WAN V.25bis): CSR 81640, CSR2 80E00, vector 92
Ifc 3 (PPP Dial Circuit): CSR 0, vector 0
Config>network 0 9
Ethernet interface configuration
ETH config>list
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:       ETHER

ETH config>exit
Config>network 2 10
V.25bis Data Link Configuration
V.25bis Config>set local local-site 11
V.25bis Config>set timeout-call-address 60 12
V.25bis Config>set retries-call-address 5 13
V.25bis Config>list 14
      V.25bis Configuration
Local Network Address Name    = local-site
Local Network Address         = 8-352-2186

Non-Responding addresses:
Retries                       = 5
Timeout                       = 60 seconds

:

```

Figure 198 (Part 1 of 3). Scenario 7: 2210B Configuration via the ASCII Console

```

:
Call timeouts:
Command Delay      = 0 ms
Connect           = 60 seconds
Disconnect         = 2 seconds
V.25bis Config>exit
Config>network 3 15
Circuit configuration
Circuit Config>set net 2 16
Circuit Config>set idle 30 17
Circuit Config>set destination remote-site 18
Circuit Config>list 19

Base net:      2
Destination name: remote-site
Outbound calls allowed
Inbound calls  allowed
Idle timer     = 30 sec
SelfTest Delay Timer = 150 ms

Circuit Config>encapsulator 20
Point-to-Point user configuration
PPP Config>list all 21

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):    No   Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

:

```

Figure 198 (Part 2 of 3). Scenario 7: 2210B Configuration via the ASCII Console


```

:

BCP Options
-----
Tinygram Compression:          Disabled

IPCP Options
-----
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>exit
Circuit Config>exit
Config>protocol ip             22
Internet protocol user configuration
IP config>add address 0 9.67.46.77 255.255.255.240
IP config>add address 3 9.67.46.131 255.255.255.240 23
IP config>add route 9.67.46.144 255.255.255.240 9.67.46.132 1 24
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.77      255.255.255.240 Network broadcast,   fill 0
  intf 1                                IP disabled on this interface
  intf 2                                IP disabled on this interface
  intf 3  9.67.46.131     255.255.255.240 Network broadcast,   fill 0

Routing

route to 9.67.46.144,255.255.255.240 via 9.67.46.132, cost 1

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled

IP config>exit
Config>Ctrl+p
*restart 25
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 198 (Part 3 of 3). Scenario 7: 2210B Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Assign the name local site to the 2210B phone number.
- 3** Assign the name remote site to the 2210A phone number.
- 4** List the customized v25-bis-addresses.
- 5** Disable serial interface 1 which is not used in this scenario.
- 6** Set the data-link of interface 2 to V.25bis.
- 7** Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 3.
- 8** List the devices configuration. Interface 1 is disabled, interface 2 is the physical switched V.25bis link and interface 3 is the logical dial-circuit with PPP encapsulation.
- 9** Access the customization of network 0 (Ethernet interface). Display the current configuration. Use the default settings.
- 10** Customization of network 2. This is the serial 2 interface with V.25bis modems.
- 11** Set the local phone number using the name defined earlier.
- 12** Set the number of seconds to wait before a retry.
- 13** Set the number of retries for a call in case of no answer.
- 14** List the interface 2 configuration.
- 15** Customization of network 3. This is the logical dial-circuit.
- 16** Set the physical network number on which the calls will be actually performed.
- 17** Set the idle timer to 30. The switched connection will be dropped if there are no frames sent for 30 seconds.
- 18** Set the destination phone number using the name defined earlier.
- 19** List the interface 3 configuration.
- 20** Access the link layer protocol that is running on this dial-circuit. The only encapsulation method available is PPP.
- 21** List the PPP link parameters. Use the default settings.
- 22** Customization of the IP protocol. Assign IP addresses to interfaces.
- 23** The IP address for the serial interfaces must be added only to the logical dial-circuit interface. No IP address must be assigned to the V.25bis interface.

24 Add a static route to reach the 9.67.46.144 subnetwork with a subnet mask 255.255.255.240 via the router 9.67.46.132.

25 Restart the 2210B to get the configuration running.

11.10.4 Scenario 8: Dial-on-Demand Implementation over IP Using ISDN

In this scenario, we have one 2210 with a token-ring interface (2210A) and one 2210 with an Ethernet interface (2210B). Both 2210s are linked together using a PPP link through the ISDN on interface 2 for both 2210s.

2210A and 2210B are both IP routers.

- Interfaces:

The token-ring interface on 2210A runs at 4 MBps, and is connected to the LAN, using the UTP connector. It uses the MAC address 40002210A001.

The Ethernet interface on the 2210B is connected to the LAN using the 10Base-T connector.

The serial link (PPP link over ISDN) is interface 2 for both 2210s.

Interface 1 is not used in either of the 2210s.

- IP routing:

The 2210A is an IP router with an IP address of 9.67.46.146 on its token-ring interface and an IP address of 9.67.46.132 on its serial 1 interface. 2210A has a static route to reach the 9.67.46.64 subnetwork with a subnetmask of 255.255.255.240 via the 9.67.46.131 router.

The 2210B is an IP router with an IP address of 9.67.46.77 on its Ethernet interface and an IP address of 9.67.46.131 on its serial 1 interface. 2210B has a static route to reach the 9.67.46.144 subnetwork with a subnetmask of 255.255.255.240 via the 9.67.46.132 router.

- Dial-on-Demand:

The dial number of 2210A is 8-352-2184. The dial number of 2210B is 8-352-2186. The call could be initiated from both 2210s.

For more information about IP protocol customization, see 8.2, "Configuring IP on the IBM 2210" on page 341. Figure 199 on page 702 shows the configuration of the network used in this scenario.

The following figures provide the customization samples that are used in this scenario:

- Figure 200 on page 703 shows the 2210A configuration via the ASCII console.
- Figure 201 on page 708 shows the 2210B configuration via the ASCII console.

In testing this scenario, both TCP/IP PING and TFTP file transfer between end user A and end user B were successful. The switched link is established as soon as one of the IBM 2210s has some data to send to the other IBM 2210.

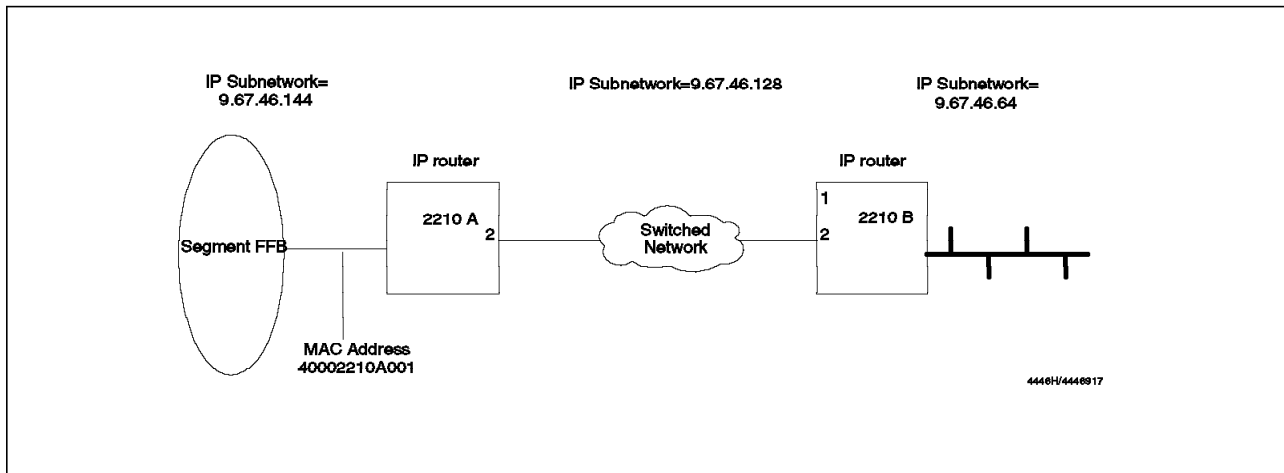


Figure 199. Scenario 8: Dial-on-Demand Using ISDN

```

*
*talk 6 1

Config>add isdn
Assign address name [1-23] chars []? local-site 2
Assign network dial address [1-25 digits] []? 8-352-2184 2
Assign network subdial address [0-20 digits] []? 2
Config>add isdn
Assign address name [1-23] chars []? remote-site 3
Assign network dial address [1-25 digits] []? 8-352-2186 3
Assign network subdial address [0-20 digits] []? 3
Config>add device dial-circuit 4
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Config>set data-link ppp 4 5
Config>list isdn-address 6

Address assigned name      Network Address  Network Subaddress
-----
local-site                 8-352-2184
remote-site                8-352-2186
Config>list devices 7
Ifc 0   Token Ring                CSR 6000000, vector 28
Ifc 1   WAN PPP                   CSR 81620, CSR2 80D00, vector 93
Ifc 2   WAN PPP                   CSR 81640, CSR2 80E00, vector 92
Ifc 3   ISDN Basic                CSR 0, vector 0
Ifc 4   PPP Dial Circuit           CSR 0, vector 0
Config>network 0 8
Token-Ring interface configuration
TKR config>media unshielded
TKR config>set physical-address 40:00:22:10:a0:01
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                     4 Mb/sec
Media:                     Unshielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              40002210A001
IPX interface configuration record missing

TKR config>exit
Config>network 3 9
ISDN user configuration
ISDN Config>set local-address-name
Assign local address name []? local-site 10
ISDN Config>set switch
Switch-Variant-Model [NET3]? net3 11

:

```

Figure 200 (Part 1 of 4). Scenario 8: 2210A Configuration via the ASCII Console

```

:
ISDN Config>set dn0
Enter DNO (Directory-Number-0) []? 8-352-2184 12
ISDN Config>set retries-call-address 5 13
ISDN Config>set timeout-call-address 60 14
ISDN Config>list 15
ISDN Configuration

Local Network Address Name      = local-site
Local Network Address:Subaddress = 8-352-2184:

Maximum frame size in bytes     = 2048
Outbound call address Timeout   = 60 Retries = 5
Switch Variant                  = Net 3
DNO (Directory Number 0)        = 8-352-2184
Multipoint Selection            = Point-to-Point
TEI                             = Automatic
PS1 detect                     = Disabled
No circuit address accounting information being kept
ISDN Config>exit
Config>network 4 16
Circuit configuration
Circuit Config>list 17

Base net                        = 0
Destination name                =
Circuit priority                = 8

Outbound calls                  = allowed
Idle timer                     = 60 sec
SelfTest Delay Timer            = 150 ms

Circuit Config>set net 3 18
Circuit Config>set calls both 18
Circuit Config>set destination remote-site 19
Circuit Config>set idle 20
Idle timer (seconds, 0 means always active) [60]? 180
Circuit Config>list 21

Base net                        = 3
Destination name                = remote-site
Circuit priority                = 8

Outbound calls                  = allowed
Inbound calls                   = allowed
Idle timer                     = 180 sec
SelfTest Delay Timer            = 150 ms

Circuit Config>encapsulator 22
Point-to-Point user configuration

:

```

Figure 200 (Part 2 of 4). Scenario 8: 2210A Configuration via the ASCII Console

```

:
PPP Config>list all      23

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):    No   Addr/Cntl Field Comp(ACFC):    No

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
-----
IPCP Compression:          None
IP Address:                Don't Send or Request
PPP Config>exit
Circuit Config>exit
Config>protocol ip      24
Internet protocol user configuration
IP config>add address 0 9.67.46.146 255.255.255.240
IP config>add address 3 9.67.46.132 255.255.255.240      25
IP config>add route      26
IP destination [0.0.0.0]? 9.67.46.64
Address mask [0.0.0.0]? 255.255.255.240
Via gateway at [0.0.0.0]? 9.67.46.131
Cost [1]?

:

```

Figure 200 (Part 3 of 4). Scenario 8: 2210A Configuration via the ASCII Console

```

:
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.146      255.255.255.240  Network broadcast,    fill 0
  intf 1                                IP disabled on this interface
  intf 2                                IP disabled on this interface
  intf 3  9.67.46.132      255.255.255.240  Network broadcast,    fill 0

Routing

route to 9.67.46.64,255.255.255.240 via 9.67.46.131, cost 1

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled

IP config>exit
Config>Ctrl+p
*restart 27
Are you sure you want to restart the gateway? (Yes or [No]): yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 200 (Part 4 of 4). Scenario 8: 2210A Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Assign the name local site to the 2210A phone number.
- 3** Assign the name remote site to the 2210B phone number.
- 4** Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 4.
- 5** Set the data-link of interface 4 to PPP.
- 6** List the customized ISDN addresses.

- 7** Lists the devices configuration. Interface 3 is the physical ISDN link and interface 4 is the logical dial-circuit with PPP encapsulation.
- 8** Customization of network 0. This is the token-ring interface. Specify that the UTP connector is used and define the locally administered address for this interface.
- 9** Customization of network 3. This is the ISDN interface.
- 10** Set the local phone number using the name defined earlier.
- 11** Set the switch type.
- 12** If you set the switch-variant to NET3, VN3, DMS250 or AUS, set the directory number of the local port. Set the network dial address (telephone number) of the local port.
- 13** Set the number of retries for a call in case of no answer.
- 14** Set the number of seconds to wait before a retry.
- 15** List the ISDN configuration.
- 16** Customization of network 4. This is the logical dial-circuit.
- 17** List the interface 4 configuration.
- 18** Set the physical network number on which the calls will be actually performed.
- 19** Set the destination phone number using the name defined earlier.
- 20** Set the idle timer to 180. The switched connection will be dropped if there are no frames sent for 180 seconds.
- 21** List the circuit configuration.
- 22** Access the link layer protocol that is running on this dial-circuit. The only encapsulation method available is PPP.
- 23** List the PPP link parameters. Use the default settings.
- 24** Customization of the IP protocol. Assign IP addresses to interfaces.
- 25** The IP address for the serial interfaces must be added only to the logical dial-circuit interface. No IP address must be assigned to the ISDN interface.
- 26** Add a static route to reach the 9.67.46.64 subnetwork with a subnet mask of 255.255.255.240 via the router 9.67.46.131.
- 27** Restart the 2210A to get the configuration running.

```

*
*talk 6 1

Config>add isdn
Assign address name [1-23] chars []? local-site 2
Assign network dial address [1-25 digits] []? 8-352-2186 2
Assign network subdial address [0-20 digits] []? 2
Config>add isdn
Assign address name [1-23] chars []? remote-site 3
Assign network dial address [1-25 digits] []? 8-352-2184 3
Assign network subdial address [0-20 digits] []? 3
Config>add device dial-circuit 4
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Config>set data-link ppp 4 5
Config>list ISDN address 6

Address assigned name      Network Address  Network Subaddress
-----
local-site                8-352-2186
remote-site               8-352-2184
Config>list devices 7

Ifc 0  Ethernet          CSR  81600, CSR2  80C00, vector 94
Ifc 1  WAN PPP           CSR  81620, CSR2  80D00, vector 93
Ifc 2  WAN PPP           CSR  81640, CSR2  80E00, vector 92
Ifc 3  ISDN Basic        CSR      0, vector 0
Ifc 4  PPP Dial Circuit   CSR      0, vector 0
Config>network 0 8
Ethernet interface configuration
ETH config>list
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 3 9
ISDN Data Link Configuration
ISDN Config>set local-address-name
Assign local address name []? local-site 10
ISDN Config>set switch
Switch-Variant-Model [NET3]? net3 11
ISDN Config>set dn0
Enter DNO (Directory-Number-0) []? 8-352-2184 12
ISDN Config>set retries-call-address 5 13
ISDN Config>set timeout-call-address 60 14
ISDN Config>list 15
ISDN Configuration

Local Network Address Name      = local-site
Local Network Address:Subaddress = 8-352-2184:

:

```

Figure 201 (Part 1 of 4). Scenario 8: 2210B Configuration via the ASCII Console

```

:
Maximum frame size in bytes      = 2048
Outbound call address Timeout    = 60 Retries = 5
Switch Variant                  = Net 3
DNO (Directory Number 0)        = 8-352-2184
Multipoint Selection             = Point-to-Point
TEI                             = Automatic
PS1 detect                      = Disabled
No circuit address accounting information being kept
ISDN Config>exit
Config>network 4 16
Circuit configuration
Circuit Config>list 17

Base net                        = 0
Destination name                =
Circuit priority                = 8

Outbound calls                  = allowed
Idle timer                     = 60 sec
SelfTest Delay Timer           = 150 ms

Circuit Config>set net 3 18
Circuit Config>set calls both 18
Circuit Config>set destination remote-site 19
Circuit Config>set idle 20
Idle timer (seconds, 0 means always active) [60]? 180
Circuit Config>list 21

Base net                        = 3
Destination name                = remote-site
Circuit priority                = 8

Outbound calls                  = allowed
Inbound calls                   = allowed
Idle timer                     = 180 sec
SelfTest Delay Timer           = 150 ms

Circuit Config>encapsulator 22
Point-to-Point user configuration
PPP Config>list all 23

LCP Parameters
-----
CONFIG Request Tries:          20  CONFIG Nak Tries:          10
Terminate Tries:               10  Retry Timer:             3000

LCP Options
-----
Max Receive Unit:              2048  Magic Number:          Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):      No    Addr/Cntl Field Comp(ACFC): No
:

```

Figure 201 (Part 2 of 4). Scenario 8: 2210B Configuration via the ASCII Console

```

:
Authentication Options
-----
Authenticate remote using: none
Identify self as: ibm

NCP Parameters
-----
CONFIG Request Tries:          20  CONFIG Nak Tries:          10
Terminate Tries:              10  Retry Timer:              3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:         Disabled

IPCP Options
-----
IPCP Compression:             None
IP Address:                   Don't Send or Request
PPP Config>exit
Circuit Config>exit
Config>protocol ip           24
Internet protocol user configuration
IP config>add address 0 9.67.46.77 255.255.255.240
IP config>add address 3 9.67.46.131 255.255.255.240 25
IP config>add route 9.67.46.144 255.255.255.240 9.67.46.132 1 26
IP config>list all
Interface addresses
IP addresses for each interface:
  intf 0  9.67.46.77      255.255.255.240 Network broadcast, fill 0
  intf 1                                     IP disabled on this interface
  intf 2                                     IP disabled on this interface
  intf 3  9.67.46.131     255.255.255.240 Network broadcast, fill 0

Routing

route to 9.67.46.144,255.255.255.240 via 9.67.46.132, cost 1

Protocols
BOOTP forwarding: disabled
Directed broadcasts: enabled
ARP Subnet routing: disabled

:

```

Figure 201 (Part 3 of 4). Scenario 8: 2210B Configuration via the ASCII Console

```

:
RFC925 routing: disabled
OSPF: disabled
Per-packet-multipath: disabled
RIP: disabled
EGP: disabled

IP config>exit
Config>Ctrl+p
*restart 27
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 201 (Part 4 of 4). Scenario 8: 2210B Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Assign the name local site to the 2210B phone number.
- 3** Assign the name remote site to the 2210A phone number.
- 4** Add a logical dial-circuit. Note that the IBM 2210 issues a message to inform us that this new device is the interface number 4.
- 5** Set the data-link of interface 4 to PPP.
- 6** List the customized ISDN addresses.
- 7** Lists the devices configuration. Interface 3 is the physical ISDN link and interface 4 is the logical dial-circuit with PPP encapsulation.
- 8** Access the customization of network 0 (Ethernet interface). Display the current configuration. Use the default settings.
- 9** Customization of network 3. This is the ISDN interface.
- 10** Set the local phone number using the name defined earlier.
- 11** Set the switch type.
- 12** If you set the switch-variant to NET3, VN3, DMS250 or AUS, set the directory number of the local port. Set the network dial address (telephone number) of the local port.
- 13** Set the number of retries for a call in case of no answer.
- 14** Set the number of seconds to wait before a retry.
- 15** List the ISDN configuration.

- 16** Customization of network 4. This is the logical dial-circuit.
- 17** List the interface 4 configuration.
- 18** Set the physical network number on which the calls will be actually performed.
- 19** Set the destination phone number using the name defined earlier.
- 20** Set the idle timer to 180. The switched connection will be dropped if there are no frames sent for 180 seconds.
- 21** List the circuit configuration.
- 22** Access the link layer protocol that is running on this dial-circuit. The encapsulation method is PPP in this scenario.
- 23** List the PPP link parameters. Use the default settings.
- 24** Customization of the IP protocol. Assign IP addresses to interfaces.
- 25** The IP address for the serial interfaces must be added only to the logical dial-circuit interface. No IP address must be assigned to the ISDN interface.
- 26** Add a static route to reach the 9.67.46.144 subnetwork with a subnet mask 255.255.255.240 via the router 9.67.46.132.
- 27** Restart the 2210B to get the configuration running.

11.11 NetBIOS Facilities

This section describes the two NetBIOS facilities available in the IBM 2210:

- NetBIOS name caching
- NetBIOS filtering

11.11.1 The NetBIOS Name Caching Facility

In this subsection, we explain NetBIOS name caching, we provide a brief description of the main commands needed to configure NetBIOS name caching, and provide a NetBIOS name caching scenario.

11.11.1.1 Introduction to the NetBIOS Name Caching Facility

This facility allows an IBM 2210, configured as a bridge, to operate more efficiently when bridging NetBIOS traffic.

Note

The NetBIOS Name Caching facility applies only on a token-ring port and a PPP serial link port.

The NetBIOS protocol issues many All Route Broadcast messages on the network which can affect the performance of a WAN link used to transport bridged traffic. In order to reduce the amount of All Route Broadcasted frames forwarded by the IBM 2210, the NetBIOS name caching facility provides two processes:

- The name caching for name-query frames

The name caching process allows the IBM 2210 to convert all of the route broadcast name-query frames into specifically routed name-query frames.

- Duplicate frames filtering for add-name, add-group-name and name-query frames

The duplicate frame filtering process allows the IBM 2210 to reduce the amount of name-query frames, add-name frames and add-name-group frames that are broadcast over the network.

Each of the above processes can be enabled independently of the other. Each process maintains a different database which is independent of the database used by the other process. However, if both are enabled, the duplicate frame filtering process is performed by the IBM 2210 before the name caching process.

Note

Duplicate frame filtering is different from the NetBIOS Filtering Facility, which is described in 11.11.2, "NetBIOS Filtering Facility" on page 723.

Name Caching Process for Name-Query Frames: In the first step of a data transfer, a NetBIOS client resolves the name of the NetBIOS server to a physical address and a route. This is done by the NetBIOS client broadcasting a spanning tree explorer (STE) group frame called name-query. The remote NetBIOS server answers with either a specifically routed frame or an all-routes frame. The response from the server is called a name-query-response and is addressed to the NetBIOS client.

In the name-query-response, the information about the NetBIOS name server is correlated with its MAC address and the route to reach it.

Unfortunately, most of NetBIOS client stations do not save the result of a name resolution contained in a name-query-response to be used when other frames are sent to the same NetBIOS server. Therefore, each time a NetBIOS client wants to send a NetBIOS frame, or initiate a NetBIOS connection, a name-query frame is broadcast over the network.

With name caching enabled, the IBM 2210 acts on the behalf of the NetBIOS server stations, by maintaining a database of server names with their MAC address and the routes to reach them.

The following is the description of the processing, which happens as a result of the name caching facility:

- When the bridge receives a name-query frame from a NetBIOS client, it checks its database to see if it knows about the NetBIOS server name that is being queried in this frame.
 - If it has an entry in its database for this server, the name-query frame is converted from a broadcast spanning tree explorer (STE) frame to a specifically routed frame (SRF), then the name-query frame is directly bridged to the NetBIOS server.
 - If it does not have an entry in its database for the server, an entry will be added to the database without a MAC address and route information for the time being. The name-query frame is then bridged without any changes to the contents of the frame.
- When the bridge receives a name-query-response frame from a NetBIOS server, it checks its database to see if it has an entry for the server that is sending this frame.
 - If yes, the MAC address and route information of the frame are used to update the corresponding entry in the database, and the frame is bridged without any changes to the contents of the frame.
 - If it does not have an entry for the server that is sending the frame, the name-query-response frame is bridged without any modification to the contents of the frame. The database is not updated.

To manage the name caching database, there are two timers for each server name entry:

- Idle-timer

If an entry in the database is not referenced by a received name-query or a name-query-response frame before the expiration of the idle-timer, this entry is deleted from the database.

- Server-timer

When the IBM 2210 receives a name-query for a server that already has an entry in the database, it starts a timer. If a name-query-response is not received from the server before the expiration of the server-timer, the MAC address and route information for the server name are deleted, but the entry will remain in the database.

Therefore, each entry in the name caching database contains the following attributes:

- The NetBIOS server name
- The MAC address of the NetBIOS server name
- The route to reach the NetBIOS server name
- The idle-timer
- The server timer

Figure 202 on page 716 shows the name caching process for the received name-query frames, and Figure 203 on page 717 shows the name caching process for the received name-query-response frames.

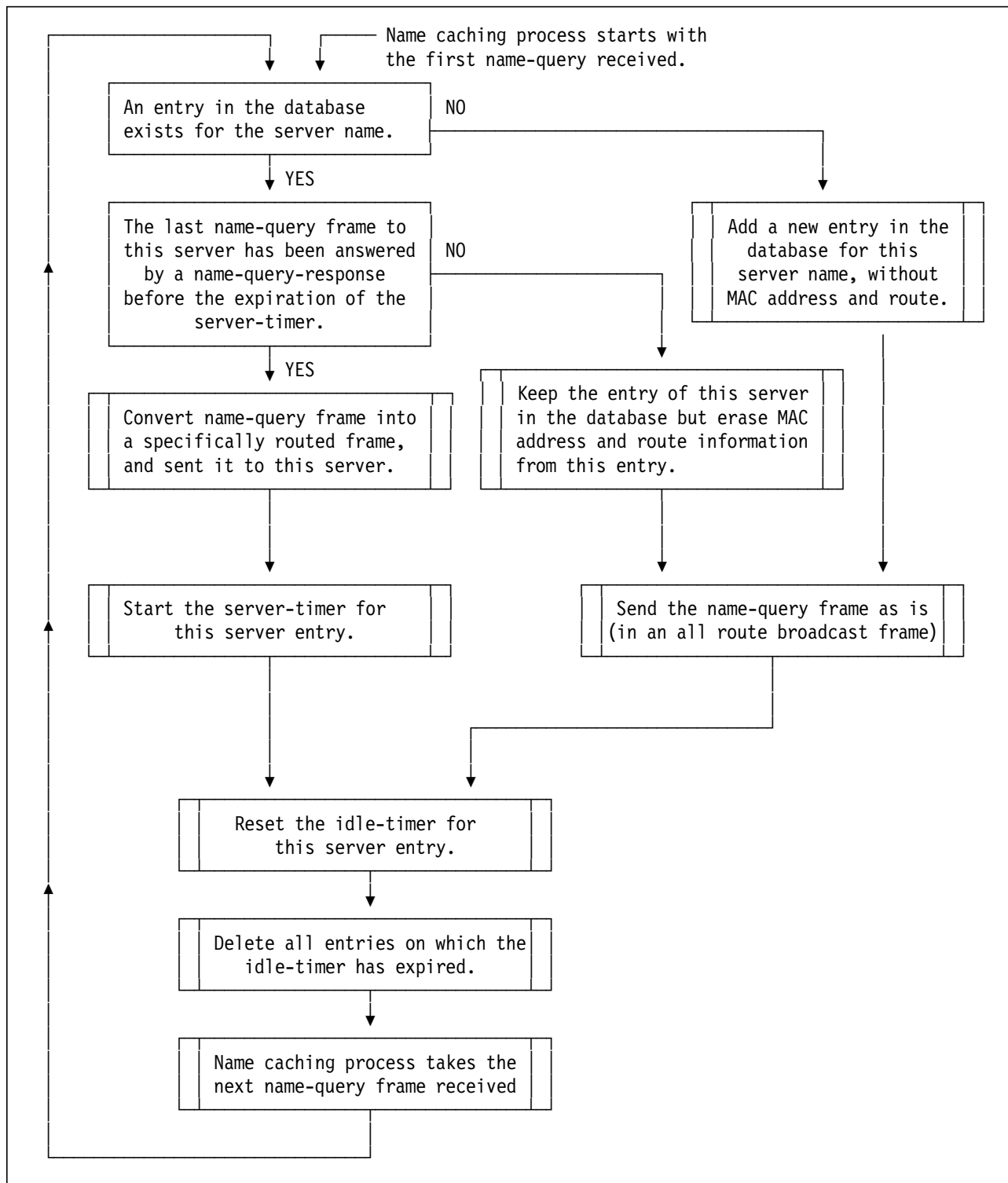


Figure 202. Name Caching Process for the Received Name-Query Frames

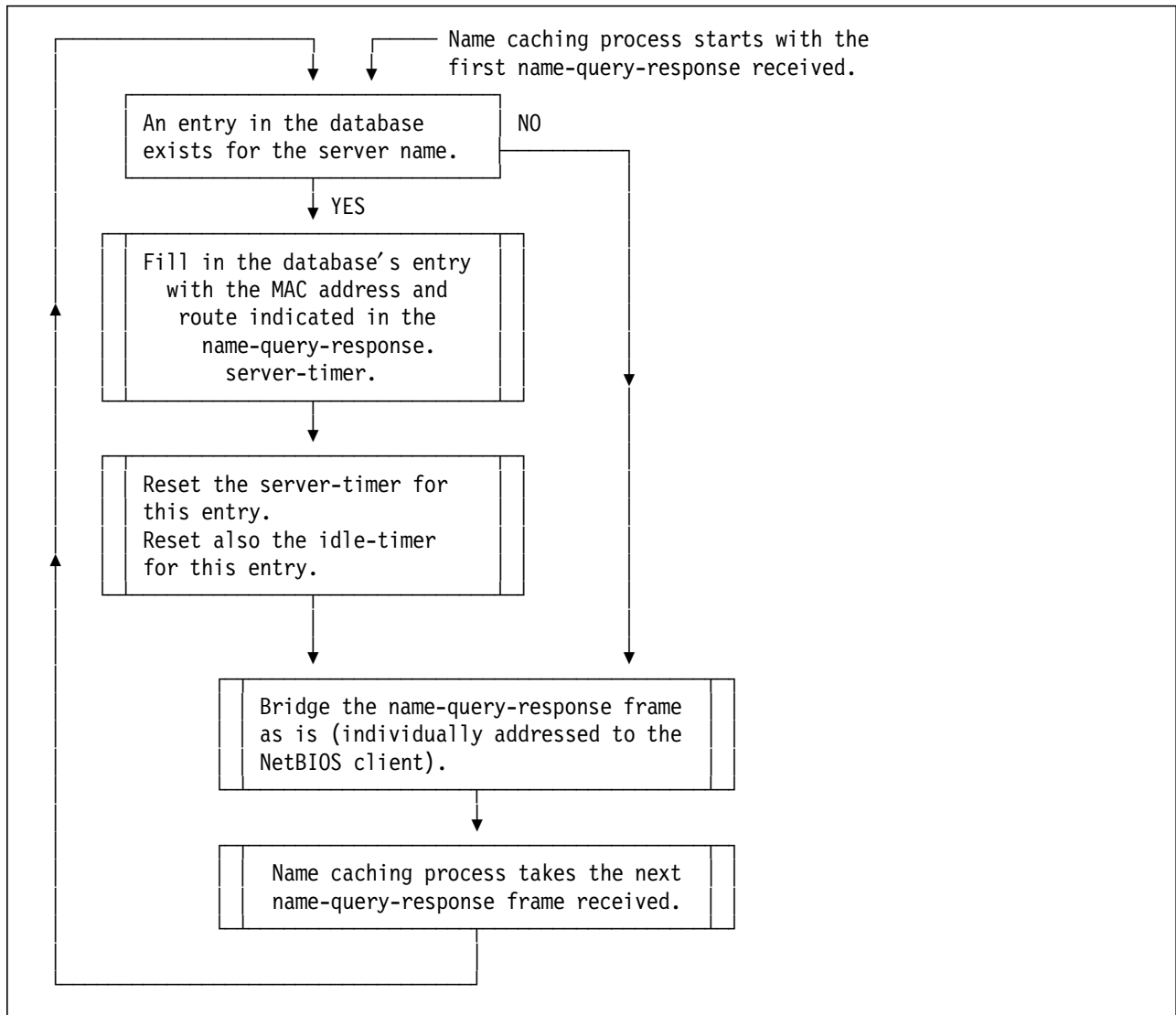


Figure 203. Name Caching Process for the Received Name-Query-Response Frames

Duplicate Frame Filtering Process: This process is performed on the following three broadcast frames:

- Name-Query
- Add-Name
- Add-Name-Group

When a NetBIOS client wants to transmit one of these three types of broadcast frames, a group of six broadcast frames of the same type is sent in half-second intervals before waiting for a response.

The duplicate frame filtering process allows only one instance of each type of frame from a specific NetBIOS client to be broadcast through the IBM 2210 bridge during a certain period of time.

Note that there is a separate timer for each of the three types of broadcast frames. Also, there is a set of these three timers for each NetBIOS client. These timers are referred to as:

- Name-Query timer

- Add-Name timer
- Add-Name-Group timer

The following is a description of the duplicate frame filtering process performed on the broadcast frames:

- When a broadcast frame (name-query, add-name or add-name-group) is received, the IBM 2210 bridges it normally and starts the corresponding timer (name-query timer, add-name timer or add-name-group timer) for the NetBIOS client referenced in this frame.
- All the following broadcast frames of the same type (name-query, add-name or add-name-group) from the same NetBIOS client are discarded by the IBM 2210 until the corresponding timer expires.
- After the timer expiration, the IBM 2210 will allow the next broadcast frame of that type from that NetBIOS client to be bridged normally.

To maintain the timers for all the NetBIOS client stations, there is a duplicate frame filtering database. Each entry in this database contains the following parameters:

- The MAC address of the NetBIOS client name
- The name-query-timer
- The add-name-timer
- The add-name-group-timer

Figure 204 on page 719 shows you the duplicate frame filtering process for the add-name broadcast frames.

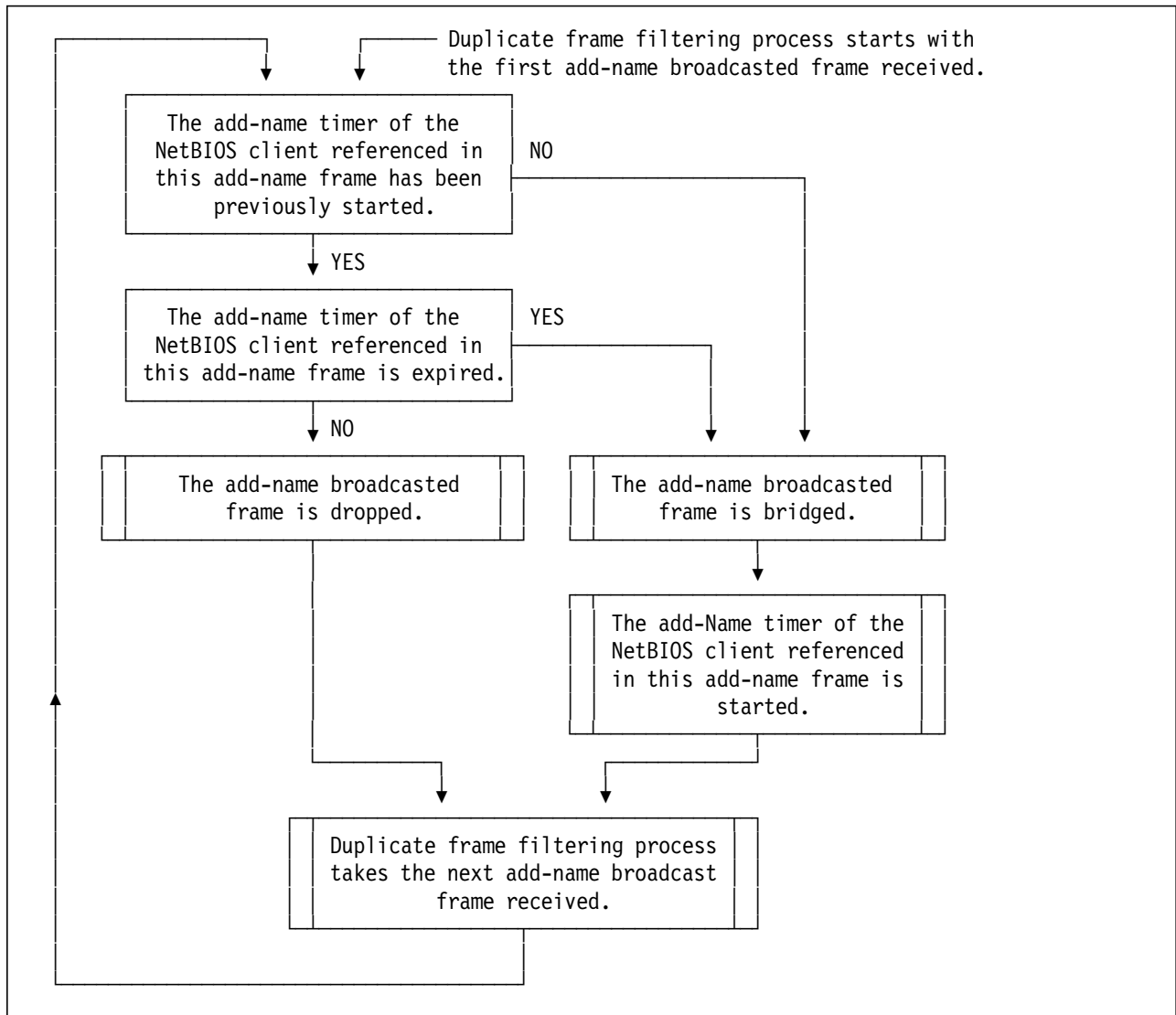


Figure 204. Duplicate Frame Filtering Process for the Add-Name Broadcasted Frames

11.11.1.2 NetBIOS Name Caching Configuration Commands

This section summarizes the configuration commands needed to customize the NetBIOS name caching via the CONFIG process of the Nways MRS, and via the Nways MRS Configuration Program.

Table 76 shows you the commands available on the NetBIOS Name Caching configuration via the Nways MRS on the ASCII Console.

Table 76 (Page 1 of 2). NetBIOS Name Caching Configuration Commands	
Command	Function
? (Help)	Displays the NetBIOS Name Caching process commands or lists subcommand options for specific commands (if available).
Disable	Disables the Name Caching process or Duplicate Frame Filtering process.
Enable	Enables the Name Caching process or Duplicate Frame Filtering process at bridge level.

<i>Table 76 (Page 2 of 2). NetBIOS Name Caching Configuration Commands</i>	
Command	Function
Port	Selects a specific port (token-ring or PPP link ports only) in order to enable or disable the Name Caching process or Duplicate Frame Filtering process at port level.
List	Displays present configuration settings of the NetBIOS Name Caching facility.
Timer	Sets the entry idle timer, the server timer or the time within.
Exit	Exits the NetBIOS Name Caching configuration process and returns to the CONFIG process.

To access the NetBIOS Name Caching facility from the CONFIG process of the IBM 2210, you must first access the Bridge protocol, using the following command:

Config>**protocol asrt**

After issuing the above command, the following prompt will be displayed:

ASRT config>

You can now access the NetBIOS Name Caching facility, using the following command:

ASRT config>**name-caching**

After issuing the above command, the following prompt will be displayed:

Name Cache Config>

For the Nways MRS Configuration Program, all of the NetBIOS Name Caching facility customization is in the NetBIOS Name Caching window. To access it, select the Name Caching panel within the NetBIOS subdirectory of the Bridging directory.

The NetBIOS Name Caching facility contains two separate processes:

- Name Caching process
- Duplicate Frame Filtering process.

The following sections describe the commands for these two processes.

Name Caching Process Configuration Command:

- To enable the Name Caching process at the bridge level, issue the following command:

Name Cache Config>**enable name_caching**

Note that the Name Caching process at bridge level is enabled by default.

For the Nways MRS Configuration Program, use the NetBIOS Name Caching window.

- You can also enable the Name Caching process at a port level. For example to enable Name Caching on bridge port 1, issue the following commands:

```
Name Cache Config>port 1
Name Cache Port Config>enable name_caching
Name Cache Port Config>exit
Name Cache Config>
```

Note that Name Caching process at port level is enabled by default.

- To list the Name Caching process of port 1, issue the following commands:

```
Name Cache Config>port 1
Name Cache Port Config>list

Server name caching:      Enabled
Add name frame filtering: Enabled
```

```
Name Cache Port Config>exit
Name Cache Config>
```

Note

Because the NetBIOS Name Caching facility applies to token-ring and PPP serial port only, you cannot issue a Port command against another type of port.

For the Nways MRS Configuration Program, enabling the Name Caching process at the port level is not supported. You must do it via the Nways MRS on an ASCII Console.

- You can set the idle-timer for the Name Caching database entry. For example, to set the idle-timer to 600 seconds, issue the following command:

```
Name Cache Config>timer entry 600
```

The time, specified in seconds, must be in the range from 10 to 65535.

Note: The default for the idle-timer is 900 seconds.

For the Nways MRS Configuration Program, use the NetBIOS Name Caching window.

- You can set the server-timer used in the Name Caching database. For example, To set the server-timer to 5, issue the following command:

```
Name Cache Config>timer server_response 5
```

The time is specified in seconds and must be in the range from 1 to 16.

Note: The default value for the server-timer is 3 seconds.

For the Nways MRS Configuration Program, use the NetBIOS Name Caching window.

- You can list configuration of the Name Caching parameters by using the List command.

Duplicate Frame Filtering Process Configuration Command:

- To enable the Duplicate Frame Filtering process at the box level, issue the following command:

```
Name Cache Config>enable add_name_filtering
```

Note that the Duplicate Frame Filtering process at the box level is enabled by default.

For the Nways MRS Configuration Program, use the NetBIOS Name Caching window.

- You can also enable the Duplicate Frame Filtering process at a port level. For example to enable Duplicate Frame Filtering on the bridged port 1, issue the following commands:

```
Name Cache Config>port 1
Name Cache Port Config>enable add_name_filtering
Name Cache Port Config>exit
Name Cache Config>
```

Note that Duplicate Frame Filtering process at port level is enabled by default.

To list the Duplicate Frame Filtering process of port 1, issue the following commands:

```
Name Cache Config>port 1
Name Cache Port Config>list

Server name caching:      Enabled
Add name frame filtering: Enabled
```

```
Name Cache Port Config>exit
Name Cache Config>
```

Note

Because the NetBIOS Name Caching facility applies to token-ring and PPP serial ports only, you cannot issue a Port command against another type of port.

For the Nways MRS Configuration Program, enabling the Duplicate Frame Filtering process at port level is not supported. You must do it via Nways MRS on an ASCII Console.

- You can set the timer used for name-query, add-name and add-name-group broadcast frames. For example, to set this timer for the add-name frames to 10, issue the following command:

```
Name Cache Config>timer add_name 10
```

The time specified is in seconds and must be in the range from 1 to 32.

Note: The default value for all the timers is 7 seconds.

For the Nways MRS Configuration Program, use the NetBIOS Name Caching window.

- You can list the configuration of the Duplicate Frame Filtering process using the List command.

11.11.1.3 Scenario of NetBIOS Name Caching Implementation

For an example of the NetBIOS Name Caching and Duplicate Frame Filtering implementation, please refer to 4.4.6, "Scenario 6: SR-TB Implementation with NetBIOS Facilities" on page 209. In this scenario, 2210A has been configured to perform both NetBIOS name caching and duplicate frame filtering.

11.11.2 NetBIOS Filtering Facility

This section provides a brief description of the main commands needed to configure NetBIOS Filtering. An example of the NetBIOS Filtering implementation is also provided.

11.11.2.1 Introduction to the NetBIOS Filtering Facility

The NetBIOS Filtering facility allows you to specify filters to be applied during the bridging process. These filters are based on either the NetBIOS host name or on any bytes contained in the NetBIOS header frame.

The filters can be applied to one or more interfaces in either direction (INPUT or OUTPUT).

The action of a filter could be:

- INCLUDE

This means that the packets will be forwarded by the bridge function.

- EXCLUDE

This means that the packets will be discarded by the bridging function and will not be forwarded to the destination.

Figure 205 provides an overview of the NetBIOS Filtering.

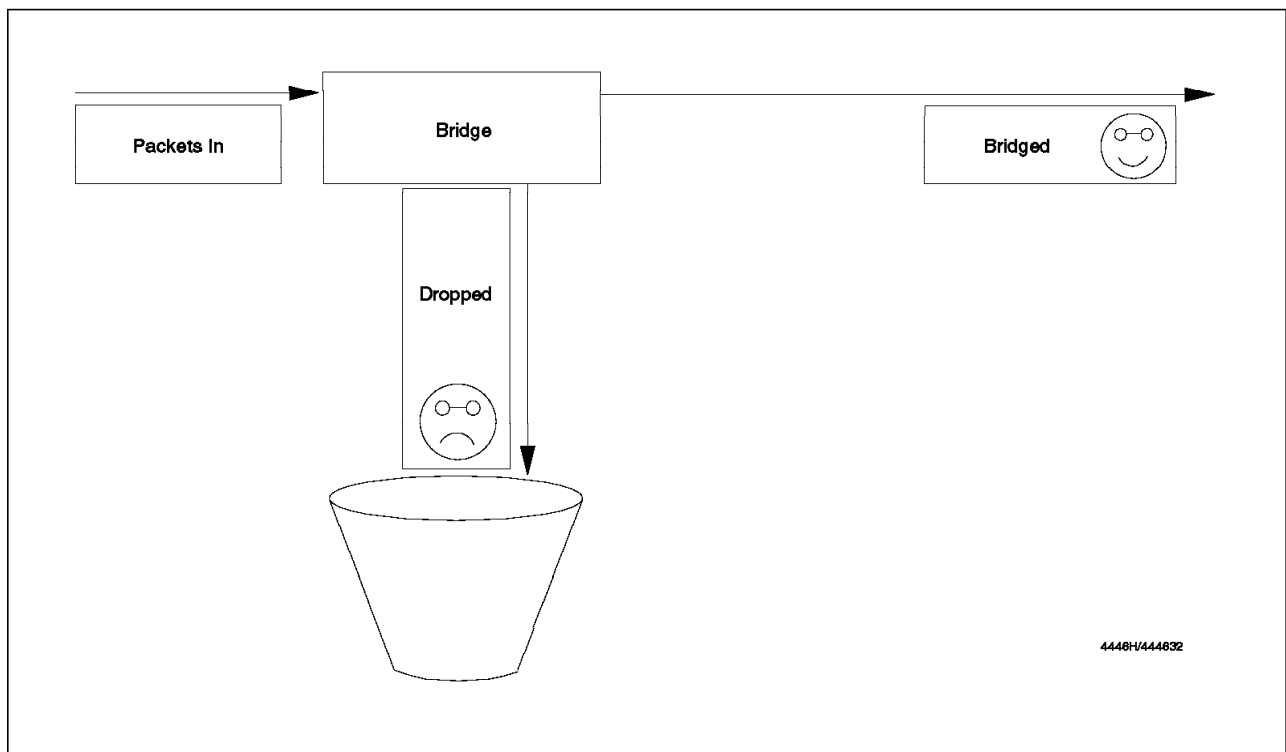


Figure 205. Actions Performed by NetBIOS Filtering Feature

The following is a description of the terminology used in the NetBIOS filtering:

- A NetBIOS *host name* filter will be compared against the following:
 - source NetBIOS name field of add-group-name-query packets
 - Source NetBIOS name field of add-name-query packets

- Destination NetBIOS name field of name-query packets
- Destination NetBIOS name field of datagram packets
- A NetBIOS *byte filter* will be compared against all NetBIOS packets.
- A NetBIOS *host name* is called a *host-name filter-item*.
- A *host-name filter-list* is a group of one or more *host-name filter-items*.
- A specific byte string to be compared to the contents of the NetBIOS header of the NetBIOS packets is called a *byte filter-item*.
- A *byte filter-list* is a group of one or more *byte filter-items*.

Note

In the following discussion, when references are made to filter-items, they apply to both host name and byte filter-items. Also, when references are made to filter-lists, they apply to both host name and byte filter-lists.

- A filter-list is attached to one or more *filters*.
- A *filter* is the combination of the following parameters:
 - The interface number
 - The traffic direction (Input or Output)

You can assign one filter-list or a unique Boolean combination of filter-lists to a filter.

This unique Boolean combination is a string of several filter-lists joined with two kinds of Boolean operator:

For example: filter-list1 AND filter-list2 OR filter-list3 is a unique Boolean combination.

Note: The filter-lists combinations should be read from left to right.

A filter-list can be applied to more than one filter.

For a specific NetBIOS packet, each filter-list provides an action. This can be either the the action of the filter-item matching the contents of the NetBIOS packet, or the default action of the filter-list if there is no matching filter-item in the filter-list.

For a specific filter-list, this resulting action can be Exclude or Include depending on the configuration of the filter-list and the contents of the NetBIOS packet.

The order of the filter-items in a filter-list is very important as described below:

- The NetBIOS Filtering facility compares the NetBIOS packet filter-item number 1 in the filter-list.
- If there is no match, the next filter-item in this filter-list is used. This process continues until the highest filter-item is checked or a match is found.
- As soon as a filter-item of the filter-list matches the NetBIOS packet, the action specified for that filter-item is performed.

Note: There will be no more checking performed for this packet.

- If no filter-item of this filter list matches the NetBIOS packet, the default action for the filter-list will be performed on the NetBIOS packets.

Figure 206 shows the NetBIOS Filtering process for a host-name filter-list.

The same process occurs for bytes-filter-list.

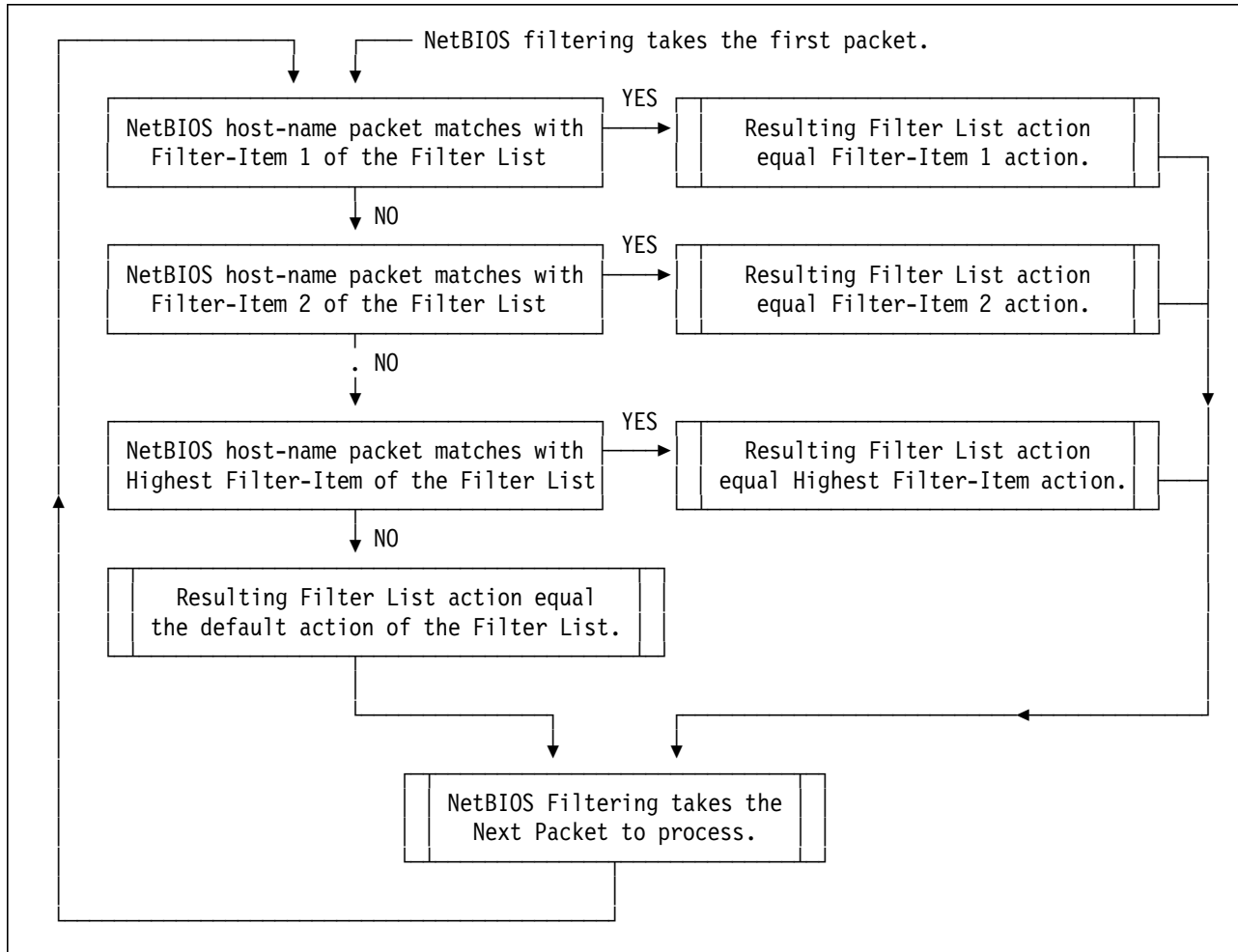


Figure 206. NetBIOS Filtering Process of a Host Name Filter List

When you assign a combination of filter-lists to a filter, you must calculate the resulting action performed by the filter while considering the following:

- Inclusive action is a true Boolean value.
- Exclusive action is a false Boolean value.

Then the action performed on the packet by this filter is the result of the Boolean operation of the filter-lists combination considering each of the resulting filter-list actions for each filter-list of this combination. For example, we have the following combination of the filter-lists attached to a filter:

filter-list1 AND filter-list2 OR filter-list3

The NetBIOS Filtering calculates the resulting filter-list action of each filter-list individually, as shown in Figure 206. Then it performs the Boolean operation (from left to right) as follows:

- Resulting action of filter-list1 AND

- Resulting action of filter-list2 OR
- Resulting filter list action of filter-list3

Then the actual action performed on the packet by the filter on which this filter-list combination is attached to is:

- Include - If the result of this Boolean operation is true
- Exclude - If the result of this Boolean operation is false

11.11.2.2 NetBIOS Filtering Configuration Commands

This section summarizes the NetBIOS filtering configuration commands available within the CONFIG process of the Nways MRS and within Nways MRS Configuration Program.

To access the NetBIOS Filtering Facility from the CONFIG process of the IBM 2210, you must first access the bridge protocol using the following command:

Config>**protocol asrt**

After issuing the above command, the following prompt will be displayed:

ASRT config>

Now, you can access the NetBIOS Filtering facility by using the following command:

ASRT config>**netbios-filtering**

After issuing the above command, the following prompt will be displayed:

NETBIOS Filter config>

First of all, you must enable the NetBIOS filtering. This is done by issuing the following command:

NETBIOS Filter config>**enable netbios-fitering**

For the Nways MRS Configuration Program, the four NetBIOS Filtering facility panels are in the Filtering subdirectory within the NetBIOS subdirectory of the Bridging directory.

Table 77 on page 727 shows the available NetBIOS filtering commands. Table 78 on page 727 shows the available NetBIOS filtering Update subcommands.

The *Nways MRS Software User's Guide* covers these commands in detail.

Table 77. NetBIOS Filtering Configuration Commands	
Command	Function
? (Help)	Displays the NetBIOS filtering configuration commands, or lists the options associated with specific commands.
Create	Creates a <i>byte filter-list</i> or a <i>host name filter-list</i> .
Delete	Deletes a <i>byte or host name filter-list</i> with all its <i>filter-items</i> . Also deletes a <i>filter</i> .
Disable	Disables NetBIOS Filtering facility.
Enable	Enables NetBIOS Filtering facility.
Filter-on	Assigns a <i>filter-list</i> or a combination of <i>filter-lists</i> to a <i>filter</i> . This <i>filter</i> is either Input or Output traffic of the specified interface.
List	Displays all information about <i>filter-lists</i> and <i>filters</i> configured by the user.
Update	Updates information for a specific filter-list. It brings you to a new prompt with a new menu of appropriate subcommands. Table 78 shows you these new subcommands.
Exit	Exits the NetBIOS filtering configuration environment and returns to the ASRT protocol process.

Table 78. NetBIOS Filtering Update Subcommands	
Command	Function
? (Help)	Displays all of the Update subcommands.
Add	Adds byte or host name filter-item to a filter-list. The value specified in the filter-item will be compared against NetBIOS packets.
Default	Sets the default action for a filter-list either to Include or Exclude.
Delete	Deletes a filter-item from a filter-list.
List	Lists all the filter-items configured by the user for a filter-list.
Move	Reorders the filter-items attached to a filter-list.
Exit	Exits the NetBIOS filtering update subcommands environment and returns to NetBIOS Filtering commands.

In the following sections, we describe the configuration steps required for:

1. Configuring NetBIOS host name filters
2. Configuring NetBIOS byte filters
3. Configuring the common options applicable to both NetBIOS host name filter and byte filter

Configuration Commands for NetBIOS Host Name Filters: The following section explains the specific commands used to configure a NetBIOS host name filter. To discuss these commands, we show the steps required to exclude packets with the NetBIOS host name of ROMEO in Input traffic of the token-ring interface 0:

1. Create a host-name filter-list with a name Mylist. This is done by using the following command:

```
NETBIOS Filter config>create name-filter-list mylist
```

For the Nways MRS Configuration Program, use the General panel within the Name Lists subdirectory of the NetBIOS Filtering directory.

2. To configure this filter-list, you must use the Update command as follows:

```
NETBIOS Filter config>update mylist
```

After issuing the above command, the following prompt will be displayed:

```
NETBIOS Name mylist config>
```

3. Add filters-items to the filter-list. This is done using the Add command, which adds NetBIOS host names you want to filter.

For example, to add a filter-item that discards bridged packets that contain the NetBIOS host name, issue the following command:

```
NETBIOS Name mylist config>add exclusive ascii romeo
```

Note that the ASCII parameter allows you to type the host name in ASCII format. The other option is HEX.

The host name could be up to 16 ASCII characters (32 hexadecimal values), and can contain two kinds of wildcard characters:

- ? - for a single ASCII character or hexadecimal digit.
- * - the final character of the hostname as a wildcard for the remainder of the host name up to the 16th ASCII character or 32nd hexadecimal value.

If the host name length is less than 16 ASCII characters (or 32 hexadecimal values) and does not contain an "*" wildcard at the end, the remainder of the host name is padded with ASCII spaces until the 15th character (30th hexadecimal value) and a "?" wildcard is assumed for the 16th character (31st and 32nd hexadecimal value).

For the Nways MRS Configuration Program, use the Name List panel of the Name Lists subdirectory of the NetBIOS Filtering directory.

4. Set the default action for this filter-list. This action will be performed if no filter-item of this filter-list matches the NetBIOS packet. You can do this by using the Action command. The specified action can be either of the following:

- Include
- Exclude

To set the Include default action for mylist, issue the following command:

```
NETBIOS Name mylist config>action include
```

For the Nways MRS Configuration Program, see the General subpanel of the Name List panel of the Name Lists subdirectory of the NetBIOS Filtering directory.

5. All the filter-items in the mylist filter-list can be displayed using the following command:

```
NETBIOS Name mylist config>list
```

6. Exit the update subcommand configuration process using the following command:

```
NETBIOS Name mylist config>exit
```

The new prompt will be:

```
NETBIOS Filter config>
```

To complete your NetBIOS host name filter customization, you must issue commands that are common to both the NetBIOS host name and byte filter as

discussed in “Common NetBIOS Filtering Configuration Commands” on page 730.

NetBIOS Filtering Configuration Commands for NetBIOS Byte: The following section explains the specific commands used to configure a NetBIOS byte filter. To discuss these commands, we will show the steps required to include packets with hexadecimal bytes of 414243 at the offset 8 of the NetBIOS header, in input traffic of the token-ring interface 0:

1. Create a byte-filter-list with the name mylist. This is done by using the following command:

```
NETBIOS Filter config>create byte-filter-list mylist
```

For the Nways MRS Configuration Program, use the General panel within the Byte Lists subdirectory of the NetBIOS Filtering directory.

2. To configure this filter-list, you must use the Update as follows:

```
NETBIOS Filter config>update mylist
```

After issuing the above command, the following prompt will be displayed:

```
NETBIOS Byte mylist config>
```

3. Add filter-items to the filter-list. This is done using the Add command which adds NetBIOS bytes you want to filter.

For example, to add a filter-item that bridges NetBIOS packets with hexadecimal bytes of 414243 at the offset 8 of the NetBIOS header, issue the following command:

```
NETBIOS Byte mylist config>add inclusive 8 414243 fffffff
```

The 8 value is a decimal offset starting at the beginning of the NetBIOS header. The 414243 value is called a hexadecimal pattern value. This pattern value must contain an even number of hexadecimal digits. Its length cannot exceed 32 hexadecimal digits. The fffffff value is called the hexadecimal mask value. Both the pattern value and mask value must have the same length.

The hexadecimal mask value works as follows:

- The comparison between the bytes into the bridged packet, and the pattern value customized in this filter-item will be done only on bits set to B'1' in the hexadecimal mask value.

For example, to ignore the contents of the second byte within the customized pattern value, you should enter the following command:

```
NETBIOS Byte mylist config>add inclusive 8 410043 ff00ff
```

For the Nways MRS Configuration Program, use the Byte List panel within the Byte Lists subdirectory of the NetBIOS Filtering directory.

4. Set the default action for this filter-list. This action will be performed if no filter-item of this filter-list matches the NetBIOS packet. You can do this by using the Action command. The specified action can be either of the following:

- Include
- Exclude

For example, to set the Exclude default action for mylist, issue the following command:

NETBIOS Byte mylist config>**action exclude**

For the Nways MRS Configuration Program, see the General subpanel within the Byte List panel of the Byte Lists subdirectory of the NetBIOS Filtering directory.

5. All the filter-items of the mylist filter-list can be displayed using the following command:

NETBIOS Byte mylist config>**list**

6. Exit the update subcommand configuration process by using the following command:

NETBIOS Byte mylist config>**exit**

The new prompt will be:

NETBIOS Filter config>

Common NetBIOS Filtering Configuration Commands: The following is the description of the common steps and commands required to configure both NetBIOS host names and byte filters.

- Attach your filter-list or a unique combination of filter-lists to a filter.

A filter-list can be attached to one or more filters at the same time.

To attach the filter-list called mylist to the input traffic filter of the token-ring interface, issue the following command:

NETBIOS Filter config>**filter-on input 1 mylist**

To specify a combination of filter-lists attached to the same filter, issue the following command:

NETBIOS Filter config>**filter-on input 1 mylist1 AND mylist2 OR mylist3**

Note: The Boolean operators must be entered in uppercase.

In the same filter-lists combination, you can mix NetBIOS host name filter-lists and NetBIOS byte filter-lists.

- When a filter-list or a combination of filter-lists is attached to a filter, you cannot issue another Filter-on command for the same filter before deleting this filter with the Delete command. For example, to delete the filter of INPUT traffic on interface 0 (token-ring), issue the following command:

NETBIOS Filter config>**delete input 0**

For the Nways MRS Configuration Program, the six possible filters are in the MAC Interfaces window. In this window select the corresponding filter and attach it to a defined filter-list (or a combination of filter-lists).

- All of the NetBIOS Filtering configurations can be listed by using the following command:

NETBIOS Filter config>**list**

- Exit the NetBIOS Filtering facility configuration process and go back to ASRT protocol process using the following command:

NETBIOS Filter config>**exit**

The new prompt will be:

ASRT config>

11.11.2.3 Scenario of NetBIOS Filtering Implementation

To see an example of NetBIOS Filtering implementation refer to 4.4.6, “Scenario 6: SR-TB Implementation with NetBIOS Facilities” on page 209. In this scenario, 2210A has been configured to use the NetBIOS filtering facility. In this scenario both NetBIOS host name filters and NetBIOS byte filters have been implemented.

11.12 Data Compression for PPP Interface

This section discusses data compression on the router at PPP interfaces. It includes these sections:

- Introduction to Data Compression
- Data Compression Configuring Commands

11.12.1 Introduction to Data Compression

Data compression lets the router software pack more user data into the packets that are moving through router interfaces. If the rate of packet transfer stays constant, the data transfer rate (throughput) for the router increases proportionately.

In general, data compression is much more effective when used in conjunction with lower speed WAN interfaces, for example, less than 64 Kbps. As you increase the WAN data rate, the effective improvement in the overall bandwidth utilization diminishes. If the link data rate is sufficiently high, enabling compression decreases router performance and throughput.

The router supports data compression on PPP serial and dial circuit interfaces. The router implements data compression on a per-interface basis for each of the router's PPP interfaces. PPP data compression is supported on PPP serial line interfaces, as well as PPP dial circuits, that are mapped to V.25bis or ISDN interfaces. You enter data compression commands at the PPP> interface along with the other commands to configure and monitor PPP.

To implement data compression, you can select one of the following protocols:

- Compression Control Protocol (CCP)
- Link Control Protocol (LCP) compression options
- Bridging Control Protocol (BCP) Tinygram compression
- IP Control Protocol (IPCP)-Van Jacobson compression of IP header

11.12.1.1 Compression Control Protocol (CCP)

The router uses this protocol to negotiate the choice of a compression algorithm with the other router on the link.

CCP is an Internet Engineering Task Force (IETF) draft protocol.

11.12.1.2 Link Control Protocol (LCP)

PPP's Link Control Protocol (LCP) establishes, configures, maintains, and terminates the point-to-point link.

11.12.1.3 Bridging Control Protocol (BCP)

BCP is specified in RFC 1220. IBM's implementation of BCP supports IEEE 802.5 Line Identification Option and the Tinygram Compression Option.

11.12.1.4 IP Control Protocol (IPCP)

IPCP is specified in RFC 1332. IBM's implementation supports the IPCP options.

- IP Compression Protocol

The only IP compression protocol supported is the Van Jacobson compression protocol as described in RFC 1144.

- IP Address

The router can query the remote end for its IP address and can supply its own address to the peer. The router does not support dynamic assignment of IP addresses. It neither assigns an address to a remote unit that requests one, nor accepts a request from the peer to change its own port address.

The *Nways MRS Software User's Guide* covers the information about the data compression in detail.

11.12.2 Data Compression Configuring Commands

This section summarizes the Data Compression commands available at the PPP configuration prompt (PPP config>).

Table 79. Data Compression Configuration Commands	
Data Compression Command	Action
? (Help)	Displays the data compression configuration commands, or lists the subcommand options for specific commands (if available).
disable ccp	Disables data compression.
enable ccp	Enables data compression.
list ccp	Displays CCP options.
set ccp options	Sets CCP options.
set lcp options	Sets LCP options. In this option, you can configure the Protocol Field Compression (PFC) and the Addr/Cntl Field Compression (ACFC).
set lcp parameters	Sets LCP parameters.
list lcp	Displays LCP parameters, LCP options and Authentication options.
set bcp options	Sets BCP options. In this option, you can configure the Tinygram compression.
list bcp	Displays BCP options.
set ipcp options	Sets IPCP options. In this option, you can configure the IP compression (Van Jacobson).
list ipcp	Displays IPCP options.
Exit	Exits the PPP configuration environment and returns to the CONFIG process.

Note:

1. The default for data compression is no data compression.
2. You cannot use Quick CONFIG to enable or disable data compression.

11.12.3 Scenario 9: PPP Data Compression with Bridging

In this scenario, we have a 2210 with a token-ring interface (2210A) and a 2210 with an Ethernet interface (2210B). Both 2210s are linked together using a PPP link with RS-232 modems.

The 2210A is a source route-translational bridge. 2210B is a transparent bridge.

- Interfaces:

2210A token-ring runs at 16 Mbps, and is attached to the LAN using the STP connector.

2210B Ethernet is attached to the Ethernet LAN using the 10Base-T connector.

- Bridging:

2210A is a source route-translational bridge with SRB on the token-ring interface, and STB on the serial 1 interface. The bridge number of 2210A is A. The LAN segment number of the 2210A on the token-ring is 111, and the TB-Domain is seen from SRB Domain as the LAN segment number 222.

2210B is a transparent bridge with STB on both serial 1 and Ethernet interfaces.

- PPP Data Compression: CCP, PFC, ACFC, Tinygram Compression and IPCP Compression enabled on PPP interfaces of both routers. We tried PING and file transfer using TFTP through the PPP link.

In the testing of this scenario:

- OS2PING and TFTP were successful between end user A and B.
- The data transfer rate of OS2PING and TFTP using PPP data compression were better than OS2PING and TFTP without PPP data compression.

Table 80. PPP Data Compression Results in This scenario

Method	Without Compression	Using Compression
OS2PING Response	110 msec.	65 msec.
TFTP	11.7K bps	15.5K bps

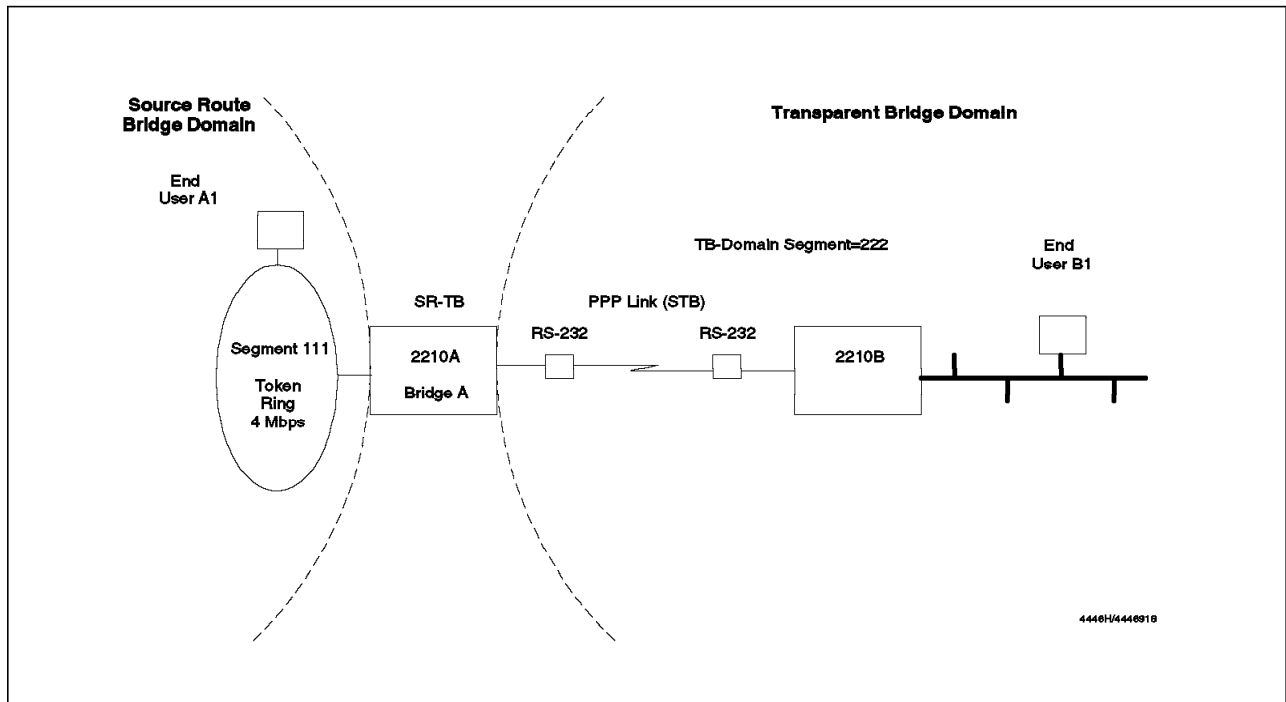


Figure 207. Scenario 9: PPP Data Compression

```

*
*talk 6      1
Gateway user configuration
Config>network 0      2
Token-Ring interface configuration
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    16 Mb/sec
Media:                    Shielded

RIF Aging Timer:         120
Source Routing:          Enabled
MAC Address:              000000000000
IPX interface configuration record missing

TKR config>exit
Config>network 1      3
Point-to-Point user configuration
PPP Config>set hdlc cable rs-232 dte
PPP Config>list hdlc
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Speed (bps): 0

Transmit Delay Counter: 0
Lower DTR: Disabled
PPP Config>exit
Config>list devices      4
Ifc 0   Token Ring                CSR 6000000, vector 28
Ifc 1   WAN PPP                   CSR 81620, CSR2 80D00, vector 93
Ifc 2   WAN PPP                   CSR 81640, CSR2 80E00, vector 92
Ifc 3   ISDN Basic                CSR      0, vector 0
Config>protocol asrt      5
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port 1 2
ASRT config>disable transparent 1
ASRT config>enable source-routing 1
Segment Number for the port in hex(1 - FFF) [1]? 111
Bridge number in hex (1 - 9, A - F) [1]? A
ASRT config>enable sr-tb-conversion
TB-Domain Segment Number in hex(1 - FFF) [1]? 222
TB-Domain's MTU [1470]?

:

```

Figure 208 (Part 1 of 5). Scenario 9: 2210A Configuration via the ASCII Console

```

:
ASRT config>list bridge

                        Source Routing Transparent Bridge Configuration
                        =====

Bridge:                Enabled                Bridge Behavior: SR<=>TB
                        +-----+
                        ] SOURCE ROUTING INFORMATION ]-----+
                        +-----+

Bridge Number:         0A                    Segments:         1
Max ARE Hop Cnt:       14                    Max STE Hop cnt:   14
1:N SRB:               Not Active             Internal Segment:
0x000
LF-bit interpret:      Extended

                        +-----+
                        ] SR-TB INFORMATION ]-----+
                        +-----+

SR-TB Conversion:      Enabled
TB-Virtual Segment:    0x222                MTU of TB-Domain: 1470

                        +-----+
                        ] SPANNING TREE PROTOCOL INFORMATION ]-----+
                        +-----+

Bridge Address:        Default                Bridge Priority: 32768/0x8000
STP Participation:     IEEE802.1d on TB ports, IBM-8209 and IBM-SRB proprietas

                        +-----+
                        ] TRANSLATION INFORMATION ]-----+
                        +-----+

FA<=>GA Conversion:    Enabled                UB-Encapsulation: Disabled
DLS for the bridge:    Disabled

                        +-----+
                        ] PORT INFORMATION ]-----+
                        +-----+

Number of ports added: 2
Port:  1      Interface:  0      Behavior:  SRB Only  STP: Enabled
Port:  2      Interface:  1      Behavior:  STB Only  STP: Enabled

ASRT config>exit
Config>network 1 6
Point-to-Point user configuration
PPP Config>list all 7
Encoding: NRZ
Idle State: Flag
Clocking: Internal
Cable type: RS-232 DCE
Speed (bps): 64000

Transmit Delay Counter: 0
Lower DTR: Disabled

:

```

Figure 208 (Part 2 of 5). Scenario 9: 2210A Configuration via the ASCII Console

```

:
LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):       No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
Authenticate remote using: none
Identify self as:              ibm

NCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:          Disabled

IPCP Options
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>enable ccp          8
PPP Config>list ccp            9

CCP Options
-----
Data Compression enabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ
PPP Config>set lcp options      10
Maximum Receive Unit (bytes) [2048]?
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) -A0000?
Protocol Field Compression(PFC) [no]: y      11
Addr/Cntl Field Compression(ACFC) [no]: y     12

:

```

Figure 208 (Part 3 of 5). Scenario 9: 2210A Configuration via the ASCII Console


```

:
PPP Config>list lcp 13

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:              Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):      Yes   Addr/Cntl Field Comp(ACFC): Yes

Authentication Options
-----
Authenticate remote using: none
Identify self as:              ibm
PPP Config>set bcp options 14
TINYGRAM COMPRESSION [no]: y 15
PPP Config>list bcp 16

BCP Options
-----
Tinygram Compression:          Enabled
PPP Config>set ipcp options 17
IP COMPRESSION [no]: y 18
Send our IP address [no]: n
Request their IP address [no]: n
PPP Config>list ipcp 19

IPCP Options
-----
IPCP Compression:              Van Jacobson   Compression Slots:          16
IP Address:                    Don't Send or Request

PPP Config>exit
Config>Ctrl+p
*restart 20
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*

:

```

Figure 208 (Part 4 of 5). Scenario 9: 2210A Configuration via the ASCII Console

:
*t 5 21

CGW Operator Console

+network 1

Point-to-Point Console

PPP>list ccp

CCP Statistic	In	Out
-----	--	---
Packets:	2	2
Octets:	18	18
Reset Reqs:	0	0
Reset Acks:	0	0
Prot Rejects:	0	-

PPP>list cdp

Compression Statistic	In	Out
-----	--	---
Packets:	65	2
Octets:	2275	12
Compressed Octets:	1407	20
Incompressible Packets:	0	0
Discarded Packets:	0	0
Prot Rejects:	0	-

Compressor (transmit) statistics:

Recent compression ratio: 0.4:1

Decompressor (receive) statistics:

Recent compression ratio: 1.6:1

PPP>list control ccp

CCP State: Open
Previous State: Ack Sent
Time Since Change: 11 minutes and 0 seconds

Compressor: STAC-LZS histories 1, check_mode SEQ

Decompressor: STAC-LZS histories 1, check_mode SEQ

Max size of compression dictionary: 12494.

Max size of decompression dictionary: 4424.

PPP>exit

+Ctrl+p

*

Figure 208 (Part 5 of 5). Scenario 9: 2210A Configuration via the ASCII Console

Notes:

1 Talk to the CONFIG process.

2 Customization of network 0. This is the token-ring interface. Specify the unshielded media connector (UTP) and the locally administered address for this interface.

- 3** Customization of network 1. This is the serial 1 interface. Specify the RS-232 DTE cable that is used.
- 4** List the devices (interfaces) configuration.
- 5** Customization of the bridging function. Customize a source route-translational bridge with SRB for the token-ring interface and STB for serial 1 interface. Assign the LAN segment numbers and bridge number.
- 6** Access the PPP configuration.
- 7** List the PPP configuration.
- 8** Enable CCP.
- 9** List the CCP Options.
- 10** Set the LCP Options.
- 11** Enable the Protocol Field Compression(PFC).
- 12** Enable the Addr/Cntl Field Compression(ACFC).
- 13** List the LCP Parameters, the LCP Options and the Authentication Options.
- 14** Set the BCP Options.
- 15** Enable the Tinygram Compression.
- 16** List the BCP Options.
- 17** Set the IPCP Options.
- 18** Enable the IPCP Compression.
- 19** List the IPCP Options.
- 20** Restart the 2210A to get the configuration running.
- 21** Talk to the gateway operator console and access the PPP Compression monitoring to list the actions performed by the compression.

```

*
*talk 6      1

Config>network 0      2
Ethernet interface configuration
ETH config>list
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 1      3
Point-to-Point user configuration
PPP Config>set hdlc cable rs-232 dte
PPP Config>exit
Config>list devices    4
Ifc 0   Ethernet          CSR  81600, CSR2  80C00, vector 94
Ifc 1   WAN PPP           CSR  81620, CSR2  80D00, vector 93
Ifc 2   WAN PPP           CSR  81640, CSR2  80E00, vector 92
Ifc 3   ISDN Basic        CSR      0, vector 0

Config>protocol asrt    5
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port 1 2
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:                Enabled                Bridge Behavior: STB
+-----+
+-----] SOURCE ROUTING INFORMATION ]-----+
+-----+

Bridge Number:          N/A                    Segments:          0
Max ARE Hop Cnt:        00                    Max STE Hop cnt:   00
1&colonN SRB:            Not Active              Internal Segment:
0x000
LF-bit interpret:       Extended
+-----+
+-----] SR-TB INFORMATION ]-----+
+-----+

SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                  MTU of TB-Domain: 0
+-----+
+-----] SPANNING TREE PROTOCOL INFORMATION ]-----+
+-----+

Bridge Address:         Default                Bridge Priority: 32768/0x8000
STP Participation:      IEEE802.1d
+-----+
+-----] TRANSLATION INFORMATION ]-----+
+-----+

FA<=>GA Conversion:     Enabled                UB-Encapsulation: Disabled
DLS for the bridge:     Disabled

:

```

Figure 209 (Part 1 of 5). Scenario 9: 2210B Configuration via the ASCII Console

```

:
+-----+
-----] PORT INFORMATION ]-----
+-----+
Number of ports added: 2
Port: 1      Interface: 0      Behavior: STB Only  STP: Enabled
Port: 2      Interface: 1      Behavior: STB Only  STP: Enabled

ASRT config>exit
Config>network 1 6
Point-to-Point user configuration
PPP Config>list all 7
Encoding: NRZ
Idle State: Flag
Clocking: Internal
Cable type: RS-232 DCE
Speed (bps): 64000

Transmit Delay Counter: 0
Lower DTR: Disabled

LCP Parameters
-----
CONFIG Request Tries:          20  CONFIG Nak Tries:          10
Terminate Tries:              10  Retry Timer:              3000

LCP Options
-----
Max Receive Unit:             2048  Magic Number:             Yes
Peer to Local (RX) ACCM:      A0000
Protocol Field Comp(PFC):     No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
Authenticate remote using: none
Identify self as:             ibm

NCP Parameters
-----
CONFIG Request Tries:          20  CONFIG Nak Tries:          10
Terminate Tries:              10  Retry Timer:              3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

:

```

Figure 209 (Part 2 of 5). Scenario 9: 2210B Configuration via the ASCII Console

```

:

BCP Options
-----
Tinygram Compression:          Disabled

IPCP Options
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>enable ccp          8
PPP Config>list ccp            9

CCP Options
-----
Data Compression enabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ
PPP Config>set lcp options     10
Maximum Receive Unit (bytes) [2048]?
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) [A0000]?
Protocol Field Compression(PFC) [no]: y 11
Addr/Cntl Field Compression(ACFC) [no]: y 12

PPP Config>list lcp           13

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:               10   Retry Timer:            3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:           Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):       Yes   Addr/Cntl Field Comp(ACFC): Yes

Authentication Options
-----
Authenticate remote using: none
Identify self as:              ibm
PPP Config>set bcp options     14
TINYGRAM COMPRESSION [no]: y   15

:

```

Figure 209 (Part 3 of 5). Scenario 9: 2210B Configuration via the ASCII Console

```

:
PPP Config>list bcp      16

BCP Options
-----
Tinygram Compression:      Enabled
PPP Config>set ipcp options  17
IP COMPRESSION [no]: y      18
Send our IP address [no]: n
Request their IP address [no]: n
PPP Config>list ipcp      19

IPCP Options
-----
IPCP Compression:      Van Jacobson      Compression Slots:      16
IP Address:      Don't Send or Request
PPP Config>exit
Config>Ctrl+p
*restart      20
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
*t 5      21

CGW Operator Console

+network 1
Point-to-Point Console
PPP>list ccp

CCP Statistic      In      Out
-----
Packets:      2      2
Octets:      18      18
Reset Reqs:      0      0
Reset Acks:      0      0
Prot Rejects:      0      -
PPP>list cdp

:

```

Figure 209 (Part 4 of 5). Scenario 9: 2210B Configuration via the ASCII Console

```

:
Compression Statistic      In              Out
-----
Packets:                   65              2
Octets:                    2275             12
Compressed Octets:         1407             20
Incompressible Packets:    0              0
Discarded Packets:         0              0
Prot Rejects:              0              -

Compressor (transmit) statistics:
  Recent compression ratio: 0.4:1
Decompressor (receive) statistics:
  Recent compression ratio: 1.6:1
PPP>list control ccp

CCP State:                  Open
Previous State:             Ack Sent
Time Since Change:          11 minutes and 0 seconds

Compressor:  STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ

Max size of compression dictionary: 12494.
Max size of decompression dictionary: 4424.

PPP>exit
+Ctrl+p
*
```

Figure 209 (Part 5 of 5). Scenario 9: 2210B Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Customization of network 0. This is the Ethernet interface. Issue a List command. No changes are made to the default values.
- 3** Customization of network 1. This is the serial 1 interface. Specify the RS-232 DTE cable that is used.
- 4** List the devices (interfaces) configuration.
- 5** Customization of the bridging function. Customize a source route-translational bridge with SRB for the token-ring interface and STB for the serial 1 interface. Assign the LAN segment numbers and bridge number.
- 6** Access the PPP configuration.
- 7** List the PPP configuration.
- 8** Enable CCP.
- 9** List the CCP Options.

- 10** Set the LCP Options.
- 11** Enable the Protocol Field Compression(PFC).
- 12** Enable the Addr/Cntl Field Compression(ACFC).
- 13** List the LCP Parameters, the LCP Options and the Authentication Options.
- 14** Set the BCP Options.
- 15** Enable the Tinygram Compression.
- 16** List the BCP Options.
- 17** Set the IPCP Options.
- 18** Enable the IPCP Compression.
- 19** List the IPCP Options.
- 20** Restart the 2210A to get the configuration running.
- 21** Talk to the gateway operator console and access the PPP Compression monitoring to list the actions performed by the compression.

11.13 PPP Authentication Protocols

This section discusses PPP Authentication Protocols on the router at PPP interfaces. It includes these sections:

- Introduction to PPP Authentication Protocols
- Password Authentication Protocol (PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- PPP Authentication Protocols Configuring Commands

11.13.1 Introduction to PPP Authentication Protocols

PPP Authentication Protocols provide a form of security between two nodes connected via a PPP link. If authentication is required on a box, then immediately after the two boxes successfully negotiate the use of the link at the LCP layer (LCP packets are exchanged until LCP goes into an "open" state), they go into an "authentication" phase where they exchange authentication packets. A box is neither able to carry network data packets nor negotiate the use of a network protocol (NCP traffic) until authentication negotiations have been completed.

There are different authentication protocols in use, PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol). These are described in detail in RFC 1334, and briefly described later in this section.

Whether a box requires the other end to authenticate itself (and if so, with what protocol) is determined during the LCP negotiation phase. Hence, in some sense authentication can be considered to "fail" even at the link establishment

phase (LCP negotiation), if one end does not know how, or refuses, to use the authentication protocol that the other end requires.

Each end of a link sets its own requirements for how it wants the other end to authenticate itself. For example, given two routers A and B connected over a PPP link, side A may require that B authenticate itself by using PAP, and side B may require that A similarly identify itself by using CHAP. It is valid for one end to require authentication while the other end requires none.

In addition to initial authentication during link establishment, with some protocols an authenticator may demand that the peer re-establish its credentials periodically. With CHAP, for example, a rechallenge may be issued at any time by the authenticator and the peer must successfully reply or lose the link. If more than one authentication protocol is enabled, the router initially attempts to use them in priority order:

1. CHAP
2. PAP

11.13.2 Password Authentication Protocol (PAP)

The Password Authentication Protocol (PAP) provides a simple method for the peer to establish its identity using a two-way handshake. This is done only upon initial link establishment. Following link establishment, the peer sends an ID/password pair to the authenticator until authentication is acknowledged or the connection is terminated. Passwords are sent over the circuit "in the clear", and there is no protection from playback or repeated trial-and-error attacks. The peer controls the frequency and timing of the attempts.

11.13.3 Challenge-Handshake Authentication Protocol (CHAP)

The Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a three-way handshake. This is done upon initial link establishment, and may be repeated anytime after the link has been established. After the initial link establishment, the authenticator sends a "challenge" message to the peer. The peer responds with a value calculated using a "one-way hash" function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection is terminated.

The *Nways MRS Software User's Guide* covers the information about the PPP Authentication Protocols in detail.

11.13.4 PPP Authentication Protocols Configuration Commands

This section summarizes the PPP Authentication Protocols configuration commands available at the PPP configuration prompt (PPP config>).

Table 81 (Page 1 of 2). PPP Authentication Protocols Configuration Commands	
PPP Authentication Command	Action
? (Help)	Displays the PPP Authentication configuration commands, or lists the subcommand options for specific commands (if available).
disable pap	Disables PAP.
enable pap	Enables PAP.

<i>Table 81 (Page 2 of 2). PPP Authentication Protocols Configuration Commands</i>	
PPP Authentication Command	Action
disable chap	Disables CHAP.
enable chap	Enables CHAP.
list lcp	Displays LCP parameters, LCP options and Authentication options. In Authentication options, you can see the status of PAP or CHAP.
set name	Sets PPP local name and password.
Exit	Exits the PPP configuration environment and returns to the CONFIG process.

11.13.5 Scenario 10: PPP Authentication Protocol with Bridging

In this scenario, we have a 2210 with a token-ring interface (2210A) and a 2210 with an Ethernet interface (2210B). Both 2210s are linked together using a PPP link with RS-232 modems.

The 2210A is a source route-translational bridge. The 2210B is a transparent bridge.

- Interfaces:

2210A token-ring runs at 16 Mbps, and is attached to the LAN using the STP connector.

2210B Ethernet is attached to the Ethernet LAN using the 10Base-T connector.

- Bridging:

2210A is a source route-translational bridge with SRB on the token-ring interface, and STB on the serial 1 interface. The bridge number of 2210A is A. The LAN segment number of the 2210A on the token-ring is 111, and the TB domain is seen from SRB Domain as the LAN segment number 222.

2210B is a transparent bridge with STB on both serial 1 and Ethernet interfaces.

- PPP Authentication Protocol:

2210A is configured to authenticate the remote router with the following configuration:

Authenticate Protocol: PAP

PPP_USER: 2210B

Password: remote

2210B is configured to identify itself on the link when being authenticated by 2210A as shown in the following configuration:

Local name: 2210B

Password: remote

In testing this scenario, PING between end user A and end user B is successful.

If the local name or password on the 2210B does not match PPP_USER on the 2210A, PPP link cannot be connected between 2210A and 2210B.

For example:

2210A:

Authenticate Protocol: PAP

PPP_USER: 2210B

Password: remote

2210B:

Local name: 2210B

Password: local

Note: If you want both sides to request authentication to each other, you must enable PAP or CHAP on both sides.

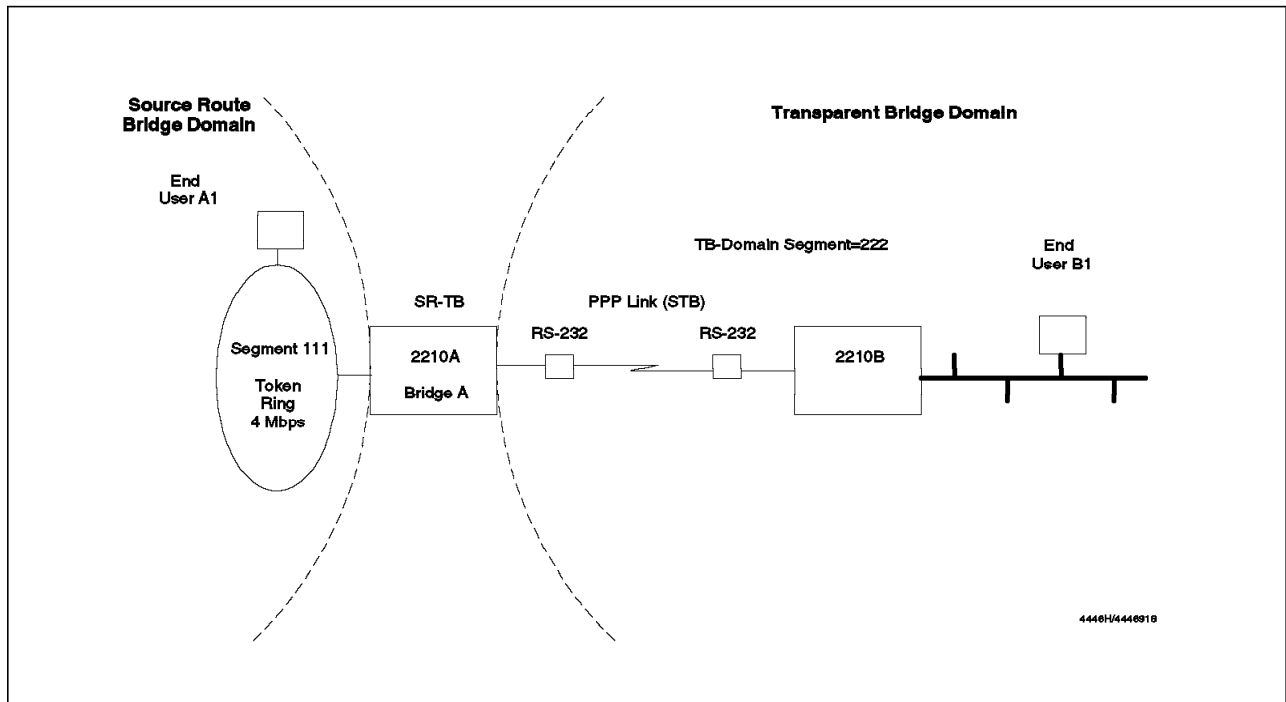


Figure 210. Scenario 10: PPP Authentication Protocol

```

*
*talk 6 1
Gateway user configuration
Config>network 0 2
Token-Ring interface configuration
TKR config>list
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                16 Mb/sec
Media:                Shielded

RIF Aging Timer:      120
Source Routing:       Enabled
MAC Address:          000000000000
IPX interface configuration record missing

TKR config>exit
Config>network 1 3
Point-to-Point user configuration
PPP Config>set hdlc cable rs-232 dte
PPP Config>list hdlc
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Speed (bps): 0

Transmit Delay Counter: 0
Lower DTR: Disabled
PPP Config>exit
Config>list devices 4
Ifc 0   Token Ring                CSR 6000000, vector 28
Ifc 1   WAN PPP                   CSR 81620, CSR2 80D00, vector 93
Ifc 2   WAN PPP                   CSR 81640, CSR2 80E00, vector 92
Ifc 3   ISDN Basic                CSR 0, vector 0
Config>protocol asrt 5
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port 1 2
ASRT config>disable transparent 1
ASRT config>enable source-routing 1
Segment Number for the port in hex(1 - FFF) [1]? 111
Bridge number in hex (1 - 9, A - F) [1]? A
ASRT config>enable sr-tb-conversion
TB-Domain Segment Number in hex(1 - FFF) [1]? 222
TB-Domain's MTU [1470]?

:

```

Figure 211 (Part 1 of 5). Scenario 10: 2210A Configuration via the ASCII Console

```

:
ASRT config>list bridge

                        Source Routing Transparent Bridge Configuration
                        =====

Bridge:                  Enabled                  Bridge Behavior: SR<=>TB
                        +-----+
                        ] SOURCE ROUTING INFORMATION ]-----
                        +-----+

Bridge Number:           0A                      Segments:           1
Max ARE Hop Cnt:         14                      Max STE Hop cnt:    14
1:N SRB:                 Not Active              Internal Segment:
0x000
LF-bit interpret:        Extended

                        +-----+
                        ] SR-TB INFORMATION ]-----
                        +-----+

SR-TB Conversion:        Enabled
TB-Virtual Segment:      0x222                  MTU of TB-Domain: 1470

                        +-----+
                        ] SPANNING TREE PROTOCOL INFORMATION ]-----
                        +-----+

Bridge Address:          Default                  Bridge Priority: 32768/0x8000
STP Participation:       IEEE802.1d on TB ports, IBM-8209 and IBM-SRB proprietas

                        +-----+
                        ] TRANSLATION INFORMATION ]-----
                        +-----+

FA<=>GA Conversion:      Enabled                  UB-Encapsulation: Disabled
DLS for the bridge:      Disabled

                        +-----+
                        ] PORT INFORMATION ]-----
                        +-----+

Number of ports added: 2
Port:  1      Interface:  0      Behavior:  SRB Only  STP: Enabled
Port:  2      Interface:  1      Behavior:  STB Only  STP: Enabled

ASRT config>exit
Config>network 1      6
Point-to-Point user configuration
PPP Config>list all   7
Encoding: NRZ
Idle State: Flag
Clocking: Internal
Cable type: RS-232 DCE
Speed (bps): 64000

Transmit Delay Counter: 0
Lower DTR: Disabled
LCP Parameters
-----
CONFIG Request Tries:      20  CONFIG Nak Tries:      10
Terminate Tries:          10  Retry Timer:      3000

:

```

Figure 211 (Part 2 of 5). Scenario 10: 2210A Configuration via the ASCII Console

```

:
LCP Options
-----
Max Receive Unit:          2048  Magic Number:          Yes
Peer to Local (RX) ACCM:   A0000
Protocol Field Comp(PFC):   No   Addr/Cntl Field Comp(ACFC):   No

Authentication Options
Authenticate remote using: none
Identify self as:          ibm

NCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:          10
Terminate Tries:          10   Retry Timer:          3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

BCP Options
-----
Tinygram Compression:      Disabled

IPCP Options
IPCP Compression:          None
IP Address:               Don't Send or Request
PPP Config>enable ccp      8
PPP Config>list ccp        9

CCP Options
-----
Data Compression enabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ
PPP Config>set lcp options 10
Maximum Receive Unit (bytes) [2048]?
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) [A0000]?
Protocol Field Compression(PFC) [no]: y 11
Addr/Cntl Field Compression(ACFC) [no]: y 12

:

```

Figure 211 (Part 3 of 5). Scenario 10: 2210A Configuration via the ASCII Console


```

:
PPP Config>list lcp      13

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):   Yes   Addr/Cntl Field Comp(ACFC): Yes

Authentication Options
-----
Authenticate remote using: none
Identify self as:          ibm
PPP Config>set bcp options  14
TINYGRAM COMPRESSION [no]: y  15
PPP Config>list bcp        16

BCP Options
-----
Tinygram Compression:      Enabled
PPP Config>set ipcp options  17
IP COMPRESSION [no]: y     18
Send our IP address [no]: n
Request their IP address [no]: n
PPP Config>list ipcp       19

IPCP Options
-----
IPCP Compression:          Van Jacobson   Compression Slots:      16
IP Address:                Don't Send or Request
PPP Config>enable pap      20
Enable PAP

:

```

Figure 211 (Part 4 of 5). Scenario 10: 2210A Configuration via the ASCII Console

```

:
PPP Config>list lcp      21

LCP Parameters
-----
CONFIG Request Tries:      20   CONFIG Nak Tries:      10
Terminate Tries:          10   Retry Timer:          3000

LCP Options
-----
Max Receive Unit:          2048   Magic Number:          Yes
Peer to Local (RX) ACCM:    A0000
Protocol Field Comp(PFC):   Yes   Addr/Cntl Field Comp(ACFC): Yes

Authentication Options
-----
Authenticate remote using: PAP
Identify self as:          ibm
PPP Config>exit
Config>add ppp_user      22
Enter user name: []? 2210B 23
Password: remote         24
Enter password again: remote 25
User '2210B' has been added
Config>list ppp_user     26
  PPP User Name
  2210B
Config>Ctrl+p
*restart      27
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 211 (Part 5 of 5). Scenario 10: 2210A Configuration via the ASCII Console

Notes:

- 1 Talk to the CONFIG process.
- 2 Customization of network 0. This is the token-ring interface. Specify the unshielded media connector (UTP) and the locally administered address for this interface.
- 3 Customization of network 1. This is the serial 1 interface. Specify the RS-232 DTE cable that is used.
- 4 List the devices (interfaces) configuration.

- 5** Customization of the bridging function. Customize a source route-translational bridge with SRB for the token-ring interface and STB for serial 1 interface. Assign the LAN segment numbers and bridge number.
- 6** Access the PPP configuration.
- 7** List the PPP configuration.
- 8** Enable CCP.
- 9** List the CCP Options.
- 10** Set the LCP Options.
- 11** Enable the Protocol Field Compression(PFC).
- 12** Enable the Addr/Cntl Field Compression(ACFC).
- 13** List the LCP Parameters, the LCP Options and the Authentication Options.
- 14** Set the BCP Options.
- 15** Enable the Tinygram Compression.
- 16** List the BCP Options.
- 17** Set the IPCP Options.
- 18** Enable the IPCP Compression.
- 19** List the IPCP Options.
- 20** Enable PAP. You can enable CHAP instead of PAP, and you can enable PAP and CHAP at the same time.
- 21** List the LCP Parameters, the LCP Options and the Authentication Options.
- 22** Set the PPP_USER.
- 23** Enter the PPP_USER name to authenticate the remote user.
- 24** Enter the Password for the PPP_USER. The password does not appear.
- 25** Enter the Password for the PPP_USER again. The password does not appear.
- 26** List the PPP_USER. **27** Restart the 2210A to get the configuration running.

```

*
*talk 6      1

Config>network 0      2
Ethernet interface configuration
ETH config>list
Connector type:          AUTO-CONFIG
No IPX interface configuration
IP Encapsulation:        ETHER

ETH config>exit
Config>network 1      3
Point-to-Point user configuration
PPP Config>set hdlc cable rs-232 dte
PPP Config>exit
Config>list devices    4
Ifc 0   Ethernet          CSR  81600, CSR2  80C00, vector 94
Ifc 1   WAN PPP           CSR  81620, CSR2  80D00, vector 93
Ifc 2   WAN PPP           CSR  81640, CSR2  80E00, vector 92
Ifc 3   ISDN Basic        CSR      0, vector 0

Config>protocol asrt    5
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
ASRT config>add port 1 2
ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                =====

Bridge:                Enabled                Bridge Behavior: STB
                +-----+
-----] SOURCE ROUTING INFORMATION ]-----
                +-----+

Bridge Number:          N/A                    Segments:          0
Max ARE Hop Cnt:        00                    Max STE Hop cnt:   00
1&colonN SRB:            Not Active              Internal Segment:
0x000
LF-bit interpret:       Extended

                +-----+
-----] SR-TB INFORMATION ]-----
                +-----+

SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                    MTU of TB-Domain: 0

                +-----+
-----] SPANNING TREE PROTOCOL INFORMATION ]-----
                +-----+

Bridge Address:         Default                Bridge Priority: 32768/0x8000
STP Participation:      IEEE802.1d

                +-----+
-----] TRANSLATION INFORMATION ]-----
                +-----+

FA<=>GA Conversion:     Enabled                UB-Encapsulation: Disabled
DLS for the bridge:     Disabled

:

```

Figure 212 (Part 1 of 4). Scenario 10: 2210B Configuration via the ASCII Console

```

:
+-----+
-----] PORT INFORMATION ]-----
+-----+
Number of ports added: 2
Port: 1      Interface: 0      Behavior: STB Only  STP: Enabled
Port: 2      Interface: 1      Behavior: STB Only  STP: Enabled

ASRT config>exit
Config>network 1 6
Point-to-Point user configuration
PPP Config>list all 7
Encoding: NRZ
Idle State: Flag
Clocking: Internal
Cable type: RS-232 DCE
Speed (bps): 64000

Transmit Delay Counter: 0
Lower DTR: Disabled

LCP Parameters
-----
CONFIG Request Tries:          20  CONFIG Nak Tries:          10
Terminate Tries:              10  Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              2048  Magic Number:              Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):      No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
Authenticate remote using: none
Identify self as:             ibm

NCP Parameters
-----
CONFIG Request Tries:          20  CONFIG Nak Tries:          10
Terminate Tries:              10  Retry Timer:              3000

CCP Options
-----
Data Compression disabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ

:

```

Figure 212 (Part 2 of 4). Scenario 10: 2210B Configuration via the ASCII Console

```

:
BCP Options
-----
Tinygram Compression:          Disabled

IPCP Options
IPCP Compression:              None
IP Address:                    Don't Send or Request
PPP Config>enable ccp          8
PPP Config>list ccp            9

CCP Options
-----
Data Compression enabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ
PPP Config>set lcp options     10
Maximum Receive Unit (bytes) [2048]?
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) [A0000]?
Protocol Field Compression(PFC) [no]: y    11
Addr/Cntl Field Compression(ACFC) [no]: y   12

PPP Config>list lcp           13

LCP Parameters
-----
CONFIG Request Tries:          20   CONFIG Nak Tries:          10
Terminate Tries:               10   Retry Timer:             3000

LCP Options
-----
Max Receive Unit:              2048   Magic Number:            Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):      Yes    Addr/Cntl Field Comp(ACFC): Yes

Authentication Options
-----
Authenticate remote using: none
Identify self as:              ibm
PPP Config>set bcp options     14
TINYGRAM COMPRESSION [no]: y   15
:

```

Figure 212 (Part 3 of 4). Scenario 10: 2210B Configuration via the ASCII Console

```

:
PPP Config>list bcp 16

BCP Options
-----
Tinygram Compression: Enabled
PPP Config>set ipcp options 17
IP COMPRESSION [no]: y 18
Send our IP address [no]: n
Request their IP address [no]: n
PPP Config>list ipcp 19

IPCP Options
-----
IPCP Compression: Van Jacobson Compression Slots: 16
IP Address: Don't Send or Request
PPP Config>set name 20
Enter Local Name: []? 2210B 21
Password: remote 22
Enter password again: remote 23
PPP Local Name = 2210B
PPP Config>list lcp 24

LCP Parameters
-----
CONFIG Request Tries: 20 CONFIG Nak Tries: 10
Terminate Tries: 10 Retry Timer: 3000

LCP Options
-----
Max Receive Unit: 2048 Magic Number: Yes
Peer to Local (RX) ACCM: A0000
Protocol Field Comp(PFC): Yes Addr/Cntl Field Comp(ACFC): Yes

Authentication Options
-----
Authenticate remote using: none
Identify self as: 2210B
PPP Config>exit
Config>Ctrl+p
*restart 25
Are you sure you want to restart the gateway? (Yes or [No]): Yes

Copyright Notices:
Copyright 1985-1994 Proteon, Inc.
Copyright 1984-1987, 1989 by J. Noel Chiappa
Token-Ring microcode Copyright IBM Corp. 1985, 1994 All rights reserved.

MOS Operator Control

*
```

Figure 212 (Part 4 of 4). Scenario 10: 2210B Configuration via the ASCII Console

Notes:

- 1** Talk to the CONFIG process.
- 2** Customization of network 0. This is the Ethernet interface. Issue a List command. No changes are made to the default values.
- 3** Customization of network 1. This is the serial 1 interface. Specify the RS-232 DTE cable that is used.
- 4** List the devices (interfaces) configuration.
- 5** Customization of the bridging function. Customize a source route-translational bridge with SRB for the token-ring interface and STB for the serial 1 interface. Assign the LAN segment numbers and bridge number.
- 6** Access the PPP configuration.
- 7** List the PPP configuration.
- 8** Enable CCP.
- 9** List the CCP Options.
- 10** Set the LCP Options.
- 11** Enable the Protocol Field Compression(PFC).
- 12** Enable the Addr/Cntl Field Compression(ACFC).
- 13** List the LCP Parameters, the LCP Options and the Authentication Options.
- 14** Set the BCP Options.
- 15** Enable the Tinygram Compression.
- 16** List the BCP Options.
- 17** Set the IPCP Options.
- 18** Enable the IPCP Compression.
- 19** List the IPCP Options.
- 20** Set the local name.
- 21** Enter the local name for authentication.
- 22** Enter the password for the local name. The password does not appear.
- 23** Enter the password for the local name again. The password does not appear.
- 24** List the LCP Parameters, the LCP Options and the Authentication Options.
- 25** Restart the 2210A to get the configuration running.

Appendix A. Special Notices

This publication is intended to help customers and system specialists to implement networks incorporating the IBM 2210. The information in this publication is not intended as the specification of any programming interfaces that are provided by the IBM 2210 and the Nways MRS. See the PUBLICATIONS section of the IBM Programming Announcement for the IBM 2210 and the Nways MRS for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of

including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

Advanced Peer-to-Peer Networking	APPN
AT	Current
IBM	Nways
AIX	OS/2
RS/6000	PS/2
AIXwindows	VTAM
Operating System/2	RISC System/6000

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

ACTION	Prodigy Services Company
ADD	Applications Design and Development, Incorporated
Always	Lotus Development Corporation
AppleTalk	Apple Computer, Incorporated
ATM	Adobe Systems, Incorporated
Banyan	Banyan Systems, Incorporated
CA	Computer Associates
DCE	The Open Software Foundation
DEC	Digital Equipment Corporation
DECnet	Digital Equipment Corporation
DMS-100	Northern Telecom Limited
Echo	Echo Speech Corporation
Enable	The Software Group
Hayes	Hayes Microcomputer Products, Incorporated
Horizon	American Telephone and Telegraph Company
Internetwork Packet Exchange	Novell, Incorporated
IPX	Novell, Incorporated
Mac	Apple Computer, Incorporated
MODE	Animatics Multimedia Corporation

MSB	Apple Computer, Incorporated
NetWare	Novell, Incorporated
Nortel	Northern Telecom
Notes	Lotus Development Corporation
Novell	Novell, Incorporated
NT	Northern Telecom Limited or Microsoft Corporation
Option	American Telephone and Telegraph Company
PATH	Prodigy Services Company
ProComm	Datastorm Technologies, Incorporated
Proteon	Proteon, Incorporated
SLC	American Telephone and Telegraph Company
STB	STB Systems, Incorporated
VINES	Banyan Systems, Incorporated
VT100	Digital Equipment Corporation
486	Intel Corporation
80386	Intel Corporation

Other trademarks are trademarks of their respective companies.

Appendix B. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

B.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How to Get ITSO Redbooks" on page 769.

- *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios - Volume I*, SG24-4957-00 (available 3Q 1997)
- *IBM 2210 Nways Multiprotocol Router, IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios - Volume II*, SG24-4956-00 (available 3Q 1997)
- *AS/400 in Multiprotocol Networks*, SG24-4522-00
- *NCP Version 7 Release 3 New Functions*, SG24-2592-00
- *MPNP V1R3 for IBM 6611 Description and Implementation Guide*, SG24-4597-00

B.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042

B.3 Other Publications

These publications are also relevant as further information sources:

- *IBM 2210 Nways Multiprotocol Router Planning and Setup Guide*, GA27-4068
- *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference*, SC30-3680
- *Nways Multiprotocol Routing Services Software User's Guide*, SC30-3681
- *Nways Multiprotocol Routing Services Event Logging System Messages Guide*, SC30-3682-01
- *IBM 2210 Nways Multiprotocol Router Maintenance Information*, SY27-0345

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL <http://www.redbooks.ibm.com>.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

To get LIST3820s of redbooks, type one of the following commands:

```
TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
```

To get BookManager BOOKs of redbooks, type the following command:

```
TOOLCAT REDBOOKS
```

To get lists of redbooks, type one of the following commands:

```
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
```

To register for information on workshops, residencies, and redbooks, type the following command:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
```

For a list of product area specialists in the ITSO: type the following command:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
```

- **Redbooks Home Page on the World Wide Web**
<http://w3.itso.ibm.com/redbooks>
- **IBM Direct Publications Catalog on the World Wide Web**
<http://www.elink.ibm.link.ibm.com/pbl/pbl>

IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibm.link.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** (Do not send credit card information over the Internet) — send orders to:

	IBMMAIL	Internet
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications Publications Customer Support P.O. Box 29570 Raleigh, NC 27626-0570 USA	IBM Publications 144-4th Avenue, S.W. Calgary, Alberta T2P 3N5 Canada	IBM Direct Services Sortemosevej 21 DK-3450 Allerød Denmark
--	--	--

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1)001-408-256-5422 (Outside USA)** — ask for:

Index # 4421 Abstracts of new redbooks
Index # 4422 IBM redbooks
Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com

- **On the World Wide Web**

Redbooks Home Page	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibm.link.ibm.com/pbl/pbl

- **Internet Listserver**

With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibm.link.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name	Last name	
Company		
Address		
City	Postal code	Country
Telephone number	Telefax number	VAT number
• Invoice to customer number _____		
• Credit card number _____		

Credit card expiration date	Card issued to	Signature
-----------------------------	----------------	-----------

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

DO NOT SEND CREDIT CARD INFORMATION OVER THE INTERNET.

Index

Numerics

802.2 LLC 58, 59

A

accept option (IPXWAN) 412
access
 local 14
 remote 15
access controls (IPX) 416
accounting ISDN 107
action command for a byte filter list 729
action command for a name filter list 728
action in MAC Filtering 566
action of NetBIOS Filtering facility 723
adaptive source routing transparent (ASRT) 119
add (MCF command) 572
add address (ASRT command) 129
add address (IP tunnel bridge command) 134
add command for a Name filter list (NetBIOS Filtering) 728
add command for NetBIOS Filtering 729
add default-gateway (TCP/IP Host Services command) 137
add device command for Dial-on-Demand 686
add device for WRS 602
add mapping (ASRT command) 130
add port (ASRT command) 125
add prot-filter (ASRT command) 132
add secondary-circuit command 607
add tunnel (ASRT command) 133
add v25-bis-address command for Dial-on-Demand 686
add v25-bis-address for WRS 602
add-class (BRS command) 535
Add-Group-Name frame 717
Add-Group-Name-Query frames 723
Add-Name frame 717
Add-Name-Query frames 723
adding users 23
Addressing (ISDN) 103
adjacent router 307
aging time of filtering database 129
aging timer (IPX RAP) 408
aging timer (IPX RIP) 405
All Route Broadcast for NetBIOS 713
all-routes broadcast 114
area border router 306
areas 305
ARP Subnet Routing 325
ARP-subnet routing
 concept of 326
 implementation of 340

AS boundary router 306
AS boundary routing 332
ASCII file command 52
ASCII format of a name filter-item 728
ASRT 119
 See also adaptive source routing transparent (ASRT)
assign to a class (BRS command) 535
attach (MCF command) 573
 authentication key 332
Authentication Protocols for PPP 747
autonomous systems (ASs) 295

B

backbone 306
backup designated router 308, 312
Bandwidth Reservation (BRS) 530
 add-class command 535
 assign protocol to a class 535
 bandwidth reservation processing 531
 classes name 531
 configuration command table for BRS 534
 configuration commands 533
 default traffic assignment 532
 filters (subprotocol) assignment 532
 introduction to 530
 percentage of the bandwidth 531
 priority within a class 531
 protocols assignment 532
 Scenario 1: BRS with IP, IPX and Bridging 536
 TAGs assignment 532
bandwidth reservation processing 531
basic bridging commands 124
behavior of a bridge 119
BGP protocol description
 Aggregator 324
 AS number 321
 AS Path 323
 Atomic_aggregate 324
 attribute type 323
 authentication code 321
 authentication data 321
 Classless Inter-Domain Routing(CIDR) 320
 Error codes 325
 hold time 321
 infeasible routes 323
 Keep alive 322
 Local_pref 323
 Maintaining the BGP Connection 322
 Multi_exit_disc 323
 Next hop 323
 Notification messages 324
 Notifying Errors 324
 Open message 321, 322

- BGP protocol description (*continued*)
 - Opening and confirming a BGP connection 320
 - Origin 323
 - path attribute 323
 - path attributes 324
 - Sending Reachability Information 322
 - update message 322
 - withdrawn routes 323
- BGP protocol description (BGP) 320
- bibliography 767
- Boolean combination of filter list 725
- Boolean combination of filter-list 724
- BOOT CONFIG process 37
- boot configuration database 19
- boot files 19
- boot processes 19
- BootP 19
 - client 338
 - forwarding 338
 - process 338
 - relay agent 338
 - server 338
- bootstrap protocol 19
- Border Gateway Protocol 320
- Border Gateway Protocol (BGP)
 - Adding Policies 358
 - BGP Configuration Commands 356
 - BGP Monitoring Commands 358
 - BGP neighbors 335
 - BGP speakers 335
 - BGP4 Configuration Steps 357
 - BGP4 Implementation 335
 - BGP4 Monitoring 358
 - Configuring BGP4 356
 - define BGP neighbors 357
 - EBGP 335
 - IBGP 335
 - Keep alive messages 336
 - Notification messages 336
 - Open messages 336
 - Originate Policies 336
 - Originate Policy 358
 - policy statements 336
 - protocol description 320
 - Receive Policies 336
 - Receive Policy 358
 - Send Policies 336
 - Send Policy 358
 - Update messages 336
- BRI (ISDN Basic Rate Interface) 103
- bridge behavior 119
- bridge number 114
- Bridge personality 119, 120
- Bridge tunnel
 - See Tunnel bridge
- bridging 111
 - aging time of filtering database 129
 - bridging methods on the 2210 119
- bridging (*continued*)
 - Bridging Scenarios 138
 - client server group 134
 - configuration commands of 122
 - DEC* LAT 131
 - Ethernet LAN 112
 - Ethernet type bridge filtering 132
 - Ethernet type mapping 131
 - filtering database size 129
 - forward delay bridge parameter 128
 - functional MAC address 130
 - group MAC address 130
 - group membership function 134
 - hello time bridge parameter 128
 - internal IP address 135
 - Internet Group Management Protocol (IGMP) 135
 - introduction to 111
 - maximum age bridge parameter 128
 - Multicast OSPF (MOSPF) 134
 - OSI reference model 111
 - OSPF 134
 - path-cost port parameter 128
 - permanent MAC address entry 129
 - ping 136
 - priority bridge parameter 128
 - priority port parameter 128
 - resolution time of filtering database 129
 - Routing Information Field (RIF) 130
 - Routing Information Indicator (RII) 130
 - SAP bridge filtering 132
 - SAP mapping 131
 - segment number of IP Tunnel 133
 - SNAP bridge filtering 132
 - SNAP mapping 131
 - SNMP management 136
 - source route - translational bridge (SR-TB) 112, 130
 - source route bridge (SRB) 112, 114, 130
 - source route transparent bridge (SRT) 112, 116
 - source route-translational bridge (SR-TB) 116
 - spanning tree bridge (STB) 113
 - spanning tree bridging (STB) 112
 - spanning tree explorer frame 130
 - TCP/IP Host Services commands table 136
 - telnet 136
 - TFTP protocol 136
 - token-ring LAN 112
 - traceroute 136
 - transparent bridge (STB) 112, 113, 130
 - transparent spanning tree frame 130
 - tunnel bridge 112, 117
- bridging commands table 123
- bridging configuration commands 122
 - add address 129
 - add address (IP tunnel) 134
 - add default-gateway (for TCP/IP Host Services) 137
 - add mapping 130

- bridging configuration commands (*continued*)
 - add port 125
 - add prot-filter 132
 - add tunnel 133
 - bridging commands table 123
 - change bridge 126
 - change segment 126
 - delete port 125
 - disable port 125
 - enable dls 124
 - enable spanning-tree-explorer 126
 - enable/disable duplicate tsf/ste 130
 - enable/disable fa-ga-mapping 131
 - enable/disable IBM8209_spanning_tree 127
 - enable/disable rip-listening (for TCP/IP Host Services) 137
 - enable/disable route-discovery (for TCP/IP Host Services) 136
 - enable/disable services (for TCP/IP Host Services) 136
 - enable/disable source-routing 125
 - enable/disable SR-TB conversion 130
 - enable/disable stp 127
 - enable/disable transparent 125
 - Join client-group (for IP tunnel) 135
 - Join peer-group (for IP tunnel) 135
 - Join server-group (for IP tunnel) 135
 - Peer to Peer group 134
 - set address (for TCP/IP Host Services) 136
 - set age 129
 - set base-multicast-address (IP Tunnel) 134
 - set bridge 127
 - set filtering 129
 - set If-bit-interpretation 126
 - set maximum-packet-size 126
 - set port 128
 - set protocol bridge 128
 - set protocol port 128
 - set route-descriptor-limit 127
 - tunnel 133
- Bridging Control Protocol (BCP) 732
- bridging methods between the 2210 and the 6611 121
 - Ethernet LAN 121
 - IBM 6611 MPNP 121
 - Nways MRNS 121
 - PPP serial link 121
 - Source Route - Translational Bridge (SR-TB) 121
 - Source Route Bridge (SRB) 121
 - token-ring LAN 121
 - transparent bridge (STB) 121
- bridging methods on the 2210 119
 - adaptive source routing transparent (ASRT) 119
 - bridge behavior 119
 - Bridge personality 119, 120
 - Dial on Demand 119
 - Frame Relay data-link 119
 - IP protocol 119

- bridging methods on the 2210 (*continued*)
 - Nways MRNS 119
 - SDLC data-link 119
 - Supported Bridging Methods table for Nways MRS 119
 - tunnel bridge 119
 - WAN Restoral (WRS) 119
 - X.25 data-link 119
- Bridging Scenarios 138
 - Frame Relay Source Routing Bridge with FR 263
 - IBM 6611 MPNP 138
 - internal segment number 138
 - Nways MRNS 138
 - scenario 1: transparent bridge with 2210s 139
 - scenario 2: transparent bridge with 2210 and 6611 149
 - Scenario 3: Source Route Bridge with 2210s 160
 - Scenario 4: Source Route Bridge with 2210 and 6611 180
 - scenario 5: source route transparent bridge with 2210s and 6611 196
 - Scenario 6: NetBIOS facilities on 2210 with SR-TB 209
 - Scenario 6: source route-translational bridge with 2210s 209
 - Scenario 7: Source Route - Translational Bridge with 2210 and 6611 233
 - Scenario 8: IP Tunnel Bridge via X.25 with 2210s 247
 - Source Route Bridge (SRB) 138
 - Source SAP inbound filters 138
- Broadcast address 344
- Broadcasted frames with Duplicate Frame Filtering Process 718
- BRS
 - See Bandwidth Reservation (BRS)
 - BRS configuration commands 533
- BSD Unix 303
- byte filter 724
- byte filter commands 729
- byte filter list process 725
- byte filter-item 724
- byte filter-list 724

C

- calls direction for Dial-on-Demand 684
- canonical MAC address 57
- Challenge-Handshake Authentication Protocol (CHAP) 748
- change bridge (ASRT command) 126
- change segment (ASRT command) 126
- circuit configuration commands for WRS 605
- circuit establishment (DLSw) 450
- classes name of BRS 531
- client server group in IP tunnel bridge 134
- client/server group (DLSw) 453
- collisions (Ethernet monitoring command) 74

- color command 52
- communications command 52
- community name rights 54
- Compression Control Protocol (CCP) 731
- confidence ID 412
- CONFIG ONLY process 28
- configuration program 19, 21, 47
 - ASCII file command 52
 - color command 52
 - communications command 52
 - configuration window 47
 - configure pull-down menu 51
 - Converting a Configuration Database File 47
 - create router configuration command 51
 - Creating Configuration Database File 46
 - default model command 52
 - delete configuration command 52
 - font command 52
 - Hardware and Software Requirement 42
 - Installation on a PC 45
 - Installation on a RISC System/6000 44
 - Installing the Configuration Program 44
 - message prompting command 52
 - Migration support 46
 - navigation window 47
 - new configuration command 51
 - open configuration command 51
 - options pull-down menu 52
 - read router configuration command 51
 - save configuration as command 51
- configuration window 47
- configurations 20
- configure pull-down menu 51
- connector-type (Ethernet command) 61
- console 14
- converted Name-Query frame 714
- counting to infinity 299, 300
- create (MCF command) 572, 573
- create byte-filter-list command 729
- create name-filter-list command (NetBIOS Filtering) 727
- create router configuration command 51

D

- Data Compression for PPP Interface 731
- Data Link Switching 449
- data-link command for WRS 601
- database description 313
- database exchange 313
- datagram frames of NetBIOS 724
- DEC* LAT 131
- default (MCF command) 573
- default filter list action for NetBIOS Filtering 724
- default model command 52
- default network gateway 331, 345
- default subnetwork gateway 331, 345
 - br.scenarios and configurations 362

- delete command for NetBIOS Filtering 730
- delete configuration command 52
- delete port (ASRT command) 125
- designated router 308, 312, 333
- Dial Backup
 - See WAN Restoral (WRS)
- dial circuit commands 104
- dial circuit interface in WRS 601
- dial circuit interface(s) for Dial-on-Demand 686
- dial circuits (ISDN) 104
- Dial on Demand 119
- Dial-on-Demand 683
 - add device command 686
 - add v25-bis-address command 686
 - calls direction 684
 - circuit configuration commands 688
 - configuration commands 685
 - configuration commands on CONFIG Process 686
 - dial circuit interface(s) 686
 - DLSw protocol for 684
 - encapsulator command 689
 - functionality of 683
 - interoperability with IBM 6611 Network Processor 685
 - introduction to Dial-on-Demand 683
 - IP protocol for 684
 - IPX protocol for 684
 - ISDN configuration commands 688
 - multiple dial circuits 689
 - protocol address configuration on serial interfaces 686
 - Scenario 7: Dial-on-Demand over IP 690
 - Scenario 8: Dial-on-Demand over IP using ISDN 701
 - set calls command 688
 - set data-link command 686
 - set destination command 689
 - set idle command 689
 - set local command 687, 688
 - set net command 688
 - V.25bis configuration commands 687
 - V.25bis interface 685, 686
 - V.25bis phone numbers 683
- Dial-on-Demand configuration commands 685
- disable port (ASRT command) 125
- discovery frame 114
- discovery response frame 114
- Distance Vector Multicast Routing Protocol 328
 - implementation of 335
- distance vector routing 297
 - advantage of 298
 - counting to infinity 299, 300
 - disadvantages of 298
 - routing table calculation 298
 - split horizon 299
 - split horizon with poison reverse 301
 - triggered updates 301

- DLC termination 449
- DLSw
 - circuit establishment 450
 - client/server group 453
 - commands 453
 - configuration 453
 - configuration overview 454
 - DLC termination 449
 - encapsulated SDLC 452
 - encapsulated SNA 453
 - functions 449
 - group 455
 - group membership 453
 - implementing 451
 - LAN to LAN over WAN 453
 - local DLSw 452
 - MOSPF 453
 - overview 449
 - peer-to-peer group 453
 - remote DLSw 452
 - SDLC to LAN over WAN 453
 - spoofing 449
 - TCP connections 449
 - TCP neighbors 455
 - virtual segment number 451, 455
- DLSw over frame relay (configuration scenario) 484
- DLSw over PPP (configuration scenario) 460
- DLSw protocol over Dial-on-Demand 684
- DLSw scenarios 510
 - 2110 and 6611 484
 - 2110s over PPP 460
- dump (token-ring monitoring command) 76
- Duplicate frame filtering database 718
- Duplicate Frame Filtering Process 713, 717
- Duplicate frame filtering process commands 721
- Duplicate frame filtering process on Add-Names frames 719
- duplicate frame filtering timer setting 722
- DVMRP
 - See Distance Vector Multicast Routing Protocol

E

- EGP
 - See Exterior Gateway Protocol (EGP)
- EGP configuration
- EGP protocol description
- enable dls (ASRT command) 124
- enable spanning-tree-explorer (ASRT command) 126
- enable/disable duplicate tsf/ste (ASRT command) 130
- enable/disable fa-ga-mapping (ASRT command) 131
- enable/disable IBM8209_spanning_tree (ASRT command) 127
- enable/disable rip-listening (TCP/IP Host Services command) 137
- enable/disable route-discovery (TCP/IP Host Services command) 136

- enable/disable services (TCP/IP Host Services command) 136
- enable/disable source-routing (ASRT command) 125
- enable/disable SR-TB conversion (ASRT command) 130
- enable/disable stp (ASRT command) 127
- enable/disable transparent (ASRT command) 125
- encapsulated SDLC 452
- encapsulated SNA 453
- encapsulation 453
- encapsulation (Ethernet command) 61
- encapsulator command for Dial-on-Demand 689
- encapsulator command for WRS 606
- Ethernet II 57
- Ethernet II layout 57
- Ethernet interface 57
 - 802.2 LLC 58
 - canonical MAC address 57
 - collisions (monitoring command) 74
 - configuration of 60
 - connector-type command 61
 - encapsulation command 61
 - Ethernet commands table 61
 - Ethernet II 57
 - Ethernet II layout 57
 - Ethernet type 57
 - frame command 62
 - IEEE 802.3 57
 - IEEE 802.3 layout 58
 - monitoring Ethernet 74
 - SNAP 58
- Ethernet interface configuration 60
- Ethernet LAN for bridging 121
- Ethernet type 57
- Ethernet type bridge filtering 132
- Ethernet type bridge mapping 131
- event logging system 36, 38
- Exterior Gateway Protocol (EGP)
- exterior gateway protocols 295

F

- Features and Facilities 525
 - Bandwidth Reservation (BRS) 530
 - Dial-on-Demand 683
 - MAC Filtering (MCF) 566
 - NetBIOS Filtering facility 723
 - NetBIOS Name Caching facility 713
 - PPP Authentication Protocols 747
 - PPP Data Compression 731
 - WAN Reroute 665
 - WAN Restoral (WRS) 599
- filter (MCF definition) 567
- filter for NetBIOS Filtering 724
- filter list (MCF definition) 567
- filter lists for NetBIOS Filtering 724
- filter-item (MCF definition) 567
- filter-item action for NetBIOS Filtering 724

- filter-items for NetBIOS Filtering 724
- filter-on command for NetBIOS Filtering 730
- filtering database 113, 116
- filtering database commands 129
- filtering database size 129
- filters (IPX SAP) 416
- flooding 302, 316
- font command 52
- forward delay bridge parameter 128
- forwarding table 113
- frame (Ethernet command) 62
- frame (token-ring command) 67
- Frame Relay Boundary Access Node
- frame relay data-link for bridging 119
- Frame Relay over ISDN 108
- frame type (IPX) 415
- functional MAC address 130

G

- gateway protocols
 - definition of 295
- get nearest server request 409, 410
- get nearest server response 409
- group (DLSw) 455
- group MAC address 130
- group membership (DLSw) 453
- group membership function in IP Tunnel Bridge 134
- GWCON process 35

H

- Hardware
 - indicators 9
 - models 1
 - reset button 9
- hello protocol 311
- hello time bridge parameter 128
- hexadecimal format of a name filter-item 728
- hexadecimal mask for MAC Filtering 572
- hexadecimal mask value of NetBIOS Filtering 729
- hexadecimal pattern value of NetBIOS Filtering 729
- hops count 115
- hops t server (IPX SAP) 408
- host name filter 723
- host name filter list process 725
- host name filter-item 724
- host name filter-list 724
- host number (IPX) 415

I

- IBD 19
- Idle-timer for Name caching process 714
- idle-timer setting for Name caching process 721
- IEEE 802.3 57
- IEEE 802.3 layout 58
- IEEE 802.5 58

- IEEE 802.5 layout 58
- IGMP
 - See Internet Group Management Protocol
- IGMP router 327
- indicators 9
- information request (IPXWAN) 413
- information response (IPXWAN) 413
- integrated boot device 19
- interface (IPX SAP) 408
- interior gateway protocols 295
- internal IP address 330, 343
- internal IP address in IP Tunnel Bridge 135
- internal segment number for bridging 138
- Internet Group Management Protocol 327
 - Host Membership Query 327
 - Host Membership Report 327
 - parameters 335
- Internet Group Management Protocol (IGMP) in IP Tunnel Bridge 135
- interoperability with IBM 6611 Network Processor for Dial-on-Demand 685
- interoperability with IBM 6611 Network Processor for WRS 600
- intra-area router 306
- IP access control 331
- IP broadcast format 330
- IP configuration 341
 - command overview 341
 - Configuring IP Source-Routing 346
 - hardware interfaces 345
 - routing protocols 346
 - steps 343
- IP Control Protocol (IPCP) 732
- IP implementation 329
 - access controls 337
 - address assignments 331
 - ARP-Subnet Routing 340
 - BootP 338
 - filters 337
 - IP source routing 337
 - SNMP 339
 - Telnet 338
 - TFTP 340
- IP LAN Network Manager 289
- IP multicast 326
 - address assignment 326
 - group membership 326
 - multicast address 335
- IP network for IP tunnel bridge 117, 119
- IP protocol over Dial-on-Demand 684
- IP routing protocols 295
 - implementation on the IBM 2210 329
- IP tunnel 327, 328
- IPX
 - access controls 416
 - configuration commands 413
 - configuration considerations 416
 - configuration overview 414

- IPX (*continued*)
 - Enhancements 417
 - frame type 415
 - global filters 417
 - host number 415
 - interface-filters 417
 - IPX filters 418
 - IPXWAN overview 410
 - keep-alive filtering 418
 - network number 415
 - RIP filter 417
 - RIP overview 405
 - SAP filter 417
 - SAP filters 416
 - SAP overview 408
 - serialization packets 418
- IPX over PPP with 6611 (configuration scenario) 440
- IPX over X.25 (configuration scenario) 418
- IPX protocol over Dial-on-Demand 684
- IPX scenarios
 - IPX over PPP with 6611 440
 - IPX over X.25 418
- IPXWAN
 - accept option 412
 - confidence ID 412
 - link master 411
 - link slave 411
 - node ID 412
 - node-id 415
 - option data 413
 - option number 412
 - overview 410
 - packet format 411
 - packet type 412
 - primary network number 411
 - router name 411, 415
 - sequence number 412
- IPXWAN overview 410
- IPXWAN packet type 412
- ISDN configuration commands for WRS 604
- isdn implementation 103
- ISDN interface 102
 - addressing 103
 - configuration commands table 105
 - configuration steps 105
 - dial circuits 104
 - Frame Relay over ISDN 108
 - ISDN Basic Rate Interface (BRI) 103
 - ISDN Implementation 103
 - ISDN interface 102
 - ISDN Primary Rate Interface (PRI) 103
 - ISDN switch 103
 - monitoring ISDN and Dial Circuits 108
 - network subdial address 103
 - optional configuration steps 107
 - WAN Restoral 107
- ISDN interface in WRS 599

ISO 8802-1 113

J

- Join client-group (IP Tunnel Bridge command) 135
- Join peer-group (IP Tunnel Bridge command) 135
- Join server-group (IP Tunnel Bridge command) 135

L

- LAN interfaces 57
 - Ethernet interface 57
 - token-ring interface 58
- LAN interfaces configuration 60
- LAN to LAN over WAN 453
- Link Control Protocol (LCP) 731
- link master 411
- link slave 411
- link state acknowledgement 316
- link state advertisement 309
- link state propagation 315
- link state request 314
- link state routing 302
 - contacting neighbors 302
 - flooding 302
 - hello 302
 - link state information 302
- link state update 315
- LNM 289
- LNM Considerations 293
- LNM Scenarios 290
- local access 14
- local DLSw 452

M

- MAC address in a filter-item 572
- MAC Filtering (MCF) 566
 - action of a filter 566
 - add command 572
 - attach command 573
 - configuration commands 570
 - create command 572, 573
 - default command 573
 - filter definition 567
 - filter list definition 567
 - filter-item definition 567
 - hexadecimal mask for a MAC address 572
 - introduction to 566
 - MAC address in a filter-item 572
 - MAC Filtering Commands Table 571
 - process of a filter 568
 - Scenario 2: MAC Filtering with Bridging 574
 - set-action command 572
 - Sliding Window Filter 570
 - TAG value for Bandwidth Reservation 574
 - update command 572
- MAC Filtering configuration commands 570

- MAC Filtering process of a filter 568
- MAC sublayer 113
- maximum age bridge parameter 128
- maximum frame size 115
- MCF

- See MAC Filtering (MCF)

- media (token-ring command) 66
- message prompting command 52
- MIB support 339
 - ELS.trap 340
- models 1

- monitoring Ethernet 74
- monitoring LAN interfaces 74
- monitoring token-ring 76
- MONITR process 36
- MOSDDT process 37
- MOSPF

- See Multicast OSPF

- MOSPF (DLSw) 453

- MRS

- adding users 23
 - BOOT CONFIG process 37
 - boot configuration database 19
 - boot files 19
 - boot processes 19
 - Bootp 19
 - bootstrap protocol 19
 - community name rights 54
 - CONFIG ONLY process 28
 - configuration program 19, 47
 - configurations 20
 - event logging system 36, 38
 - GWCON process 35
 - IBD 19
 - integrated boot device 19
 - MONITR process 36
 - MOSDDT process 37
 - OPCON process 29
 - overview 19
 - process structure 24
 - QUICK CONFIG process 25
 - reload 20
 - restart 21
 - sending/Retrieving the configuration file 53
 - software packages 10
 - startup 19

- Multicast OSPF 327

- implementation of 335

- Multicast OSPF for IP Tunnel Bridge 134

- multiple dial circuits for Dial-on-Demand 689

N

- Name caching database 714
- Name caching process 713
- Name caching process commands 720
- Name caching process for Name-Query frames 716
- Name caching process for Name-Query-Response frames 716

- Name-Query frame 713, 717

- Name-Query frames 724

- Name-Query-Response frame 713

- navigation window 47

- neighbor interface state 311

- neighbor router 307

- NetBIOS Facilities 713

- NetBIOS Filtering Facility 723

- NetBIOS Name Caching Facility 713

- NetBIOS Filtering configuration commands 726

- NetBIOS Filtering Facility 723

- action command for a byte filter list 729

- action command for a Name filter list 728

- add command 729

- add command for a Name filter list 728

- Add-Group-Name-Query frames 723

- Add-Name-Query frames 723

- ASCII format 728

- Boolean combination of filter list 725

- Boolean combination of filter-list 724

- byte filter 724

- byte filter configuration commands 729

- byte filter list process 725

- byte filter-item 724

- byte filter-list 724

- configuration commands 726

- create byte-filter-list command 729

- create name-filter-list command 727

- datagram frames 724

- default filter list action 724

- delete command 730

- filter 724

- filter action 723

- filter lists 724

- filter-item action 724

- filter-items 724

- filter-on command 730

- hexadecimal format 728

- hexadecimal mask value 729

- hexadecimal pattern value 729

- host name filter 723

- host name filter commands 727

- Host name filter list process 725

- host name filter-item 724

- host name filter-list 724

- introduction to 723

- Name-Query frames 724

- NetBIOS Filtering commands table 727

- NetBIOS Filtering process 724

- offset 729

- resulting filter list action 725

- Scenario of NetBIOS Filtering 731

- update command for a byte filter list 729

- update command for a Name filter list 728

- Wildcard in host name 728

- NetBIOS Name Caching 713

- Add-Group-Name frame 717

- Add-Name frame 717

NetBIOS Name Caching (*continued*)

- All Route Broadcast 713
- Broadcasted frames 718
- configuration commands 719
- converted Name-Query frame 714
- Duplicate frame filtering database 718
- Duplicate Frame Filtering Process 713, 717
- Duplicate frame filtering process commands 721
- Duplicate frame filtering process on Add-Names frames 719
- duplicate frame filtering timer setting 722
- Idle-timer 714
- idle-timer setting 721
- introduction to 713
- Name caching database 714
- Name caching process 713
- Name caching process commands 720
- Name caching process for Name-Query frames 716
- Name caching process for Name-Query-Response frames 716
- Name-Query frame 713, 717
- Name-Query-Response frame 713
- NetBIOS Name Caching commands table 719
- NetBIOS Name Caching scenario 722
- Server-timer 714
- server-timer setting 721
- timer add-name command 722
- timer entry command 721
- timer server-response command 721
- NetBIOS Name Caching Facility commands 719
- network address (IPX) 410
- Network Information Center 295
- network number (IPX) 405, 415
- network subdial address 103
- networks
 - broadcast 308
 - multiaccess 308
 - non-broadcast 308
 - point to point 308
- networks supported 10
- new configuration command 51
- node address (IPX) 410
- node ID (IPXWAN) 412
- node-id (IPXWAN) 415
- non-broadcast multi-access 333, 334
- non-canonical MAC address 58
- number of hops (IPX RIP) 405
- number of ticks (IPX RIP) 405

O

- offset of NetBIOS Filtering 729
- OPCON process 29
- open configuration command 51
- Open Shortest Path First (OSPF) 305
 - and frame relay 333
 - and non-broadcast networks 333
 - implementation 332

Open Shortest Path First (OSPF) (*continued*)

- interoperability with 6611 334
- protocol description 309
- terminology 305
- option data (IPXWAN) 413
- option number (IPXWAN) 412
- options pull-down menu 52
- OSI Reference Model 111
- OSPF
 - See Open Shortest Path First (OSPF)
- OSPF configuration
- OSPF in IP Tunnel Bridge 134
- OSPF protocol description 309
 - database description 313
 - database exchange 313
 - designated router election 312
 - discovering neighbors 311
 - establishing adjacencies 313
 - flooding 316
 - hello protocol 311
 - link state acknowledgement 316
 - link state propagation 315
 - link state request 314
 - link state update 315
 - neighbor state 311
 - router interface state 310
 - routing table calculation 317

- OSPF router ID 332
- OSPF terminology 305
 - adjacent router 307
 - area border router 306
 - areas 305
 - AS boundary router 306
 - backbone 306
 - backup designated router 308
 - designated router 308
 - intra-area router 306
 - link state advertisement 309
 - neighbor router 307
 - network types 308

P

- packet format (IPX RIP) 406
- packet format (IPX SAP) 409
- packet format (IPXWAN) 411
- packet-size (token-ring command) 66
- Password Authentication Protocol (PAP) 748
 - refid=Challenge-Handshake Authentication Protocol (CHAP) 748
- path-cost port parameter 128
- peer-to-peer group (DLSw) 453
- Peer-to-peer group in IP Tunnel Bridge 134
- permanent MAC address entry 129
- personality of a bridge 120
 - bridging methods between the 2210 and the 6611 121
- ping (IP ping for bridge) 136

- point-to-multipoint 335
 - id=ipimp.static routes 336
- Power Source 1 (ISDN switch) 107
- PPP Authentication Protocols
 - configuration command table for PAP and CHAP 748
 - introduction to PPP Authentication Protocols 747
 - Password Authentication Protocol (PAP) 748
 - Scenario 10: PPP Authentication with Bridging 750
- PPP Data Compression
 - Bridging Control Protocol (BCP) 732
 - Compression Control Protocol (CCP) 731
 - configuration command table for data compression 733
 - introduction to data compression 731
 - IP Control Protocol (IPCP) 732
 - Link Control Protocol (LCP) 731
 - Scenario 9: PPP Data Compression with Bridging 734
- PPP serial link for bridging 121
- PRI (ISDN Primary Rate Interface) 103
- primary interface in WRS 601
- primary network number (IPXWAN) 411
- priority bridge parameter 128
- priority port parameter 128
- priority within a class of BRS 531
- process structure 24
- PROM Load/Dump program
 - Loading the PROM Load/Dump program 54
 - PROM Load/Dump Program 54
- protocol address on serial interfaces (in Dial-on-Demand) 686
- protocol address on serial interfaces (in WRS) 601
- Protocol Filtering commands 132
- protocols
 - Border Gateway Protocol 320
 - Open Shortest Path First 305
 - Routing Information Protocol 303
- Proxy-ARP
 - See ARP-subnet routing

Q

QUICK CONFIG process 25

R

- read router configuration command 51
- reassembly size 331, 345
- reload 20
- remote access 15
- remote DLSw 452
- reset button 9
- resolution time of filtering database 129
- restart 21
- resulting filter list action for NetBIOS Filtering 725
- RFC1795 508
- RIF layout 59

RIP

See also Routing Information Protocol (RIP)
update interval 417

RIP (IPX)

- aging timer 405
- network number 405
- number of hops 405
- number of ticks 405
- overview 405
- packet format 406
- route selection 407
- routing table 405, 417
- split-horizon 406
- update interval 406

RIP configuration

RIP overview 405

RIP protocol description 303

- maximum RIP metric 304

- RIP packet format 304

route designator 60

route selection (IPX RIP) 407

ROUTED 303

router cache size 330, 344

router configurations 362

router id 330, 344

router interface state 310

router name (IPXWAN) 411, 415

router priority 333

routing algorithms 296

- distance vector routing 297

- link state routing 302

- LNM scenarios 290

- static routing 296, 510

Routing Information Field (RIF) 59, 60, 114, 116, 118, 130

Routing Information Indicator (RII) 59, 60, 114, 116, 117, 130

Routing Information Protocol (RIP) 303

- implementation of 331

- interoperability with 6611 332

- protocol description 303

routing table (IPX RIP) 405, 417

routing table size 330, 344

S

SAP

- filters 416

- get nearest server request 409, 410

- get nearest server response 409

- information request 413

- information response 413

- network address 410

- node address 410

- packet format 409

- server information table 417

- server name 410

- service type 410

- socket address 410

SAP (continued)

- timer request 413
- timer response 413
- update interval 409, 417

SAP (IPX)

- aging timer 408
- hops to server 408
- interface 408
- overview 408
- server address 408
- server information table 408
- server name 408
- server type 408

SAP bridge filtering 132

SAP bridge mapping 131

SAP overview 408

save configuration as command 51

Scenario 1: BRS with IP, IPX and Bridging 536

Scenario 1: DLSw over PPP 460

Scenario 1: IPX over X.25 418

scenario 1: transparent bridge with 2210s 139

Scenario 10: PPP Authentication with Bridging 750

Scenario 2: DLSw over frame relay 484

Scenario 2: IPX over PPP with 6611 440

Scenario 2: MAC Filtering with Bridging 574

scenario 2: transparent bridge with 2210 and 6611 149

Scenario 3: Source Route Bridge with 2210s 160

Scenario 3: WAN Restoral with IP, DLSw and Bridging 608

Scenario 4: Source Route Bridge with 2210 and 6611 180

Scenario 4: WAN Restoral with IP, DLSw and Bridging using ISDN 641

scenario 5: source route transparent bridge with 2210s and 6611 196

Scenario 5: WAN Reroute 667

Scenario 6: NetBIOS facilities on 2210 with SR-TB 209

Scenario 6: Source route-translational bridge with 2210s 209

Scenario 6: WAN Reroute using ISDN 672

Scenario 7: Dial-on-Demand over IP 690

Scenario 7: Source Route - Translational Bridge with 2210 and 6611 233

Scenario 8: Dial-on-Demand over IP using ISDN 701

Scenario 8: IP Tunnel Bridge via X.25 with 2210s 247

Scenario 9: PPP Data Compression with Bridging 734

Scenario of NetBIOS Filtering 731

Scenario of NetBIOS Name Caching 722

SDLC

- Configuring SDLC 92
- Monitoring SDLC 93
- negotiable 90
- primary 90
- SDLC Configuration Commands 92
- SDLC Configuration Steps 92
- SDLC Implementation 89

SDLC (continued)

SDLC session establishment 89

secondary 90

spoofing 90

SDLC data-link for bridging 119

SDLC to LAN over WAN 453

secondary interface in WRS 601

segment number 60, 114, 118

segment number of IP Tunnel 133

sending/Retrieving the configuration file 53

server address (IPX SAP) 408

server information table (IPX SAP) 408, 417

server name (IPX SAP) 408, 410

server type (IPX SAP) 408

Server-timer for Name caching process 714

server-timer setting for Name caching process 721

service type (IPX SAP) 410

set address (TCP/IP Host Services command) 136

set age (ASRT command) 129

set base-multicast-address (IP tunnel bridge command) 134

set bridge (ASRT command) 127

set calls command for Dial-on-Demand 688

set calls command for WRS 605

set data-link command for Dial-on-Demand 686

set destination command for Dial-on-Demand 689

set destination command for WRS 606

set filtering (ASRT command) 129

set idle command for Dial-on-Demand 689

set idle command for WRS 605

set If-bit-interpretation (ASRT command) 126

set local command for Dial-on-Demand 687, 688

set local command for WRS 603, 604

set maximum-packet-size (ASRT command) 126

set net command for Dial-on-Demand 688

set net command for WRS 605

set physical-address (token-ring command) 66

set port command for bridging 128

set protocol bridge (ASRT command) 128

set protocol port (ASRT command) 128

set rif-timer (token-ring command) 66

set route-descriptor-limit (ASRT) command 127

shielded (STP) 66

Simple Network Management Protocol

agent 339

authentication 339

community 339

mib support 339

subtree 339

traps 339

view 339

single route broadcast 114

Sliding Window Filter

SNAP 58, 59

SNAP bridge filtering 132

SNAP bridge mapping 131

SNMP

See Simple Network Management Protocol

- socket address (IPX) 410
- software packages 10
- Source route - translational bridge (SR-TB) 112, 121, 130
 - Ethernet LAN 116
 - routing information indicator (RII) 117
 - Source Route Bridge (SRB) 116
 - token-ring LAN 116
 - transparent bridge (STB) 116
- source route - translational bridge commands 130
- Source Route Bridge (SRB) 59, 60, 112, 114, 121, 130, 138
- Source Route Bridge commands 126
- source route transparent bridge (SRT) 112, 116
 - filtering database 116
 - routing information field (RIF) 116
 - routing information indicator (RII) 116
 - Source Route Bridge (SRB) 116
 - transparent bridge (STB) 116
- source route-translational bridge (SR-TB) 116
- Source Routing Bridge (SRB)
 - all-routes broadcast 114
 - bridge number 114
 - discovery frame 114
 - discovery response frame 114
 - hops count 115
 - maximum frame size 115
 - routing information field (RIF) 114
 - Routing Information Indicator (RII) 114
 - segment number 114
 - single route broadcast 114
 - token-ring LAN 114
 - token-ring spanning tree algorithm 114
- Source SAP inbound filters 138
- source-routing (token-ring command) 67
- spanning tree bridge (STB) 113
 - See also* transparent bridge (STB)
- spanning tree bridging (STB) 112
- spanning tree explorer frame 130
- spanning tree protocol 114
- Spanning Tree Protocol commands 127
- speed (token-ring command) 67
- split horizon 299
- split horizon with poison reverse 301
- split-horizon 406
- spoofing 449
- SR-TB
 - See* source route transparent bridge (SRT)
- SRB
 - See* Source Routing Bridge (SRB)
- SRT
 - See* source route transparent bridge (SRT)
- startup 19
- static routes
 - implementation of 336
- static routing 296
- STB
 - See* transparent bridge (STB)

- STP
 - See* shielded (STP)
- switch (ISDN) 103

T

- TAG value for BRS 574
- TAGs assignment 532
- TCP connections (DLSw) 449
- TCP neighbors (DLSw) 455
- TCP/IP Host Services commands 135
- TCP/IP Host Services commands table 136
- telnet (IP telnet for bridge) 136
- TFTP 338
 - See also* Trivial File Transfer Protocol
- TFTP protocol (for bridge) 136
- timer add-name command for Duplicate frame filtering process 722
- timer entry command for Name caching process 721
- timer request (IPXWAN) 413
- timer response (IPXWAN) 413
- timer server-response command for Name caching process 721
- token-ring interface 58
 - 802.2 LLC 59
 - configuration of 64
 - dump (monitoring command) 76
 - frame command 67
 - IEEE 802.5 58
 - IEEE 802.5 layout 58
 - media command 66
 - monitoring token-ring 76
 - non-canonical MAC address 58
 - packet-size command 66
 - RIF layout 59
 - route designator 60
 - Routing Information Field (RIF) 59, 60
 - Routing Information Indicator (RII) 59, 60
 - segment number 60
 - set physical-address command 66
 - set rif-timer command 66
 - shielded (STP) 66
 - SNAP 59
 - Source Route Bridge (SRB) 59, 60
 - source-routing command 67
 - speed command 67
 - token-ring commands table 65
 - Transparent Bridge (STB) 60
 - unshielded (UTP) 66
- token-ring interface configuration 64
- token-ring LAN 114
- token-ring LAN for bridging 121
- token-ring spanning tree algorithm 114
- TOS support 332
- traceroute (IP traceroute for bridge) 136
- Transparent Bridge (STB) 60, 112, 113, 121, 130
 - Ethernet LAN 113
 - filtering database 113
 - forwarding table 113

- Transparent Bridge (STB) (*continued*)
 - ISO 8802-1 113
 - MAC sublayer 113
 - spanning tree bridge (STB) 113
 - spanning tree protocol 114
 - token-ring LAN 113
 - transparent bridge process 113
- transparent bridge process 113
- transparent spanning tree frame 130
- triggered updates 301
- Trivial File Transfer Protocol 340
 - client 340
 - message viewing 340
 - server 340
- tunnel (ASRT command) 133
- Tunnel bridge 112, 117, 119
 - Hops count 118
 - IP network 117
 - routing information field (RIF) 118
 - segment number 118
 - Source Route Bridge (SRB) 117
 - transparent bridge (STB) 117
- tunnel bridge commands 132
- tunnel bridge commands table 133

U

- unshielded (UTP) 66
- update (MCF command) 572
- update command for a byte filter list 729
- update command for a Name filter list (NetBIOS Filtering) 728
- update interval (IPX RIP) 406, 417
- update interval (IPX SAP) 409, 417
- Using TFTP 15
- Using Zmodem 16
- UTP
 - See unshielded (UTP)

V

- V.25bis configuration commands for WRS 603
- V.25bis interface for Dial-on-Demand 685, 686
- V.25bis interface in WRS 599, 601
- V.25bis phone numbers for Dial-on-Demand 683
- virtual segment number 451, 455

W

- WAN Reroute
 - Configuration commands 667
 - Implementation
 - Scenario 5: WAN Reroute 667
 - Scenario 6: WAN Reroute using ISDN 672
- WAN Restoral (WRS) 119, 599
 - add device command 602
 - add secondary-circuit command 607
 - add v25-bis-address command 602
 - circuit configuration commands 605

- WAN Restoral (WRS) (*continued*)
 - commands needed via CONFIG Process 601
 - configuration 600
 - configuration commands 606
 - configuration commands table 607
 - data-link command 601
 - Dial Backup 599
 - dial circuit interface 601
 - encapsulator command 606
 - functionality of 599
 - interoperability with IBM 6611 Network Processor 600
 - introduction to WAN Restoral (WRS) 599
 - ISDN configuration commands 604
 - ISDN interface 599
 - primary interface 601
 - protocol address on serial interfaces 601
 - Scenario 3: WAN Restoral with IP, DLSw and Bridging 608
 - Scenario 4: WAN Restoral with IP, DLSw and Bridging using ISDN 641
 - secondary interface 601
 - set calls command 605
 - set destination command 606
 - set idle command 605
 - set local command 603, 604
 - set net command 605
 - V.25bis configuration commands 603
 - V.25bis interface 599, 601
 - WAN Restoral commands 606
 - Wildcard in NetBIOS host name 728
 - WRS
 - See WAN Restoral (WRS)
 - WRS configuration 600

X

- X.25 data-link for bridging 119

ITSO Redbook Evaluation

IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios - Volume I
SG24-4446-02

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at <http://www.redbooks.com>
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redeval@vnet.ibm.com

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes____ No____

If no, please explain:

What other redbooks would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)



Printed in U.S.A.

S624-4446-02

