



FlowPoint™ DSL Router

USER GUIDE

First Edition (April, 1998)

Copyright

FlowPoint provides this publication “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose.

All rights reserved. No part of this book may be reproduced in any form or by any means without written permission from FlowPoint.

Changes are periodically made to the information in this book. They will be incorporated in subsequent editions. FlowPoint may make improvements and/or changes in the product described in this publication at any time.

© Copyright 1995-1998 FlowPoint Corporation

Trademarks

FlowPoint is a trademark of FlowPoint Corporation.

All other trademarks and registered trademarks mentioned in this manual are the sole property of their respective companies.



180 Knowles Drive, Suite 100
Los Gatos, California 95030
Telephone: (408) 364-8300
Fax: (408) 364-8301
Email: support@flowpoint.com

Part Number 222-00388-01

Software License Agreement and Warranties

License Agreement

This product contains certain Software (computer programs, firmware and media) the use of which are subject to this license agreement. If you do not agree with all the terms, you must return this product, all manuals and documentation, and proof of payments, to the place you obtained them for a full refund within 30 days of first acquiring this product. Your written approval is not prerequisite to the validity or enforceability of this agreement and no solicitation of any such written approval by or on behalf of FlowPoint shall be construed as an inference to the contrary.

License and Term

FlowPoint and any applicable sublicensors grant to you a non-exclusive, non-transferable license to use the FlowPoint software programs and related documentation in this package (collectively referred to as the “Software”) on one licensed router. If the FlowPoint product that you acquired is an upgrade, then the terms and conditions of this agreement apply equally to the upgraded product. Any attempted sublicense, assignment, rental, sale or other transfer of the Software or the rights or obligations of this Agreement without the prior written consent of FlowPoint shall be null and void. You agree not to export or re-export this product without prior authorization from the U.S. and other applicable government authorities. This License will automatically terminate without notice to you if you fail to comply with its terms. This Agreement will be covered by the laws of the State of California. The Software and documentation are copyrighted. You may make copies of the Software only for backup and archival purposes. Unauthorized copying, reverse engineering, decompiling, disassembling, and creating derivative works based on the Software are prohibited. Title to the Software is not transferred to you by this license. Ownership and title to the Software and to the actual contents of this package, including the copy of the Software and the media on which it is stored and the associated documentation, are retained by FlowPoint and/or its licensors.

U.S. Government End Users. The [Licensed Product] is a “commercial item,” as that term is defined at 48 C.F.R. 2.101 (OCT 1995), consisting of “commercial computer software” and “commercial computer software documentation,” as such terms are used in 48 C.F.R. 12.212 (SEPT 1995) and is provided to the U.S. Government only as a commercial end item. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (JUNE 1995), all U.S. Government End Users acquire the [Licensed Product] with only those rights set forth herein.

Limited Warranty on Media and Damages Disclaimer

FlowPoint or its distributors or resellers will repair or replace free of charge any defective recording medium on which the Software is recorded if the medium is returned to FlowPoint or its distributor or reseller within ninety (90) days after the purchase of License for the Software. This warranty does NOT cover defects due to accident, or abuse occurring after your receipt of the Software. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM STATE TO STATE.

Limited Warranty on Hardware

FlowPoint warrants that Products delivered hereunder shall be free from defects in materials and workmanship for a period of one (1) year from the date of purchase.

The liability of FlowPoint is limited to replacing or repairing, at Manufacturer's option, any defective Products that are returned F.O.B. Manufacturer's factory, California. In no case are Products to be returned without first obtaining permission and a customer return material authorization number from Manufacturer.

THIS WARRANTY DOES NOT APPLY TO DEFECTS DUE DIRECTLY OR INDIRECTLY TO MISUSE, ABUSE, NEGLIGENCE, ACCIDENT, REPAIRS, OR ALTERATIONS MADE BY THE CUSTOMER OR ANOTHER PARTY OR IF THE FLOWPOINT SERIAL NUMBER HAS BEEN REMOVED OR DEFACED. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM STATE TO STATE.

EXCEPT FOR THE WARRANTY SET FORTH HEREIN, MANUFACTURER DISCLAIMS ALL WARRANTIES WITH REGARD TO THE PRODUCTS, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Hardware and Software Limitations

FlowPoint does not warrant that the Software will be free from error or will meet your specific requirements. You assume complete responsibility for decisions made or actions taken based on information obtained using the Software. Any statements made concerning the utility of the Software are not to be construed as unexpressed or implied warranties.

FLOWPOINT SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS SOFTWARE LICENSE AGREEMENT, THE HARDWARE, OR THE AGREEMENTS OF WHICH THEY ARE A PART OR ANY MEDIA ATTACHMENT, PRODUCT ORDER, SCHEDULE OR TERMS OR CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR OTHER THEORY: A) FOR LOSS OR INACCURACY OF DATA OR (EXCEPT FOR RETURN OF AMOUNTS PAID TO FLOWPOINT THEREFORE), COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES, OR TECHNOLOGY, B) FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES INCLUDING BUT NOT LIMITED TO LOSS OF REVENUES AND LOSS OF PROFITS; HOWEVER CAUSED, WHETHER FOR BREACH OF WARRANTY, BREACH OF CONTRACT, REPUDIATION OF CONTRACT, NEGLIGENCE OR OTHERWISE.

NEITHER FLOWPOINT NOR ANY OF ITS REPRESENTATIVES, DISTRIBUTORS OR OTHER RESELLERS MAKES OR PASSES ON ANY WARRANTY OR REPRESENTATION ON BEHALF OF FLOWPOINT'S THIRD PARTY SUPPLIERS.

Post Warranty Services

Contact FlowPoint for information regarding post-warranty hardware and software services.

Federal Communications Commission (FCC)

Part 15 CLASS B Statement

Section 15.105(b) of the Code of Federal Regulations

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant of Part 15 of the FCC Rules. These limits are

designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION: Any changes or modifications not expressly approved by the party responsible for this device could void the user's authority to operate this equipment.

Canadian D.O.C. Notice

This product conforms with Canadian Class B emissions regulations.
Ce produit se conforme aux règlements d'émission canadienne classe B.

Instructions for Trained Service Personnel Only

CAUTION: Danger of explosion if battery is incorrectly placed. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Approvals

Safety: EN60950, UL 1950, CUL to CSA 22.2 No. 950

Emissions: FCC Part 15 Class B, EN55022/CISPR22 Class B, VCCI Class 2

Immunity: EN50082-1

Table of Contents

Introduction	1
About The Router	1
About This Book	2
How This Book is Organized	3
References	4
Typographic Conventions	4
Chapter 1. Installing And Accessing Configuration Manager	5
About Configuration Manager	5
Hardware Installation	6
Hardware And Software Prerequisites	6
Install Configuration Manager	7
Set your PC to Obtain an IP Address	7
Install Configuration Manager on your PC	8
Access Configuration Manager	8
Instructions	8
Chapter 2. Configuration	11
Important Terminology	11
Important Protocol Notes	13
Collect Your Configuration Information	14
PPP Link Protocol	15
RFC 1483 Link Protocol	24
RFC 1483MER Link Protocol	30
Configuration Tables	32
Configuring PPP with IP Routing	33
Configuring PPP with IPX Routing	34
Configuring PPP with Bridging	35
Configuring RFC 1483 with IP Routing	36
Configuring RFC 1483 with IPX Routing	37
Configuring RFC 1483 with Bridging	38
Configuring RFC 1483MER with IP Routing	39
Mixed Network Protocols Configuration	40
Sample Configurations	41
Sample Configuration 1 — PPP with IP and IPX	41
Sample Configuration 2 — RFC 1483 with IP and Bridging	48
Chapter 3. Configuration Reference	53
Configuration Reference	53
Connect and Login	53
System Settings	55
Remote Router Database	59

IP and IPX Routing Controls	68
Store the Configuration	69
Verify the Router Configuration	70
Disconnect from the Router	71
Chapter 4. Advanced Features And Management Tools	73
Advanced Features	73
Dynamic Host Configuration Protocol (DHCP)	73
Network Address Translation (NAT)	77
Routing Information Protocol (RIP)	78
Management Tools	80
Terminal Window	80
Upgrade/Backup	82
Reboot From Network	84
SNMP Options	85
Chapter 5. Router Feature Descriptions	87
IEEE 802.3 Ethernet	88
Point-To-Point Link Protocol (PPP)	88
Asymmetric Digital Subscriber Line (ADSL)	88
Asynchronous Transfer Mode (ATM)	88
High-Speed Digital Subscriber Line (HDSL)	89
Symmetrical Digital Subscriber Line (SDSL)	89
RFC 1483 Link Protocol	89
RFC 1483MER Link Protocol	89
PAP And CHAP Security	89
Bridging And Routing	90
Bridging	90
Routing	90
Bridging and Routing	91
IEEE 802.1D Bridging	92
IP Routing	92
IPX Routing	92
Bridging And Routing Protocol Filtering	93
IP Internet Firewall	93
Bridge Filtering	93
Simple Network Management Protocol (SNMP)	94
Dynamic Host Configuration Protocol (DHCP)	94
Network Address Translation (NAT)	95
Software Upgrades	95
TELNET	95
Windows GUI Configurator	96
Command Line Interface	96

Chapter 6. Troubleshooting	97
Diagnostic Tools	97
Using LEDs	97
Troubleshooting Help File	99
History Log	99
Ping Command	100
Investigating Hardware Installation Problems	101
Check the LEDs to Solve Common Hardware Problems	101
Problems with the Terminal Window Display	101
Problems with the Factory Configuration	102
Investigating Software Configuration Problems	102
Problems Connecting to the Router	102
Problems with the Login Password	103
Problems Accessing the Remote Network	103
How To Obtain Technical Support	105
Appendix A. Software Specifications	107
Appendix B. Network Information Worksheets	108
Appendix C. Command Line Interface	116
Why Use The Command Line Interface?	116
Connecting The Router To The PC	117
Accessing The Command Line Interface	118
Appendix D. Changing Configuration Switch Settings	120
Configuration Switch Settings	120
Appendix E. Subnetwork Tables	121
Glossary	123
Index	131

Introduction

About The Router

This DSL router belongs to the FlowPoint Business DSL family which features a range of DSL solutions for the Corporate environment, the small office, and the single user. It provides high-speed digital access to the Internet and Corporate Intranets. The single-user version offers the same high-speed access benefits for telecommuters and home and remote office workers.

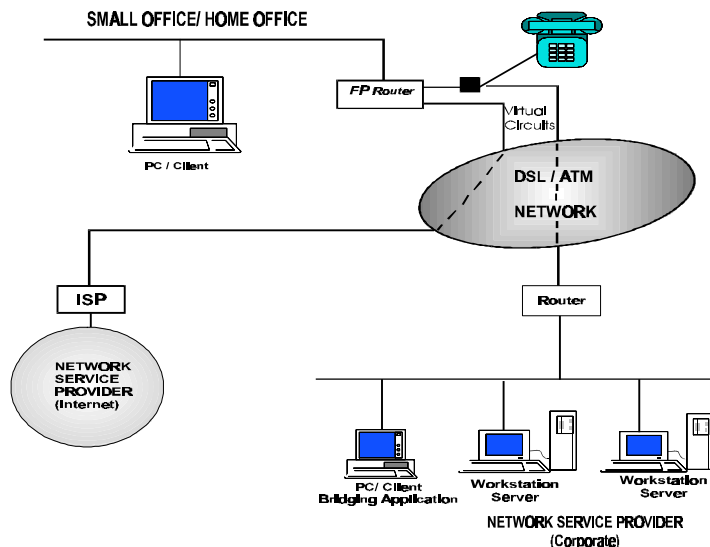
The FlowPoint DSL router features industry-standard DSL and 10Base-T Ethernet interfaces which provide data rates ranging from 144 Kbps to up to 8 Mbps depending on the DSL model. For model-specific information, please refer to the accompanying *Quick Start Guide*.

The FlowPoint DSL router supports IEEE 802.1D/transparent bridging and IP and IPX routing between Ethernet LAN networks across a WAN resource.

The following FlowPoint software features are available on all DSL routers:

- Configuration Manager, an easy-to-use Windows-based management application.
- Several built-in features that let users connect to a Network Service Provider (NSP) in minutes.
- Dynamic IP address assignment which lets an ISP issue an address upon initial connection.
- DHCP: the router's built-in Dynamic Host Configuration Protocol (DHCP) server also automatically assigns IP addresses to all workstations on the LAN.
- NAT: the router supports Network Address Translation which lets multiple users of a FlowPoint router simultaneously share one Internet connection.
- DNS Relay: This feature allows for automatic name resolution when no DNS information is configured by the user.

Following is a sample network configuration:



About This Book

This *FlowPoint User Guide* contains an introduction to the FlowPoint router and provides the steps and basic information needed to configure the router. Configuration of network connections, bridging, routing, and security features are also described.

Note: Hardware installation instructions and hardware reference information are described in the *Quick Start Guide*.

Target Audience

This book is intended for business users, small home and remote office users, and other networking professionals who are installing and configuring the router for bridged and routed networks.

Note: If you only intend to connect to the Internet, use the *Quick Start Guide* and the Quick Start program.

If you want to connect to the Internet and use bridging or IPX, run the Quick Start program first, and then use the Configuration Manager program to add options.

How This Book is Organized

This *User Guide* is intended to help you easily configure and use the FlowPoint Router. The guide is divided into six parts:

Chapter 1, “Installing and Accessing Configuration Manager”, explains how to install and access Configuration Manager running under Microsoft Windows.

Chapter 2, “Configuration”, contains configuration information and tables that review the steps needed to configure the router for each Link Protocol and Network Protocol combination.

Chapter 3, “Configuration Reference”, lists and explains each configuration button in Configuration Manager.

Chapter 4, “Advanced Features and Management Tools”, describes features used for complex configuration tasks and a set of tools used for file system management and software maintenance.

Chapter 5, “Router Feature Descriptions”, lists and describes industry-standard protocols, security features, compression algorithms, and network management tools.

Chapter 6, “Troubleshooting”, provides suggestions for locating the source of problems depending upon the trouble symptom.

Additionally, **Appendices A-E** provide software and configuration references. A **Glossary** and an **Index** are provided at the back of this book.

References

Command Line Interface

Contains configuration and reference material for the Command Line Interface, advanced topics such as bridging and routing operations, PPP addressing, standard configurations for the PPP, RFC 1483, and RFC 1483MER Link Protocols, and a description of network management features. This manual is delivered on a DOS diskette as a Word for Windows 6.0 document and is supplied with the router.

Quick Start Guide

Describes the configuration process involved in setting up your router for an ATM-based service to your a Network Service Provider.

Typographic Conventions

The following figure summarizes the conventions used in this guide:

Item	Type Face	Example
Words defined in glossary, book titles, figure captions	Italics	Refer to <i>Installing the Hardware</i> .
Menu choices, keys and button names in instructions	Bold	Click Tools .
Examples showing you what to type	Mono-spaced font	Enter the router system name, for example: Router1
File names, keywords	Upper case	Copy file CFGMGR.EXE

Chapter 1. Installing And Accessing Configuration Manager

This chapter describes how to install and access FlowPoint's **Configuration Manager** running under Microsoft Windows.

About Configuration Manager

Configuration Manager is an easy-to-use, point-and-click graphical user interface (GUI) used to perform all the configurations described in this guide. It is a Windows-based application and can run under Windows for Workgroups, Windows 95, and Windows NT.

Configuration Manager allows you to configure the router's system settings, routing and bridging function, remote router access, bandwidth management, and security features.

It also includes a set of tools designed to simplify some configuration tasks. Personal computer hardware and software prerequisites are listed in the following section.

An Ethernet LAN connection between the router and the personal computer is needed to configure the router using the Graphical User Interface.

Note: If you are simply connecting to the Internet, use the *Quick Start* application and guide instead of this document.

Important

There will be a few “unusual” situations where the user will have to use the **Command Line Interface** (instead of the Configuration Manager program) to configure the FlowPoint router:

- IP address initialization and router configuration for **non**-Windows-based platforms (such as Macintosh and UNIX)
- Advanced settings of DHCP and filters
- Changing an existing IP address
- Setting traffic-shaping parameters

The Command Line Interface (CLI) requires a console or Telnet connection. Detailed information about installing and accessing the CLI is described in Appendix C, *Command Line Interface (CLI)*.

Hardware Installation

This chapter assumes that you have already installed the router hardware as described in the *Hardware Installation* section of the accompanying *Quick Start Guide*.

Please note that *Hardware Reference* information specific to your router model is also found in the *Quick Start Guide*.

Hardware And Software Prerequisites

The Configuration Manager program requires the following hardware and system configuration:

- IBM-compatible Personal Computer
- Ethernet network interface card
- 8.0 MB of available hard disk space (5.0 MB for Configuration Manager and online documentation plus up to 3.0 MB for the files to be installed in the \WINDOWS\SYSTEM directory)
- Microsoft Windows 3.1, Windows for Workgroups, Windows 95, or Windows NT
- Winsock 1.1-compliant TCP/IP stack installed and running on your PC (included with Windows 95)

Install Configuration Manager

To access the FlowPoint Configuration Manager, you will first configure your PC to obtain an IP address automatically (DHCP) and then install Configuration Manager.

Note: Windows 95 is assumed throughout this section.

Set your PC to Obtain an IP Address

This section assumes that you have already:

- connected the router's cables.
- powered on the router.

◇ Instructions

1. Click the **Start** button on your PC desktop.
2. Click **Settings, Control Panels, and Network**.
3. You are now in the **Network** window. In the **Configuration Tab** page, double-click **TCP/IP** (for your network adapter).



4. Click the **DNS Configuration** tab and select **Disable DNS**.
5. In the **TCP/IP Properties** window, enable **Obtain an IP address automatically** by clicking the appropriate radio button.
6. Click **OK**.
7. Answer **Yes** to "Do you want to restart your computer?" Your computer will restart. Your PC will now learn an IP address from the router.

Install Configuration Manager on your PC

This section assumes that you have already:

- connected the router's cables.
- powered the router on.
- set your PC to obtain an IP address.
- rebooted your PC.

◇ Instructions

The three diskettes included in the router box contain the Configuration Manager and Quick Start programs and an electronic copy of the *Command Line Interface* manual.

1. To install the Configuration Manager program, insert diskette #1 in drive A: (or B:) of your PC.
2. Click the **Start** button on your PC desktop.
3. Click **Run**. In the **Run** dialog box, type:

A:\SETUP.EXE (or B:\SETUP.EXE)

The Configuration Manager program will be installed in the C:\DSL directory by default. However, you may choose to install it in another directory.

Access Configuration Manager

Instructions

1. Click the **Start** button on your PC desktop.
2. Select **Programs**.
3. Select **FlowPoint DSL Tools**.
4. Click the **Configuration Manager** icon.

Configuration Manager's main menu will appear as shown below:



You are now ready to start configuring your router. Refer to chapter 2 for configuration instructions and information.

Chapter 2. Configuration

This chapter contains configuration information, instructions, and tables for the three Link Protocols supported by the FlowPoint router. Configuration of network connections, bridging, routing, and security features are essentially the same for all DSL routers (ADSL, ATM, SDSL, etc.), unless otherwise noted. Two sample configurations are provided at the end of the chapter.

The information needed to configure the router is contingent on the chosen Link Protocol. It is therefore necessary to know which Link Protocol you are using (this is determined by your Network Service Provider) to be able to refer to the configuration sections that apply to your setup.

How to Use This Chapter

1. Collect the relevant information as described in the following *Collect Your Configuration Information* section.
2. Find the configuration table that fits your particular Network Protocol/Link Protocol association in the *Configuration Tables* section. These tables are designed to provide easy step-by-step instructions.
3. You may want to refer to the sample configurations at the end of the chapter.

Important Terminology

You should familiarize yourself with the following terminology as it will be used throughout this chapter.

Target router

Router that you are configuring. Also referred to as **local** router.

Remote routers

All the routers to which the target (local) router may connect.

Remote router database

Database which resides in the target router and contains information about the remote routers to which the target router may connect.

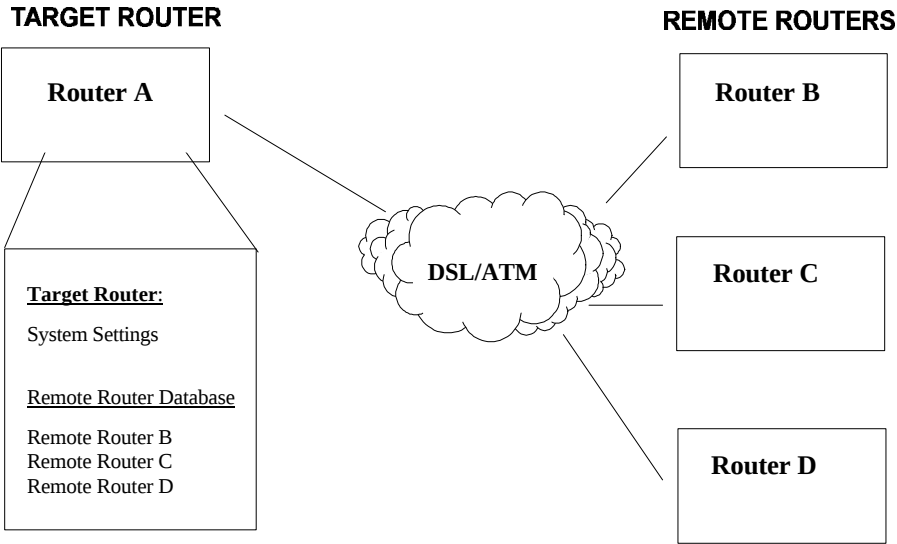
Remote router entry

Entry about a remote router in the target router database. A remote router entry defines:

- Connection parameters
- Security features
- Route addressing and bridging functions

The following diagram illustrates these key words and concepts.

Configuration Process for Router A



Important Protocol Notes

For best performance, we suggest that you use the PPP/IP protocol combination. Authentication should be disabled on both ends to avoid using passwords.

The protocol combination RFC 1483/Bridging is the easiest to configure. DHCP should be disabled on one end of the connection to avoid conflicts.

The protocol combination RFC 1483MER/IP allows the router to appear as a Bridge on the DSL link and as a router on the Ethernet. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment.

Collect Your Configuration Information

This section describes the configuration information for each Link Protocol/Network Protocol association. It is organized as follows:

- PPP Link Protocol with IP, or IPX, or Bridging Network Protocol
- RFC 1483 Link Protocol with IP, or IPX, or Bridging Network Protocol
- RFC 1483MER Link Protocol with IP Network Protocol

Instructions — Please read the following carefully:

1. Determine which Link Protocol/Network Protocol association you are using. This information is obtained from your Network Service Provider (NSP).
2. To locate the Link/Network information that applies to your situation, use the following list:

PPP Link Protocol with:

- IP Routing Network Protocol, page 15.
- IPX Routing Network Protocol, page 19.
- Bridging Network Protocol, page 22.

RFC 1483 Link Protocol with:

- IP Routing Network Protocol, page 24.
- IPX Routing Network Protocol, page 27.
- Bridging Network Protocol, page 29.

RFC 1483MER Link Protocol with:

- IP Routing Network Protocol, page 30.

3. You will then enter the information associated with your Link/Network protocols in the various screens of Configuration Manager. To do so, turn to the *Configuration Tables* section where step-by-step configuration instructions are provided for your particular Link Protocol/Network Protocol association.

Note: Use the blank Network Information Worksheets in Appendix B to collect your network information.

PPP Link Protocol

If you are using the PPP Link Protocol, select the Network Protocol that applies to your situation: IP, or IPX, or Bridging. Collect the information described in the appropriate section. This data will be later used to configure your router using Configuration Manager (see *Configuration Tables*, starting on page 32).

◇ IP Routing Network Protocol

System Names and Authentication Passwords

- **For the Target Router**

This information is defined by the user.

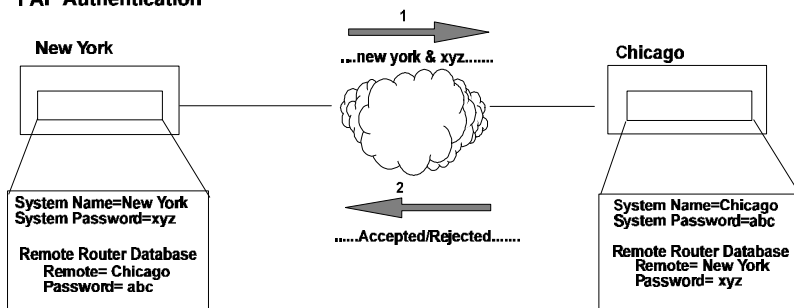
You must choose a name and authentication password for the target router. They are used by a remote router to authenticate the target router.

- **For the Remote Site(s)**

This information is obtained from the Network Service Provider.

For each remote site, you must have the site name and its authentication password. They are used by this target router to authenticate the remote end. The name and password are used in both PAP and CHAP authentication. The following diagram shows how this information is used.

PAP Authentication



Note: A sample configuration containing Names and Passwords is provided in the section *Sample Configuration — Configuration 1*, starting on page 41.

VPI and VCI Numbers

The VPI/VCI numbers are preconfigured. Make sure that these numbers are right for your setup. If in doubt, check with your Network Service Provider.

If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider. These numbers identify the remote destination and must, therefore, be unique for each remote.

DNS Internet Account Information (optional)

This information is obtained from the Network Service Provider.

Consult with your Network Service Provider to find out if you need to enter the following information:

- DNS Server Address
- DNS Second Server Address
- DNS Domain Name

Note: If you intend to connect to the Internet only, enter this information using the Internet Quick Start configurator.

IP Routing Addresses

- **For the Ethernet Interface**

This information is defined by the user or the Network Administrator.

Ethernet IP Address (Local LAN)

An Ethernet LAN IP address and subnet mask are required for the router's local Ethernet LAN connection.

Note: An **Ethernet route** is usually defined when there are multiple routers on the Ethernet that cannot exchange routing information between them. This feature is normally not used except in very special circumstances.

- **For the DSL WAN Interface**

This information is defined by the Network Service Provider.

Source (Target/Local) WAN Port Address

If Network Address Translation is enabled, you must specify a source WAN IP address for the WAN connection to the remote router if IP address negotiation under PPP does not provide one.

Check with your system administrator for details on whether the router must communicate in numbered or unnumbered mode and what addresses are required.

Remote WAN Address

You may need to specify a remote WAN IP address for the WAN connection to the remote router depending on IP address negotiation under PPP.

Check with your system administrator for details on whether the router must communicate in numbered or unnumbered mode and what addresses are required.

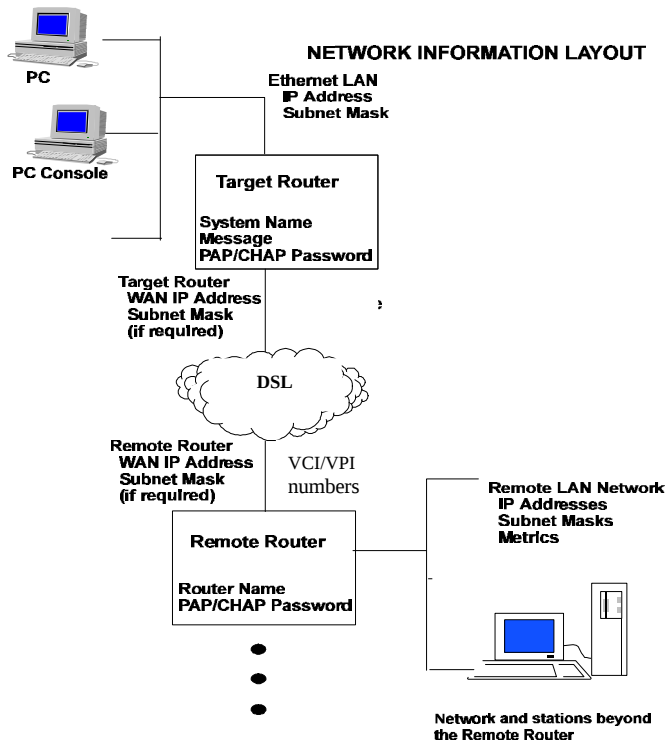
TCP/IP Remote Routes

An IP route includes an IP address, subnet mask, and metric (a number representing the perceived cost in reaching the remote network or station).

A **TCP/IP Default Route** should be designated in the routing table for all traffic that cannot be directed to other specific routes.

You will need to define the default route to a remote router or, if required due to special circumstances, define an Ethernet gateway. There can be only one default route specified.

Note: It is often helpful to draw a diagram including all locations, addresses, routes names, etc. This diagram shows the network information required for configuration of the target router. If you need to configure both ends of the WAN link, you will need to label all information for the network.



◇ IPX Routing Network Protocol

System Names and Authentication Passwords

- **For the Target Router**

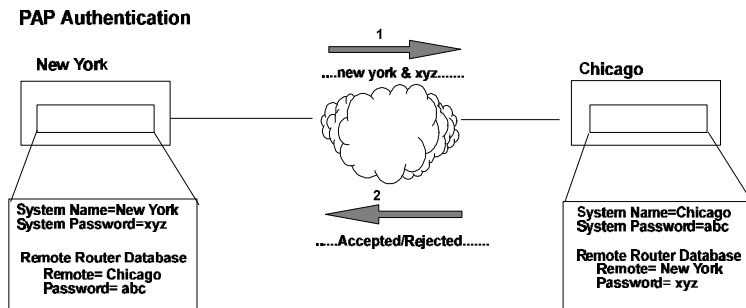
This information is defined by the user.

You must choose a name and authentication password for the target router. They are used by a remote router to authenticate the target router.

- **For the Remote Site(s)**

This information is obtained from the Network Service Provider.

For each remote site, you must have the site name and its authentication password. They are used by this target router to authenticate the remote end. The name and password are used in both PAP and CHAP authentication. The following diagram shows how this information is used.



Note: A sample configuration containing Names and Passwords is provided in the section *Sample Configuration — Configuration 1*, starting on page 41.

VPI and VCI Numbers

The VPI/VCI numbers are preconfigured. Make sure that these numbers are right for your setup. If in doubt, check with your Network Service Provider.

If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider. These numbers identify the remote destination and must, therefore, be unique for each remote.

IPX Routing Entries

The following information is defined by and obtained from your Network Administrator.

Note: **IPX routes** define a path to a specific destination. They are primarily needed by the routers to allow the servers and clients to exchange packets. A path to a file server will be based on the Internal Network Number of the server.

A path to a client will be based on the External Network Number (Ethernet) of the client.

- **Internal Network Number**

It is a logical network number that identifies an individual Novell server. It is needed to specify a route to the services (i.e., file services, print services) that Novell offers. It must be a unique number.

- **External Network (a.k.a. IPX Network Number)**

It refers to a physical LAN/wire network segment to which servers, routers, and PCs are connected (Ethernet cable-to-router segment). It must be a unique number.

- **WAN Network Number**

Important: This number is part of the routing information. It is used to identify the WAN segment between the two routers. Note that only both routers need to have the WAN Network Number configured.

- **SAP (Service Advertisement Protocol)**

SAP entries should reflect primary logon servers for the clients on the local LAN. Only the servers on the remote side of the link have to be entered. Local servers do not need to be entered.

- **Frame type**

With local servers on your LAN, make sure to select the proper frame type for the IPX network number. To determine this, consult with your network administrator. When you have only NetWare clients on your LAN, leave the default (802.2) selected as most clients support any type. The frame type choices are:

- 802.2** Default recommended by Novell
- 802.3** Other most common type
- DIX** For DEC, Intel, Xerox; this setting is also referred to as “Ethernet II”, and is rapidly becoming obsolete.

◇ Bridging Network Protocol

System Names and Authentication Passwords

- **For the Target Router**

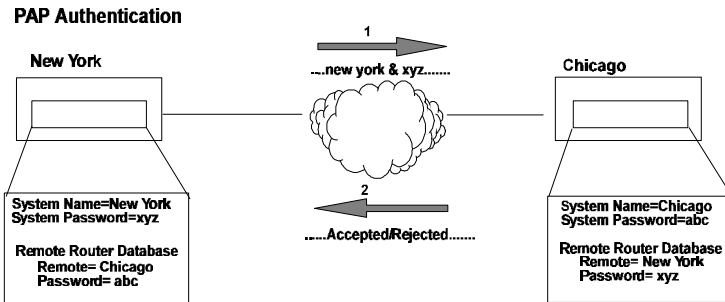
This information is defined by the user.

You must choose a name and authentication password for the target router. They are used by a remote router to authenticate the target router.

- **For the Remote Site(s)**

This information is obtained from the Network Service Provider.

For each remote site, you must have the site name and its authentication password. They are used by this target router to authenticate the remote end. The name and password are used in both PAP and CHAP authentication. The following diagram shows how this information is used.



Note: A sample configuration containing Names and Passwords is provided in the section *Sample Configuration, Configuration 1*, page 41.

VPI and VCI Numbers

The VPI/VCI numbers are preconfigured. Make sure that these numbers are right for your setup. If in doubt, check with your Network Service Provider.

If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider. These numbers identify the remote destination and must, therefore, be unique for each remote.

DNS Internet Account Information (optional)

This information is obtained from the Network Service Provider.

Consult with your Network Service Provider to find out if you need to enter the following information:

- DNS Server Address
- DNS Second Server Address
- DNS Domain Name

Note: If you intend to connect to the Internet only, enter this information using the Internet Quick Start configurator. RFC 1483 Link Protocol

If you are using the RFC 1483 Link Protocol, select the Network Protocol that applies to your situation: IP, or IPX, or Bridging. Collect the information described in the appropriate section. This data will be later used to configure your router using Configuration Manager (see *Configuration Tables*, starting on page 32).

RFC 1483 Link Protocol

If you are using the RFC 1483 Link Protocol, select the Network Protocol that applies to your situation: IP, or IPX, or Bridging. Collect the information described in the appropriate section. This data will be later used to configure your router using Configuration Manager (see *Configuration Tables*, starting on page 32).

◇ IP Routing Network Protocol

VPI and VCI Numbers

The VPI/VCI numbers are preconfigured. Make sure that these numbers are right for your setup. If in doubt, check with your Network Service Provider.

If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider. These numbers identify the remote destination and must, therefore, be unique for each remote.

DNS Internet Account Information (optional)

This information is obtained from the Network Service Provider.

Consult with your Network Service Provider to find out if you need to enter the following information:

- DNS Server Address
- DNS Second Server Address
- DNS Domain Name

Note: If you intend to connect to the Internet only, enter this information using the Internet Quick Start configurator.

IP Routing Entries

- **For the Ethernet Interface**

This information is defined by the user or the Network Administrator.

Ethernet IP Address (Local LAN)

An Ethernet LAN IP address and subnet mask are required for the router's local Ethernet LAN connection.

TCP/IP Ethernet Routes

You normally do not need to define an Ethernet IP route. An Ethernet IP route consists of an IP address, a mask, a metric, and a gateway. An Ethernet route is usually defined when there are multiple routers on the Ethernet which cannot exchange routing information between them.

- **For the DSL WAN Interface**

This information is obtained from the Network Administrator.

Source (Target/Local) WAN Port Address

If NAT is enabled, you must specify a source WAN IP address for the WAN connection to the remote router. Check with your system administrator for details.

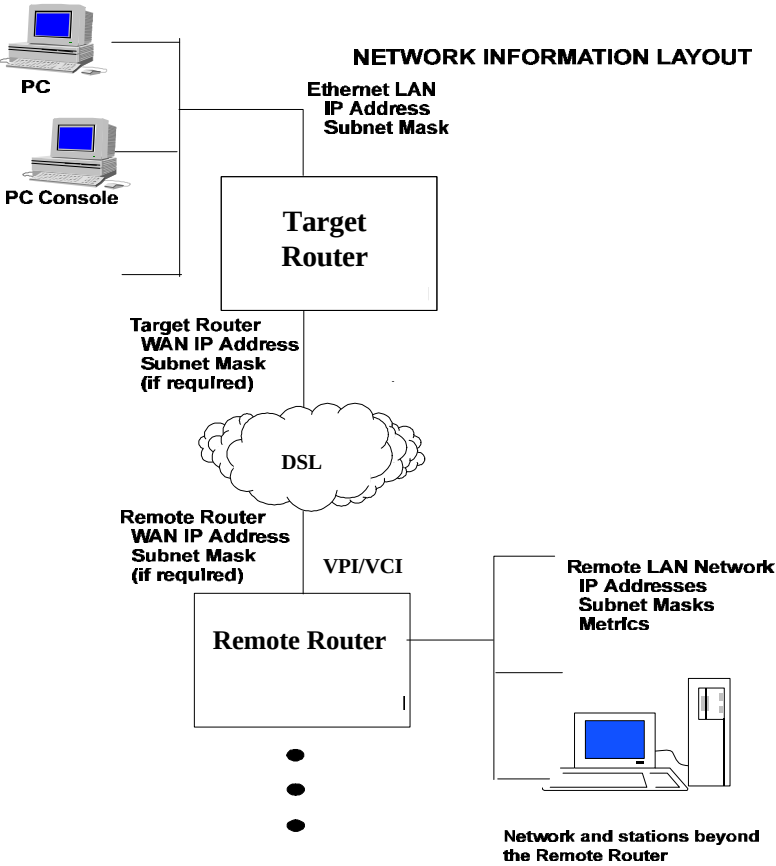
If NAT is not enabled, you may need to specify a source WAN IP address for the WAN connection to the remote router. Check with your system administrator for details.

TCP/IP Remote Routes

An IP route includes an IP address, subnet mask, and metric (a number representing the perceived cost in reaching the remote network or station).

A **TCP/IP Default Route** default route should be designated in the routing table for all traffic that cannot be directed to other specific routes. You will need to define the default route to a remote router or, if required due to special circumstances, define an Ethernet gateway. There can be only one default route specified.

Note: It is often helpful to draw a diagram including all locations, addresses, router names, etc. The following diagram shows the network information required to configure *only* the target router's side. If you need to configure both ends of the WAN link, you will want to label all information for the network.



◇ IPX Routing Network Protocol

VPI and VCI Numbers

The VPI/VCI numbers are preconfigured. Make sure that these numbers are right for your setup. If in doubt, check with your Network Service Provider.

If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider. These numbers identify the remote destination and must, therefore, be unique for each remote.

IPX Routing Entries

This information is defined by the user or the Network Administrator.

Note: IPX routes define a path to a specific destination. They are primarily needed by the routers to allow the servers and clients to exchange packets. A path to a file server will be based on the Internal Network Number of the server.

A path to a client will be based on the External Network Number (Ethernet) of the client.

- **Internal Network Number**

It is a logical network number that identifies an individual Novell server. It is needed to specify a route to the services (i.e. file services, print services) that Novell offers. It must be a unique number.

- **External Network (a.k.a. IPX Network Number)**

It refers to a physical LAN/wire network segment to which servers, routers, and PCs are connected (Ethernet cable-to-router segment). It must be a unique number.

- **WAN Network Number**

Important: This number is part of the routing information.

It is used to identify the WAN segment between the two routers only. Note that only both routers need to have the WAN Network Number configured.

- **SAP (Service Advertisement Protocol)**

SAP entries should reflect primary logon servers for the clients on the local LAN. Only the servers on the remote side of the link have to be entered. Local servers do not need to be entered.

- **Frame type**

With local servers on your LAN, make sure to select the proper frame type for the IPX network number. To determine this, consult with your network administrator. When you have only NetWare clients on your LAN, leave the default (802.2) selected as most clients support any type. The frame type choices are:

- 802.2** Default recommended by Novell
- 802.3** Other most common type
- DIX** For DEC, Intel, Xerox; this setting is also referred to as “Ethernet II”, and is rapidly becoming obsolete.

◇ Bridging Network Protocol

VPI and VCI Numbers

The VPI/VCI numbers are preconfigured. Make sure that these numbers are right for your setup. If in doubt, check with your Network Service Provider.

If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider.

These numbers identify the remote destination and must, therefore, be unique for each remote.

DNS Internet Account Information (optional)

This information is obtained from the Network Service Provider.

Consult with your Network Service Provider to find out if you need to enter the following information:

- DNS Server Address
- DNS Second Server Address
- DNS Domain Name

Note: If you intend to connect to the Internet only, enter this information using the Internet Quick Start configurator.

RFC 1483MER Link Protocol

The RFC 1483MER (MAC Encapsulated Routing) Link Protocol is only used in conjunction with the IP Network Protocol. With RFC 1483MER, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment.

Collect the information described below. This data will be later used to configure your router using Configuration Manager (see *Configuration Tables*, starting on page 32).

◇ IP Routing Network Protocol

VPI and VCI Numbers

The VPI/VCI numbers are preconfigured. Make sure that these numbers are right for your setup. If in doubt, check with your Network Service Provider.

If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider.

These numbers identify the remote destination and must, therefore, be unique for each remote.

DNS Internet Account Information (optional)

This information is obtained from the Network Service Provider.

Consult with your Network Service Provider to find out if you need to enter the following information:

- DNS Server Address
- DNS Second Server Address
- DNS Domain Name

Note: If you intend to connect to the Internet only, enter this information using the Internet Quick Start configurator.

IP Routing Entries

- **For the Ethernet Interface**

This information is defined by the user or the Network Administrator.

Ethernet IP Address (Local LAN)

An Ethernet LAN IP address and subnet mask are required for the router's local Ethernet LAN connection.

TCP/IP Ethernet Routes

You normally do not need to define an Ethernet IP route. An Ethernet IP route consists of an IP address, a mask, a metric, and a gateway. An Ethernet route is usually defined when there are multiple routers on the Ethernet which cannot exchange routing information between them.

- **For the DSL WAN Interface**

This information is obtained from the Network Administrator or the NSP.

Source (Target/Local) WAN Port Address and Mask

You must specify a Source WAN IP address for the WAN connection to the remote router (whether or not NAT is enabled). The Source WAN Address is the address of the local router on the remote network. The mask is the mask used on the remote network. Check with your system administrator for details.

TCP/IP Remote Routes

When using RFC 1483MER, the IP route includes an IP address, subnet mask, metric (a number representing the perceived cost in reaching the remote network or station), and a gateway. The gateway address that you enter is the address of a router on the remote LAN. Check with your system administrator for details.

A **TCP/IP Default Route** default route should be designated in the routing table for all traffic that cannot be directed to other specific routes. You will need to define the default route to a remote router or, if required due to special circumstances, define an Ethernet gateway. There can be only one default route specified.

Configuration Tables

The following tables give you step-by-step instructions for standard configurations of the following Network Protocols / Link Protocol associations:

- PPP Link Protocol with IP Routing Network Protocol, p. 33
- PPP Link Protocol with IPX Routing Network Protocol, p. 34
- PPP Link Protocol with Bridging Network Protocol, p. 35
- RFC 1483 Link Protocol with IP Routing Network Protocol, p. 36
- RFC 1483 Link Protocol with IPX Routing Network Protocol, p. 37
- RFC 1483 Link Protocol with Bridging Network Protocol, p. 38
- RFC 1483MER Link Protocol with IP Routing Network Protocol, p. 39
- Combinations of two or more of the preceding Link Protocols Network Protocols, p. 40

Note: Blank Network Configuration Worksheets are available in Appendix B.

How to use the tables

This section assumes that you have already installed the Configuration Manager program on your PC and know how to access it (if not, refer to Chapter 1 for details).

Click the buttons of Configuration Manager in the order that they are given in the Configuration tables' *Step/Button* column. Each button is associated with a configuration screen. Follow the instructions given in each configuration screen.

The *Settings* column contains comments or specific configuration settings that you should enter for your chosen Network Protocol/Link Protocol.

If you need additional information on certain configuration points in a table, use the *Configuration Reference* column to easily locate this information.

Configuration examples are provided at the end of this chapter.

Configuring PPP with IP Routing

This table outlines a standard configuration for the PPP Link Protocol with the IP Routing Network Protocol.

PPP with IP Routing		
STEP/BUTTON	SETTINGS	CONFIGURATION REFERENCE
Connect		<i>Connect and Login, p. 53</i>
System Settings		
System Name	Required	<i>System Settings, p. 55</i>
System Message	Optional	<i>System Settings, p. 55</i>
Authentication Password	Required	<i>System Settings, p. 55</i>
Ethernet IP Address	As required	<i>System Settings, p. 55</i>
DHCP Settings	Already enabled; additional settings may be required	<i>System Settings, p. 55, and DHCP, p. 73</i>
Change Login	Optional	<i>System Settings, p. 55</i>
Remote Routers		
New Entry	Enter: Remote Name	<i>Remote Router Database, p. 59</i>
Link Protocol/PVC	Select: PPP Enter: VPI/VCI numbers	<i>Remote Router Database, p. 59</i>
Security Remote's Password	Choose security level Enter: password	<i>Remote Router Database, p. 59</i>
Bridging On/Off	Select: OFF	<i>Remote Router Database, p. 59</i>
TCP/IP Route Addresses	Enter required information	<i>Remote Router Database, p. 59</i>
If NAT is enabled: TCP/IP Route Addresses Advanced	Enter: Source WAN Port Address (if required by ISP)	<i>Remote Router Database, p. 59, and NAT, p. 77</i>
If NAT is not enabled: TCP/IP Route Addresses Advanced	Enter: Source WAN Port Address (if required by ISP)	<i>Remote Router Database, p. 59,</i>
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Select: ON (Optional)	<i>IP and IPX Routing Controls, p. 68</i>
IPX Routing	Select: OFF	<i>IP and IPX Routing Controls, p. 68</i>
Store Reboot		<i>Store the Configuration, p. 69</i>
Exit		

Configuring PPP with IPX Routing

This table outlines a standard configuration for the PPP Link Protocol with the IPX Routing Network Protocol.

PPP with IPX Routing		
STEP/BUTTON	SETTINGS	CONFIGURATION REFERENCE
Connect		<i>Connect and Login, p. 53</i>
System Settings		
System Name	Required	<i>System Settings, p. 55</i>
System Message	Optional	<i>System Settings, p. 55</i>
Authentication Password	Required	<i>System Settings, p. 55</i>
Ethernet IP Address	As required	<i>System Settings, p. 55</i>
DHCP Settings	Already enabled	<i>System Settings, p. 55, DHCP, p. 73</i>
Change Login	Optional	<i>System Settings, p. 55</i>
Ethernet IPX Network #	Enter: IPX Network # Frame Type	<i>System Settings, p. 55</i>
Remote Routers		
New Entry	Enter: Remote Name	<i>Remote Router Database, p. 59</i>
Link Protocol/PVC	Select: PPP Enter: VPI/VCI Numbers	<i>Remote Router Database, p. 59</i>
Security Remote's Password	Choose security level Enter: Password	<i>Remote Router Database, p. 59</i>
Bridging On/Off	Select: OFF	<i>Remote Router Database, p. 59</i>
IPX Routes Add	Enter appropriate info	<i>Remote Router Database, p. 59</i>
IPX SAPs Add, Modify	Enter appropriate info Enter WAN Network #	<i>Remote Router Database, p. 59</i>
IP and IPX Routing		
TCP/IP Routing	Select: OFF	<i>IP and IPX Routing Controls, p. 68</i>
IPX Routing	Select: ON	<i>IP and IPX Routing Controls, p. 68</i>
Store Reboot		<i>Store the Configuration, p. 69</i>
Exit		

Configuring PPP with Bridging

This table outlines a standard configuration for the PPP Link Protocol with the Bridging Network Protocol.

PPP with Bridging		
STEP/BUTTON	SETTINGS	CONFIGURATION REFERENCE
Connect		<i>Connect and Login</i> , p. 53
System Settings		
System Name	Required	<i>System Settings</i> , p. 55
System Message	Optional	<i>System Settings</i> , p. 55
Authorization Password	Required	<i>System Settings</i> , p. 55
DHCP Settings	Already enabled;	<i>System Settings</i> , p. 55 and <i>DHCP</i> , p. 73
Change Login	Optional	<i>System Settings</i> , p. 55
Remote Routers		
New Entry	Enter: Remote Name	<i>Remote Router Database</i> , p. 59
Link Protocol/PVC	Select: PPP Enter: VPI/VCI	<i>Remote Router Database</i> , p. 59
Security Remote's Password	Choose security level Enter: Password	<i>Remote Router Database</i> , p. 59
Bridging On/Off	Select: ON	<i>Remote Router Database</i> , p. 59
IP and IPX Routing		
IP Routing	Select: OFF	<i>IP and IPX Routing Controls</i> , p. 68
IPX Routing	Select: OFF	<i>IP and IPX Routing Controls</i> , p. 68
Store Reboot		<i>Store the Configuration</i> , p. 69
Exit		

Configuring RFC 1483 with IP Routing

This table outlines a standard configuration for the RFC 1483 Link Protocol with the IP Routing Network Protocol.

RFC 1483 with IP Routing		
STEP/BUTTON	SETTINGS	CONFIGURATION REFERENCE
Connect		<i>Connect and Login</i> , p. 53
System Settings		
System Message	Optional	<i>System Settings</i> , p. 55
Ethernet IP Address	As required	<i>System Settings</i> , p. 55
DHCP Settings	Already enabled; additional settings may be required	<i>System Settings</i> , p. 55, and <i>DHCP</i> , p. 73
Change Login	Optional	<i>System Settings</i> , p. 55
Remote Routers		
New Entry	Enter: Remote Name	<i>Remote Router Database</i> , p. 59
Link Protocol/PVC	Select: RFC1483 Enter: VPI/VCI Numbers	<i>Remote Router Database</i> , p. 59
Bridging On/Off	Select: OFF	<i>Remote Router Database</i> , p. 59
TCP/IP Route Addresses Add	Enter: explicit or default route	<i>Remote Router Database</i> , p. 59
If NAT is enabled: TCP/IP Route Addresses, Advanced	Enter: Source WAN Port Address	<i>Remote Router Database</i> , p. 59, and <i>NAT</i> , p. 77
If NAT is OFF: TCP/IP Route Addresses, Advanced	You may need to enter a Source WAN Port Address	<i>Remote Router Database</i> , p. 59 and <i>NAT</i> , p. 77
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Select: ON (Optional)	<i>IP and IPX Routing Controls</i> , p. 68
IPX Routing	Select: OFF	<i>IP and IPX Routing Controls</i> , p. 68
Store Reboot		<i>Store the Configuration</i> , p. 69
Exit		

Configuring RFC 1483 with IPX Routing

This table outlines a standard configuration for the RFC 1483 Link Protocol with the IPX Routing Network Protocol.

RFC 1483 with IPX Routing		
STEP/BUTTON	SETTINGS	CONFIGURATION REFERENCE
Connect		<i>Connect and Login, p. 53</i>
System Settings		
System Message	Optional	<i>System Settings, p. 55</i>
Ethernet IP Address	As required	<i>System Settings, p. 55</i>
DHCP Settings	Already enabled	<i>System Settings, p. 55, DHCP, p. 73</i>
Ethernet IPX Network #	Enter: IPX Network # Frame Type	<i>System Settings, p. 55</i>
Change Login	Optional	<i>System Settings, p. 55</i>
Remote Routers		
New Entry	Enter: Remote Name	<i>Remote Router Database, p. 59</i>
Link Protocol/PVC	Select: RFC1483 Enter: VPI/VCI Numbers	<i>Remote Router Database, p. 59</i>
Bridging On/Off	Select: OFF	<i>Remote Router Database, p. 59</i>
IPX Routes Add	Enter appropriate information	<i>Remote Router Database, p. 59</i>
IPX SAPs Add Modify	Enter appropriate information Enter WAN Network Number	<i>Remote Router Database, p. 59</i>
IP and IPX Routing		
TCP/IP Routing	Select: OFF	<i>IP and IPX Routing Controls, p. 68</i>
IPX Routing	Select: ON	<i>IP and IPX Routing Controls, p. 68</i>
Store Reboot		<i>Store the Configuration, p. 69</i>
Exit		

Configuring RFC 1483 with Bridging

This table outlines a standard configuration for the RFC 1483 Link Protocol with the Bridging Network Protocol.

RFC 1483 with Bridging		
STEP/BUTTON	SETTINGS	CONFIGURATION REFERENCE
Connect		<i>Connect and Login, p. 53</i>
System Settings		
System Message	Optional	<i>System Settings, p. 55</i>
DHCP Settings	Already enabled; additional settings may be required	<i>System Settings, p. 55</i> <i>DHCP, p. 73.</i>
Change Login	Optional	<i>System Settings, p. 55</i>
Remote Routers		
New Entry	Enter: Remote Name	<i>Remote Router Database, p. 59</i>
Link Protocol/PVC	Select: RFC1483 Enter: VPI/VCI Numbers	<i>Remote Router Database, p. 59</i>
Bridging On/Off	Select: ON	<i>Remote Router Database, p. 59</i>
IP and IPX Routing		
IP Routing	Select: OFF	<i>IP and IPX Routing Controls, p. 68</i>
IPX Routing	Select: OFF	<i>IP and IPX Routing Controls, p. 68</i>
Store Reboot		<i>Store the Configuration, p. 69</i>
Exit		

Configuring RFC 1483MER with IP Routing

This table outlines a standard configuration for the RFC 1483MER (MAC Encapsulated Routing) Link Protocol with the IP Routing Network Protocol.

RFC 1483MER with IP Routing		
STEP/BUTTON	SETTINGS	CONFIGURATION REFERENCE
Connect		<i>Connect and Login, p. 53</i>
System Settings		
System Message	Optional	<i>System Settings, p. 55</i>
Ethernet IP Address	As required	<i>System Settings, p. 55</i>
DHCP Settings	Already enabled; additional settings may be required	<i>System Settings, p. 55, DHCP, p. 73</i>
Change Login	Optional	<i>System Settings, p. 55</i>
Remote Routers		
New Entry	Enter: Remote Name	<i>Remote Router Database, p. 59</i>
Link Protocol/PVC	Select: RFC1483MER Enter: VPI/VCI Numbers	<i>Remote Router Database, p. 59</i>
Bridging On/Off	Select: OFF	<i>Remote Router Database, p. 59</i>
TCP/IP Route Addresses Add	Enter: explicit or default route with remote gateway	<i>Remote Router Database, p. 59</i>
If NAT is enabled: TCP/IP Route Addresses Advanced	Enter: Source WAN Port Address and Mask	<i>Remote Router Database, p., 59</i>
If NAT is OFF: TCP/IP Route Addresses, Advanced	Enter: Source WAN Port Address and Mask	<i>Remote Router Database, p. 59</i>
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Select: ON (Optional)	<i>IP and IPX Routing Controls, p. 68</i>
IPX Routing	Select: OFF	<i>IP and IPX Routing Controls, p. 68</i>
Store Reboot		<i>Store the Configuration, p. 69</i>
Exit		

Mixed Network Protocols Configuration

Several Network Protocols can be configured concurrently in the same router. The possible combinations are:

- Bridging + IP Routing
- Bridging + IPX Routing
- Bridging + IP Routing + IPX Routing
- IP Routing + IPX Routing

General Configuration Rules:

IP (and IPX) Routing takes precedence over Bridging.

Each Network Protocol in the combination is individually configured as described in the preceding tables.

When configuring multiple network protocols, **make sure that they are all enabled** (even though the preceding individual configuration tables show them to be mutually exclusive).

Example:

To configure Bridging + IP Routing (both with RFC 1483), refer to the preceding *RFC 1483 with Bridging* and *RFC 1483 with IP Routing* tables. Follow the instructions described in the tables, except for the Bridging and IP Routing settings: since you are configuring both Bridging and IP, make sure that these two protocols are both enabled (even though the individual configuration tables you are referring to are showing them to be mutually exclusive. Configure Bridging and then IP Routing. Remember that IP Routing has precedence over Bridging

Sample Configurations

Sample Configuration 1 — PPP with IP and IPX

This configuration example comprises:

- A scenario describing the configuration
- A diagram showing the configuration of the SOHO router
- Tables containing the configuration settings for this example
- Information about the Names and Passwords that are used in this configuration example (required for PPP)

Note: Blank Network Information Worksheets are available to fill in the information for your own configuration in Appendix B.

◇ Scenario

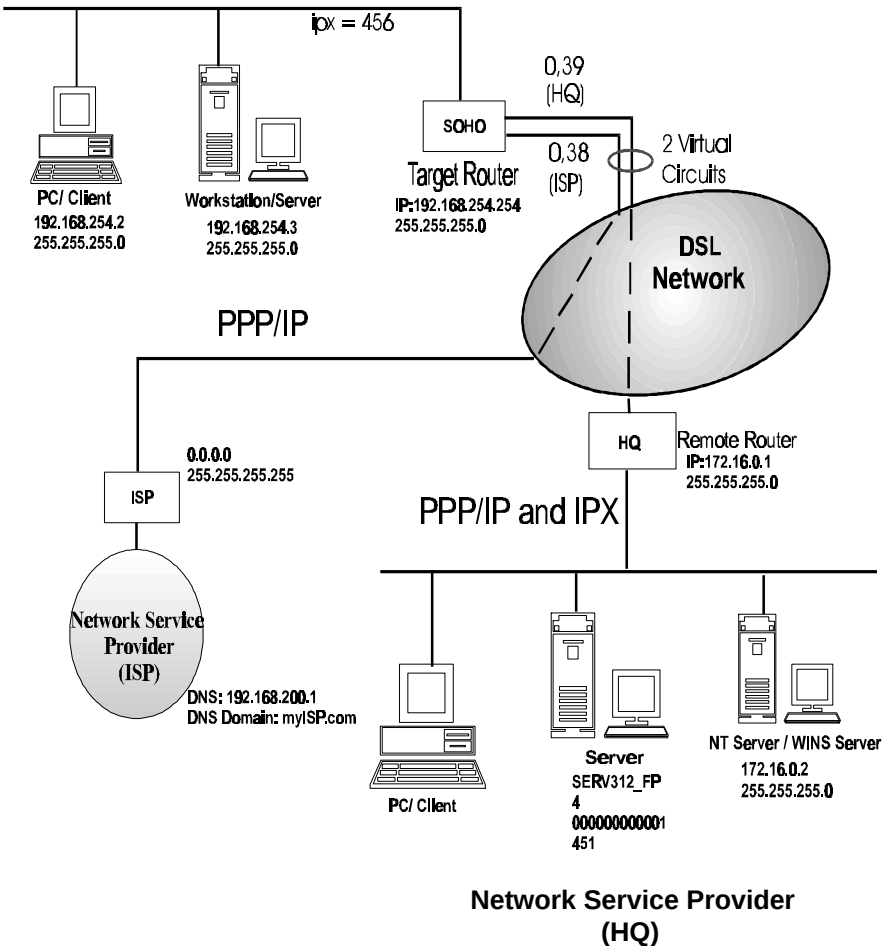
In this configuration example of a hypothetical network, a small office/home office (**SOHO**) will access:

- The Internet through an Internet Service Provider (**ISP**); it uses PPP as the Link Protocol with IP Routing as the Network Protocol.
Network Address Translation (NAT) is enabled to the ISP, since the ISP assigned the SOHO only one IP address.
- A central site (HQ); it uses PPP as the Link Protocol with IP and IPX as its Network Protocols.

IP addresses are issued by the DHCP server. DHCP will be set up to issue DNS information to the SOHO LAN.

◇ **Sample Configuration 1 — Diagram for Target Router (SOHO)**

Small Office Home Office SOHO (Target/Local Router)



◇ Sample Configuration 1 — Tables For Target Router (SOHO)

SOHO SYSTEM SETTINGS		
Configuration Section	Item	Settings
System Settings <u>Name</u>	System Name	SOHO
System Settings <u>Message</u>	Message (optional)	Configured_Oct_1997
System Settings <u>Authentication Password</u>	Authentication Password	SOHOpasswd
System Settings <u>Ethernet IP Address</u>	Ethernet IP Address and Subnet Mask	192.168.254.254 255.255.255.0
<u>Ethernet IPX Network #</u>	IPX Network number	456
System Settings <u>DHCP Settings</u>	DNS Domain Name	myISP.com
	DNS Server	192.168.200.1
	WINS Server Address	172.16.0.2

SOHO REMOTE ROUTER DATABASE		
ENTRY: HQ		
Configuration Section	Item	Settings
Remote Routers <u>New Entry</u> <u>Link Protocol</u> <u>PVC</u>	New remote router name	HQ
	Link Protocol	PPP
	VPI Number	0
	VCI Number	39
Remote Routers <u>Security</u>	Minimum Authentication	PAP
	Disable Authentication	NO
	Remote Router's Password	HQpasswd
Remote Routers <u>Bridging</u>	Bridging On/Off	OFF
Remote Routers <u>TCP/IP Route Addresses</u>	Remote Network's IP Addresses, Subnet Masks, and Metric	172.16.0.0 255.255.255.0 1
Remote Routers <u>IPX Routes</u>	IPX Address: Network #, Hop Count, Ticks	1001 1 4
Remote Routers IPX SAPs	SAPS: Server Name, Server Type, Network #, Node #, Sockets	SERV312_FP 4 1001 00-00-00-00-00-01 451
	WAN Network #	789

SOHO REMOTE ROUTER DATABASE		
ENTRY: ISP		
Configuration Section	Item	Settings
Remote Routers <u>New Entry</u> <u>Link Protocol</u> <u>PVC</u>	New remote router name Link Protocol VPI Number VCI Number	ISP PPP 0 38
Remote Routers <u>Security</u>	Minimum Authentication Disable Authentication Remote Router's Password	PAP NO ISPpasswd
Remote Routers <u>Bridging</u>	Bridging On/Off	OFF
Remote Routers <u>TCP/IP Route</u> <u>Addresses</u>	Remote Network's IP Addresses, Subnet Masks, and Metric Network Address Translation (NAT) In <u>Advanced</u> : Source WAN IP Address and Subnet Mask	0.0.0.0 255.255.255.255 1 (Default Route) Enabled <u>See Note below</u>

Note: This information is required if the WAN address is statically configured. It is not required if the WAN address is statically assigned by the ISP. It is recommended that you check with your Network Administrator regarding this issue.

SOHO ROUTING CONTROLS		
Configuration Section	Item	Settings
IP and IPX Routing	TCP/IP Routing On/Off	ON
	IPX Routing On/Off	ON
	Internet Firewall On/Off	ON

◇ Information about Names and Passwords

In this configuration example, the PPP Link Protocol requires using systems names and passwords.

System Passwords

SOHO has a system password 'SOHOpasswd'. This password is used when SOHO communicates with HQ for authentication by that site and at any time when HQ challenges SOHO.

HQ has a system password 'HQpasswd' which is, likewise, used when HQ communicates with site SOHO for authentication by SOHO and at any time SOHO challenges HQ.

ISP has a system password 'ISPpasswd' used for the same purpose.

Remote Passwords

Each router has a remote router's password for each remote router defined in its Remote Router Database. The router will use the remote password to authenticate the remote router when the remote router communicates with or is challenged by the local site.

For example, SOHO has remote router entries for HQ and ISP, and defined in each table entry are the respective remote router's password.

The following table shows the names and passwords for each router that must be defined for authentication to be performed correctly. (This assumes that all three systems use some form of authentication protocol.)

Note: To avoid problems with passwords, it is recommended that you set the remote router security to “**disable authentication**” to simplify the process.

	Names & passwords configured in SOHO Router	Names & passwords configured in HQ Router	Names & passwords configured in ISP Router
System Name	SOHO	HQ	ISP
System Password	SOHOpasswd	HQpasswd	ISPpasswd
Remote Router Database	HQpasswd ISPpasswd	SOHOpasswd	SOHOpasswd

Sample Configuration 2 — RFC 1483 with IP and Bridging

This configuration example comprises:

- A scenario describing this configuration of the router SOHO
- A diagram showing the configuration information needed for this example
- Tables containing the configuration settings for this example

Note 1: Names and Passwords are not used with the RFC 1483 Link Protocol.

Note 2: Blank Network Information Worksheets are available to fill in the information for your own configuration in Appendix B.

◇ Scenario

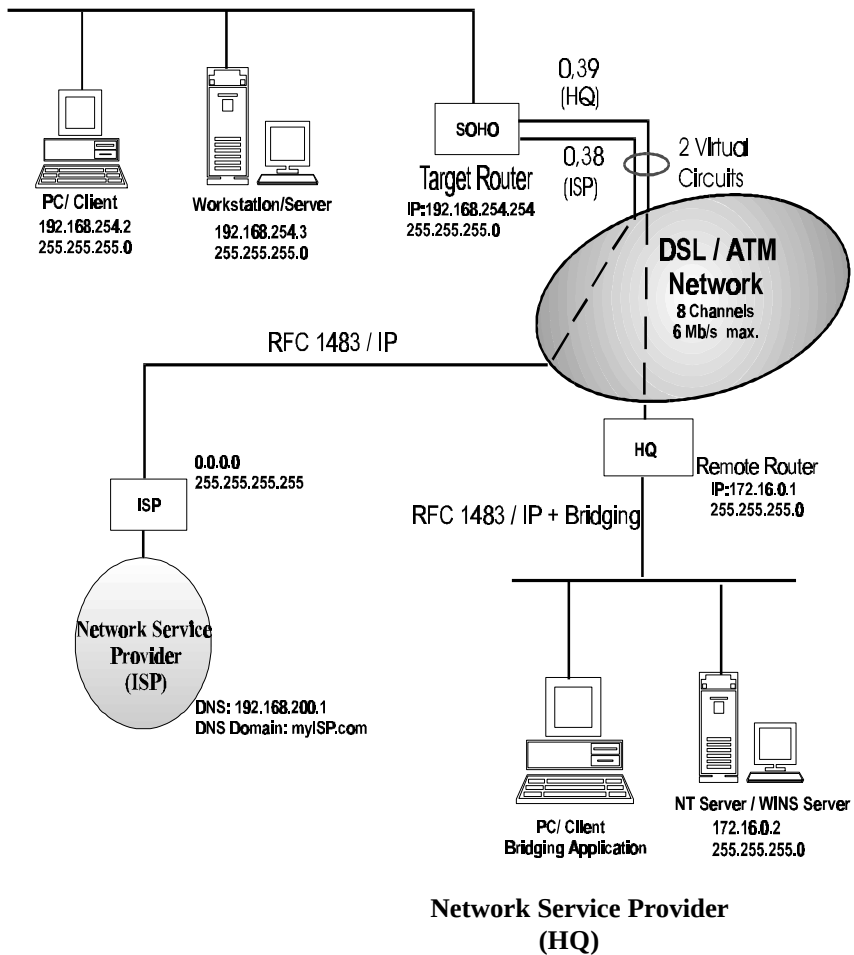
In this configuration example of a hypothetical network, a small office/home office (**SOHO**) will access:

- The Internet through an Internet Service Provider (**ISP**); it uses RFC 1483 as the Link Protocol with IP Routing as the Network Protocol.
Network Address Translation (NAT) is enabled to the ISP, since the ISP assigned SOHO only one IP address.
- A central site (HQ); it uses RFC 1483 as the Link Protocol with Bridging and IP Routing as its Network Protocols.

IP addresses are issued by the DHCP server. DHCP will be set up to issue DNS information to the SOHO LAN.

◇ Sample Configuration 2 — Diagram for Target Router SOHO

Small Office Home Office SOHO (Target Router)



◇ Sample Configuration 2 — Tables For Target Router (SOHO)

SOHO SYSTEM SETTINGS		
Configuration Section	Item	Settings
System Settings <u>Message</u>	Message (optional)	Configured_apr98
System Settings <u>Ethernet IP Address</u>	Ethernet IP Address and Subnet Mask	192.168.254.254 255.255.255.0
System Settings <u>DHCP Settings</u>	DNS Domain Name	myISP.com
	DNS Server	192.168.200.1
	WINS Server address	172.16.0.2

SOHO REMOTE ROUTER DATABASE		
ENTRY: HQ		
Configuration Section	Item	Settings
Remote Routers <u>New Entry</u>	New remote router name	HQ
<u>Link Protocol</u> <u>PVC</u>	Link Protocol	RFC 1483
	VPI Number	0
	VCI Number	39
Remote Routers <u>Bridging</u>	Bridging On/Off	ON
Remote Routers <u>TCP/IP Route</u> <u>Addresses</u>	Remote Network's IP Addresses, Subnet Masks, and Metric	172.16.0.0 255.255.255.0 1

SOHO REMOTE ROUTER DATABASE		
ENTRY: ISP		
Configuration Section	Item	Settings
Remote Routers <u>New Entry</u> <u>Link Protocol</u> <u>PVC</u>	New remote router name	ISP
	Link Protocol	RFC 1483
	VPI Number	0
	VCI Number	38
Remote Routers <u>Bridging</u>	Bridging On/Off	OFF
Remote Routers <u>TCP/IP Route</u> <u>Addresses</u>	Remote Network's IP Addresses, Subnet Masks, and Metric	0.0.0.0 255.255.255.255 1 (Default Route)
	Network Address Translation (NAT)	Enabled
	In <u>Advanced</u> : Source WAN IP Address and Subnet Mask	Required (see your Network Administrator)

SOHO ROUTING CONTROLS		
Configuration Section	Item	Settings
IP and IPX Routing	TCP/IP Routing On/Off	ON
	IPX Routing On/Off	OFF
	Internet Firewall On/Off	ON

Chapter 3. Configuration Reference

Configuration Reference

This section lists and describes each configuration button in Configuration Manager. It provides additional information for each configuration point listed previously in the Configuration Tables.

Note: This information is for use as reference material only. It does not include step-by-step instructions.

Connect and Login

◇ Connect

The router is shipped to the users with a default IP address that does **not** need to be changed *. This default address is: 192.168.254.254.

- ⇒ Click the **Connect** button to connect your PC to the target router. This will open the **Select the Router** window where the default IP address (192.168.254.254) is already entered.
- ⇒ Click **OK**.

If Configuration Manager cannot successfully connect to the target router, you will get a message asking you if you wish to retry to connect. If you cannot connect to the router:

1. Verify the router's LAN IP address and subnet mask by using the Terminal Window (under **Tools**) and typing **eth list**.

Note: Refer to Appendix C for instructions on how to access the Terminal Window.

2. Check the PC and router's physical connections to the LAN.

*You may decide to change your router's IP address during the configuration process. Refer to *System Settings, Ethernet LAN IP Address and Protocols*, page 56, for more information on this topic.

◇ Password, Login, Skip

Login

⇒ Enter the Login Password **admin** in the **Login** Window.

The default login password is **admin** when first configuring the router. Type it in lowercase and verify that your keyboard Caps Lock key is not active.

⇒ You will then be prompted to enter your own password twice in the **Login Password** window as a security measure.

This security feature allows you to prevent unauthorized write access to the router's configuration.

After successfully connecting to the router, the main menu screen will display the router's software level, IP address, and hardware model number.

Skip

⇒ Click **Skip**, if you only want to view the router's configuration settings.

If you attempt to change any of the router's configuration settings while in **View-Only mode**, you will again be prompted for the write enable **Login Password**.

◇ Name, Message, Software, and Hardware

Name is the name for the target (local) router.

Message is an informational message that you can enter and save for this display.

The **Name** and **Message** fields are blank for the initial configuration. If you click either of these fields after the label, a menu is displayed allowing you to alter this information. You do not need to do this at this time; this is the same menu displayed when you click the button **System Settings** later in the configuration process.

Software is the router software level.

Hardware is the Model Number, Serial Number, and Revision Level of the router.

⇒ Click **About** and a window displays the Configuration Manager Version number and date.

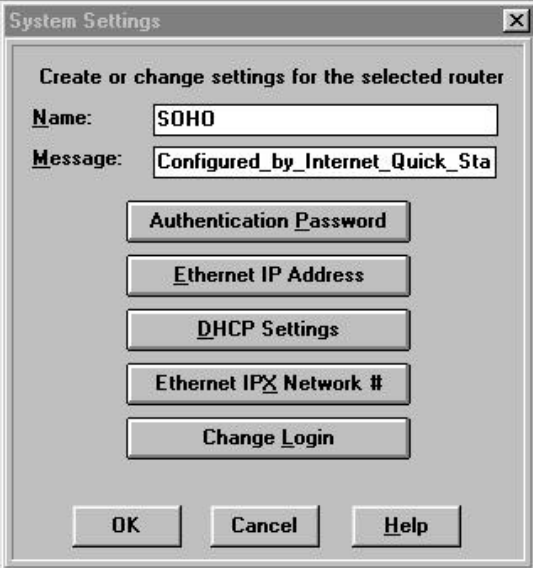
System Settings

The information about the target router you are configuring and adding to your network includes:

- The system name (for PPP only)
- An optional system message
- An authentication password (for PPP only)
- An Ethernet IP address
- DHCP settings (if required)
- An Ethernet IPX address (if IPX Routing)
- Change the Login Password (optional)

⇒ Click **System Settings** from the main menu.

Note: The **Name** and **Message** fields are blank when you first configure the router.



The screenshot shows a dialog box titled "System Settings" with a close button (X) in the top right corner. The main text inside the dialog is "Create or change settings for the selected router". Below this text are two input fields: "Name:" with the value "SOHO" and "Message:" with the value "Configured_by_Internet_Quick_Sta". Below these fields are six buttons stacked vertically: "Authentication Password", "Ethernet IP Address", "DHCP Settings", "Ethernet IPX Network #", "Change Login", and "OK", "Cancel", "Help" at the bottom.

◇ System Name

⇒ Enter a router name in the field labeled **Name** (PPP only).

You **must** enter a system name for the target router if your Link Protocol is PPP. This name is sent to other routers during authentication. Space characters within the name are converted to underscores as the system name is a ‘word’ when exchanged with PAP/CHAP.

◇ System Message

⇒ You may enter an optional **Message**.

This message is saved in the router and is displayed on Configuration Manager’s main menu screen. This field is useful for specifying, for example, the name of the person configuring this router and the last changes made.

◇ Authentication Password (PPP only)

The target router’s authentication password is used for authentication when the target router communicates with the other routers or is challenged by them. It is needed only if the remote router you are connecting to supports PPP. The password is not displayed as you enter it and must be entered twice. A new password overrides the previous one.

⇒ To set the password, click **Authentication Password** and enter the new password in the text box.

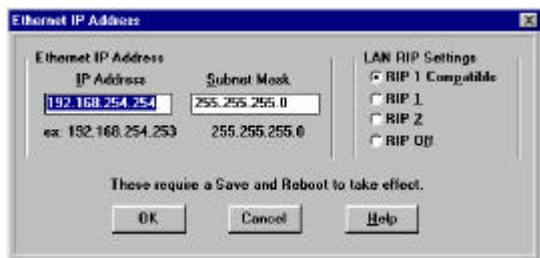
⇒ Click **OK** to set the password.

◇ Ethernet LAN IP Address and Protocol Controls

You have the option to enter or change your router’s Ethernet IP address and IP protocol control information.

Ethernet IP Address

For IP routing, click **Ethernet IP Address** if you wish to change the Ethernet IP Address and Subnet Mask from the default. This window displays the default IP Address and Subnet Mask (factory default).



To Change the IP Address and Mask

⇒ Use this window if you wish to change the IP Address and Subnet Mask of the target router. This may occur, for example, if a company already has a LAN network and users are given specific addresses to use by their network administrator.

⇒ Click **OK** to save the changes and exit the window.

Note: When changing either of these fields, you must always perform a **Store** and **Reboot** as shown in later steps.

LAN RIP Settings

The router supports RIP-1 Compatible, RIP-1, and RIP-2.

RIP-1 Compatible is enabled by default. RIP options should be handled by experienced users or network administrators.

For further information on this topic, refer to Chapter 5, *Configuring Advanced Features, Routing Information Protocol*, page 78.

◇ Ethernet IPX Network Numbers

⇒ For IPX routing, click **Ethernet IPX Network #**.

⇒ Enter your IPX Network Number. Select the appropriate frame type.

The frame types supported are:

802.2 Default recommended by Novell

802.3 Other most common type

DIX For DEC, Intel, Xerox; this setting is also referred to as “Ethernet II”, and is rapidly becoming obsolete.

⇒ Click **OK** to save the changes and exit the window.

The IPX Network Number (also known as the External Network Number) is an 8-character hexadecimal string representing the Ethernet LAN. You can now use this window to change the settings.

The frame types must be compatible with the Novell server located on the same LAN. To determine this, consult with your network administrator.

◇ DHCP

The FlowPoint router supports **DHCP (Dynamic Host Configuration Protocol)** and acts as a DHCP server. This allows hosts (PCs, etc.) to acquire initialization parameters (IP addresses, masks, domain names, etc.) from the router. DHCP is enabled by default.

For more information on DHCP configuration, refer to Chapter 5, *Configuring Advanced Features*.

◇ Change Login Password

⇒ If you wish to change your Login Password, click **Change Login** on the main menu.

⇒ In the **Login Password** window, enter a new password in the fields provided.

The password is not displayed as you enter it and must be entered twice. A new password overrides the previous one set.

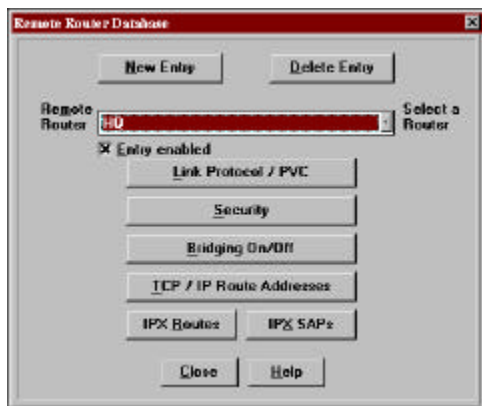
⇒ Click **OK** to set the password.

Remote Router Database

The information about all the remote routers to which this (local/target) router may connect on the Wide Area Network (WAN) is entered into the router's Remote Router Database. The remote router information includes:

- Link Protocol/PVC
- Security
- Bridging specifications
- TCP/IP route addressing ,RIP protocol controls, address translation
- Remote IPX route services (IPX Routes - IPX SAPs)

⇒ Click **Remote Routers** from the main menu. This will open the **Remote Router Database** window.



◇ Add, Delete, Modify, Enable/Disable an Entry

Add a New Remote Router

Initially, the **Remote Router** field is blank. After adding a router, the screen displays the information as shown above.

- ⇒ To add a new remote router to the remote router database, click **New Entry**. A new window opens (not shown).
- ⇒ Enter the new router name in the field provided and then click **OK**. The router name will then be placed in the list of routers, at the top of the list on the previous screen.

Delete a Remote Router Database Entry

- ⇒ Click the down arrow next to the field labeled **Select a Router** to display the list of remote routers entered into the database.
- ⇒ Click the name of the router entry you wish to delete.
- ⇒ Then click **Delete Entry** and in the next window displayed, confirm by clicking **Yes**.
- ⇒ Click **Close** to exit the **Remote Router Database** screen.

Modify a Remote Router Database Entry

- ⇒ Click the down arrow next to the field labeled **Select a Router** to display the list of remote routers entered into the database.
- ⇒ Click the router name of the router entry you wish to modify.
- ⇒ Then select the items to modify (like **Link Protocol**, **Security**, etc.). Click **Close** to exit the **Remote Router Database** screen.

Enable or Disable Remote Router Entry

Router entries and changes are enabled by default. Make sure that the **Entry Enabled** box is checked. Disabling and then re-enabling an entry requires a reboot unless you have not rebooted between the changes.

- ⇒ When you are done, click **Close** in the **Remote Router Database** window to return to the main window.

◇ Link Protocol/PVC

Link Protocol

Your Network Service Provider will tell you which Link Protocol to use. Do not attempt to choose the Link Protocol yourself.

- ⇒ Select the appropriate Link Protocol as directed by your Network Service Provider. The protocols are:

PPP

RFC 1483

RFC 1483MER (MAC Encapsulated Routing)

Important link protocol configuration notes:

- **PPP:**

If PPP is selected, you will need to enter a **User Name** and **Password** for your Internet connection.

- **RFC 1483:**

If you are using RFC 1483, do **not** enter a **User Name** and **Password** for your Internet connection.

If Network Address Translation (NAT) and IP are enabled, you must enter **Source WAN IP Address** information for this type of connection. You will obtain this information from your ISP or your Network Administrator.

If NAT is OFF, you may still need to enter **Source WAN IP Address** information. You will obtain this information from your ISP or your Network Administrator.

- **RFC 1483MER (MAC Encapsulated Routing):**

You must specify a **Source WAN IP Address** and **Remote Gateway**. You will obtain this information from your ISP or your Network Administrator.

PVC

- ⇒ The VPI/VCI numbers are preconfigured. Make sure that these numbers are right for your setup. If in doubt, check with your Network Service Provider.
- ⇒ If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider. These numbers identify the remote destination and must, therefore, be unique for each remote.

◇ Security Information (PPP only)

The **Security** window allows you to specify the type of authentication and password required by the target router when communicating with the remote router.

⇒ From the remote router menu screen, select **Security**.

Security Authentication Protocol

The authentication protocol is the minimum security level that the target router must use when communicating with the remote router. This protocol level is checked during security negotiation. The FlowPoint router will *always* attempt to negotiate CHAP, the highest level of security possible. The router will not accept a negotiated security level less than the minimum authentication level selected.

⇒ Click **CHAP**, **PAP**, or **None**. PAP is the default.

Note: The authentication process occurs regardless of which side (local or remote) initiates the communication; this holds true even if the remote end does not request authentication. Authentication is a bi-directional process, where each end can authenticate the other using the protocol of its choice (provided the other end supports it). The parameter in the remote router database is the minimum security level used by the target router when challenging or authenticating the remote router.

Disable Authentication

⇒ Check the **Disable Authentication** box if you wish to prevent your router from authenticating the remote router when communicating.

The router will not request any authentication information from the remote router, but will still reply to any PAP or CHAP authentication request performed by the remote, such as your ISP.

Security Authentication Password

This password is the remote router's password used by the target router to authenticate the remote router.

⇒ To enter or change the remote router's password, click **Remote's Password**.

⇒ In the next window, enter a new password in both fields.

The password is not displayed as you enter it and must be entered twice. A new password overrides the previous one set. Blank passwords are not acceptable.

⇒ Click **OK** to set the password. Click **OK** again to save the security specification.

◇ Bridging Capability

⇒ From the **Remote Router Database** menu screen, select **Bridging On/Off**.

You specify whether the target router bridges traffic to/from this remote router.

⇒ Click **On** or **Off** (default) to turn bridging On or Off.

Spanning Tree Protocol (STP)

The Spanning Tree Protocol is **On** by default. STP is used to allow the router to check for bridging loops and communicate with other sites that support the default.

If you choose to turn STP **Off**, you need to disable it with the Command Line Interface. Turning it **Off** assumes that no pair of nodes on the larger network, made by joining all the local LANs that can communicate with each other, can be connected by more than one path.

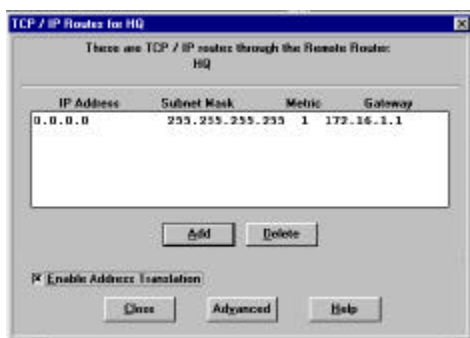
◇ TCP/IP Route Addressing and IP Protocol Controls

TCP/IP Route Addresses

If you are configuring TCP/IP Routing, you now need to enter details about routing to stations/networks on the LAN connected beyond the remote router. Consult with your Network Administrator to find out if you need to seed the routing table and which information is required.

⇒ From the **Remote Router Database** menu screen, select **TCP/IP Route Addresses**.

- ⇒ To seed the routing table, you will enter the **TCP/IP Route Addresses** into the table using this window.



This window displays a list of each network IP address with the corresponding subnet mask, metric, and gateway. The metric is a number between 1 and 15 that indicates the perceived cost in reaching the remote network or station.

Note: The gateway must be specified when the RFC 1483MER link protocol is selected.

- ⇒ To add a new entry, click **Add**, enter the IP address, subnet mask, and metric in the text box displayed and click **OK**.

Note 1: The default route is specified as: **0.0.0.0 255.255.255.255 1** (or you may click the **Default Route** button).

Note 2: There can be only one default route specified. Defining a default route on the WAN is comparable to defining a gateway on the LAN. If you have more than one router, be sure to choose only one router as the default router and change the configuration of the other routers accordingly.

Enable Address Translation (Network Address Translation)

- ⇒ You will need to check this box if you are connecting to an Internet Service Provider that has assigned you a single IP address.

Refer to *Network Address Translation*, page 77, for more details.

Advanced - Source and Remote WAN IP Addresses

⇒ Click the **Advanced** button if you wish to specify WAN Port addresses or set IP protocol options.

Source WAN Port Address

PPP:

The **Source WAN IP Port Address** can be assigned dynamically or statically. Verify this information with your Network Service Provider.

RFC 1483:

If Network Address Translation (NAT) and IP are enabled, you must enter **Source WAN Port Address** and mask information for this type of connection. You will obtain this information from your ISP or your Network Administrator.

If NAT is OFF, you may still need to enter **Source WAN Port Address** information. You will obtain this information from your ISP or your Network Administrator.

RFC 1483MER (MAC Encapsulated Routing):

You must specify **Source WAN Port Address** information. You will obtain this information from your ISP or your Network Administrator.

Remote WAN Port Address

Check with Network Administrator if you need to specify a **Remote WAN Port Address** for the WAN connection to the remote router.

WAN RIP Settings

For more information on IP protocol controls, refer to Chapter 5, *Configuring Advanced Features*.

◇ IPX Route Addressing/Services

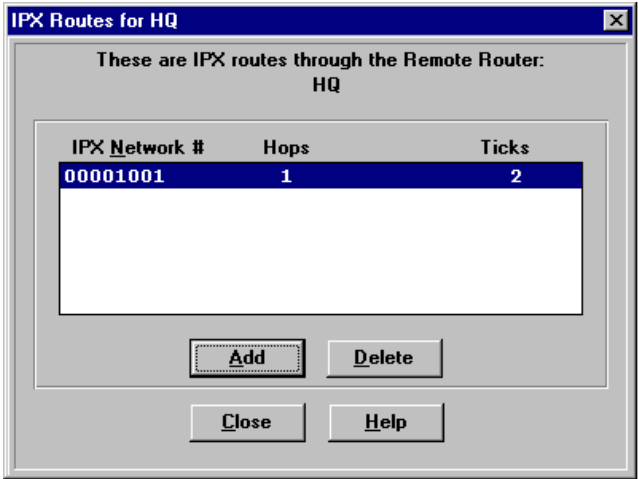
⇒ From the remote router menu screen, select **IPX Routes**.

If you are configuring IPX Routing, enter details about routing to network segments connected beyond the remote router.

Ask your network administrator to determine if you need to seed the routing table and what information is required.

IPX Routes

To seed the routing table, you will enter **IPX Route Addresses** using this window.



This window displays a list of each **IPX Network #** with the corresponding **Hops** count and number of **Ticks**.

The IPX routes entered here may be to an internal or external network number depending upon how the router is being used.

The **Hops** count is a number greater than 1 representing the number of routers that must be passed through to reach the network number.

The number of **Ticks** indicates how much time that the packet takes to reach the network number in units of roughly 1/18th of a second. This number must be at least 1.

- ⇒ To add a new entry, click **Add**, enter the IPX Network Number, Hops count, and Ticks in the text box displayed, and click **OK**. (The **Tab** key can be used to tab between each item on the entry window.)
- ⇒ To delete any entry, click the line containing the entry, click **Delete**, and click **OK** on the verification window.

IPX SAPs

If you are configuring IPX Routing, you will also need to enter details about services that are available on the LAN networks connected beyond the remote router.

Ask your network administrator to determine if you need to seed the services table and what information is required. To seed the services table, you will enter **IPX SAPs** using the window.

This window displays a list of each **Server Name** with the corresponding **Server Type**, **Network #**, **Node #**, and **Socket**. The **WAN Network Number** is displayed.

IPX SAPs and WAN Network # for HQ

When connected to the Remote Router: HQ

SAPs

Server Name
SERV312_FP

Add

Delete

Server Type	Network #	Node #	Socket
4 File Server	00001001	00-00-00-00-00-01	451

WAN

WAN Network #: 00000789

Modify

Close

Help

- ⇒ To add a new server entry, click **Add**.
- ⇒ Select a server by entering the **Server Type**, click one of the servers already defined, or define your own.
- ⇒ Seed the table with the **SAP** information of the primary logon server on the remote network:
 - Service Name
 - Network # (The Network # is the 8-character hexadecimal internal network number associated with the server)

- Node # (The Node # is the 12-character hexadecimal internal node number associated with the server entered in the format xx-xx-xx-xx-xx-xx)
- Socket # (The Socket # is the 4-character hexadecimal number representing the service —application— within the server node)

Note 1: All other SAPs are automatically learned. This entry is used for spoofing.

Note 2: SAP information is available from your Network Administrator.

- ⇒ You can modify the **WAN Network Number** by clicking **Modify**. Enter the 8-character hexadecimal network number for the WAN link and click **OK**.

IP and IPX Routing Controls

- ⇒ To enable IP or IPX routing controls and an Internet Firewall, click **IP and IPX Routing** from the main menu.

◇ TCP/IP Routing

- ⇒ Set TCP/IP Routing to **On** or **Off**.

The default is TCP/IP Routing **Off**. If TCP/IP Routing is **Off**, then the Internet Firewall is forced inactive.

◇ Internet Firewall

- ⇒ Set the Internet Firewall to **On** or **Off**.

When the Internet Firewall is **On**, the router performs IP Internet Firewall filtering to prevent unauthorized access to your system and network resources from the Internet. This filter discards packets received from the WAN which have a source IP address recognized as a local LAN address.

◇ IPX Routing

- ⇒ Set IPX Routing to **On** or **Off**. The default is IPX Routing **Off**.

◇ WAN-to-WAN Forwarding

This option is **On** by default to allow users to manage forwarding of data from one WAN link to another.

In some cases, it may be desirable to disable WAN-to-WAN Forwarding to stop the data from being forwarded from one WAN link to another WAN link.

Example: if the router is used at home to access both a company network and the Internet at the same time, and company information should not pass to the Internet, then disable WAN-to-WAN forwarding.

Store the Configuration

◇ Store

To save the configuration to FLASH in the router:

⇒ Click **Store** on the main menu. Click **OK** again to confirm the store operation.

Any settings that you have modified will be permanently stored in the router's configuration. Any settings you have not modified will be unchanged (or will default if this is your first configuration). If you do not save the configuration to FLASH, the configuration is lost upon reboot or power down of the router.

◇ Reboot

After storing the configuration, you will be asked if you wish to reboot the router.

⇒ Click **Yes** to confirm. A message window will inform you that router rebooting is occurring.

⇒ Click **Exit** to leave Configuration Manager.

If you are using IPX routing, bridging, or DHCP, you may need to also reboot PC clients so they can locate the new network segment or settings.

Verify the Router Configuration

◇ Test IP Routing

Test IP Routing over the Local Ethernet LAN

1. Check that the PWR, TEST, and LINK LEDs on the front panel of your router are lit green. Then proceed to step 2.

All lights should be lit green: If not, the link is not working. At this stage, it is recommended that you turn your router off and then turn it back on.. If the lights still don't display properly, contact your Network Service Provider.

2. Use the TCP/IP **ping** command or similar method to contact the configured target router specifying the Ethernet LAN IP address. For example, to ping your router (assuming its default IP address has not been changed), you would enter from your DOS prompt:

```
ping 192.168.254.254
```

If the router and PC are properly configured and connected, you will get a reply from the router.

Note: For more information on how to use the **ping** command, refer to page 100.

If you cannot contact the router:

- Verify that the IP address and subnet mask are correct.
- Check cable connections and pin connections.

Test IP Routing To a Remote Destination

Using the TCP/IP **ping** command, contact a remote router from a local LAN-connected PC.

If you cannot ping the remote router:

- Check that, if required, you specified a valid remote WAN IP address and local WAN IP addresses.
- Check the TCP/IP remote routes.
- Verify the security authentication method and password of the remote router. Also, the router's entry must be enabled.

Test Routing From a Remote Destination

Have a remote router contact the target router using a similar method.

Test TCP/IP Routes

Contact a station, subnetwork, or host on the network beyond a remote router to verify the TCP/IP route addresses entered in the remote router database.

◇ Test IPX Routing

Test IPX Routing to a Remote Destination

Check for access to servers on the remote LAN as follows:

- Use the 'NetWare Connections' selection provided with NetWare User Tools under Windows or issue the command 'pconsole' under DOS.

If you cannot access the remote server:

- Check that the local Ethernet LAN IPX Network Number is correct.
- Verify that the WAN link Network Number is the same as the remote WAN link Network Number.
- Check cable connections and pinouts.
- Verify that the IPX Routes and IPX SAPs you have specified are correct.
- Verify the security authentication method and password of the remote router.

Disconnect from the Router

- ⇒ You can release the connection between your PC and the target router at any time by clicking **Disconnect** on the main menu.
- ⇒ Click **Exit** to leave Configuration Manager.
- ⇒ If you change any of the router's configuration settings, be sure to store the configuration into FLASH memory and reboot the router.
- ⇒ Once you have rebooted the router, you will be prompted to log in again if you wish to further change the configuration.

Chapter 4. Advanced Features And Management Tools

Advanced Features

The features described in this section are advanced topics. They are primarily intended for experienced users and network administrators to perform network management and more complex configurations.

These following features are accessed and configured from Configuration Manager:

- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)
- Routing Information Protocol (RIP)

Dynamic Host Configuration Protocol (DHCP)

The FlowPoint router supports **DHCP** and acts as a DHCP server itself, allowing hosts (PCs, etc.) to acquire initialization parameters (IP addresses, masks, domain names, etc.) automatically. These initialization parameters are collectively called the **lease** and are valid for a certain amount of time (usually one week). When a lease expires, a new one is acquired. For this to happen, your PC has to be configured to use DHCP.

◇ PC Configuration

DHCP has to be enabled on your PC. The following instructions assume a Windows 95 environment.

1. Follow the instructions in the *Quick Start Guide, Hardware Installation*, for connecting your network cables.
2. Power the router **On**.
3. Click the **Start** button on your PC desktop. Select **Settings**. Click **Control Panel**. Select **Network**.

4. If the TCP/IP stack is installed on your PC (it will be listed under **Configuration**), proceed to step 5. If not, see note 1.
5. Under **Configuration**, double-click **TCP/IP**. Select **Obtain an IP address automatically**. If you are connecting to a Windows NT server, see note 2.
6. Click the **DNS Configuration** tab and select **Disable DNS**. Click **OK**.
7. You are now back in the **Network** window. Select the **Identification** tab. Enter a **computer name**, a **workgroup name**, and a **computer description** if you wish. Click **OK**.
8. Files are now being copied. A “*Setting Changes*” message will ask you if you wish to restart your computer. Answer **Yes**. After the PC has finished rebooting, it will acquire its own IP address from the router using DHCP.
9. You now need to run the Configuration Manager program to enter the DNS and a domain name into the router. On the next boot, the PC will learn the DNS and Domain Name from the router.

Note 1:

If you do not have a TCP/IP stack installed on your computer, you need to install it as follows:

1. In **Configuration**, click **Add**.
2. In **Select Network Component Type**, click **Protocol** and click **Add**.
3. In **Select Network Protocols**, under **Manufacturers**, click **Microsoft**.
4. In the same **Network Protocols** window, click **TCP/IP** and click **OK**.

Note 2:

If you are connecting to a Windows NT server:

1. Click the **Wins Configuration** tab.
2. Click **Use DHCP for WINS Resolution**.
3. Click **OK**.

◇ Router Configuration

DHCP Settings

DHCP is enabled initially by default (the **IP Address Pool** field is already filled in). Before becoming active, the router's DHCP server attempts to locate other active DHCP servers on the network such as Windows NT servers. If one is detected, the router's DHCP server disables itself.

The DHCP Server Settings screen allows users to:

- Change the IP Address Pool if needed
- Configure DNS information specifically for Internet access
- Configure the WINS Servers settings if working with Windows NT

⇒ To access the **DHCP Server Settings** screen, click **System Settings** and **DHCP Settings**.

This picture shows a DHCP sample configuration

DHCP IP Address Pool	
First IP Address	Last IP Address
192.168.254.2	192.168.254.20
Default Gateway	
192.168.254.254	

DNS Configuration	
Server Address	Second Server
192.168.200.1	192.168.200.3
Domain Name	
myip.com	

WINS Servers	
Primary IP Address	Secondary Address
192.84.210.89	

☒ DHCP Server is enabled

OK Cancel Help

DHCP IP Address Pool

The existing IP Address Pool settings can be changed if you need to modify/increase the range of your address pool.

If you change your router's IP address, the router's DHCP server will automatically provide a new IP address pool for the new subnet if the preceding subnet was enabled.

DNS Configuration

If you intend to primarily configure your router for Internet access, you need to enter DNS information provided by your Internet Service Provider.

WINS Servers

If you work with Windows NT, you should enter your WINS Servers' IP addresses in the **WINS Servers** fields.

◇ Storing and Rebooting

Changing or entering new DHCP settings requires a **Store** in the router and a **Reboot** of the PC. This step is necessary so that the PC can acquire its initialization parameters from the router.

Note: Windows 95 users can easily acquire an IP address without restarting the PC using the **Winipcfg** utility as follows:

1. Click the **Start** button located on your PC desktop screen.
2. Click **Run**. Enter WINIPCFG.
3. Click **Release** to clear your current IP address and **Renew** to acquire new IP parameters. The new settings will be displayed.
4. Click **OK**.

◇ Disabling DHCP on the PC

- ⇒ To disable DHCP, click the **Start** button on your PC desktop, **Settings, Control Panel**, and **Network**.
- ⇒ In **Network**, under the **Configuration** tab, double-click **TCP/IP**.
- ⇒ Select **IP Address** tab. Select **Specify an IP Address**. Enter your PC's IP address and its subnet mask. Click **OK**.
- ⇒ Select the **DNS Configuration** tab.
Select **Enable DNS**. Enter the DNS information (check with your Network Administrator). Click **OK**. Click **OK** again.

Network Address Translation (NAT)

NAT is an IP address conversion feature that translates a PC's local (internal) address into a temporary global (outside/Internet) IP address.

NAT is needed when a PC (or several PCs) on a Local Area Network wants to connect to the outside/Internet to get to a remote network: NAT swaps the local IP address to a global IP address. Our version of NAT goes one step further by allowing several PCs to share one single IP address to the Internet, thus reducing connection costs. In effect, it allows a whole LAN to connect to the Internet as a Single User.

◇ Instructions to Enable NAT:

Important: First, make sure that IP routing is enabled.

- ⇒ From Configuration Manager's main menu, click **Remote Routers** and then **TCP/IP Route Addresses**.
- ⇒ In the **TCP/IP Routes** window, check the **Enable Address Translation** box to enable NAT.

◇ Source WAN IP Address

If you are running IP Routing with RFC 1483 or RFC 1483MER, you must enter a Source WAN Port Address for your router since the remote end will not be able to assign you (the local router) a WAN IP address dynamically. This address corresponds to the global IP address and is obtained from your Network Service Provider.

- ⇒ In the **TCP/IP Routes** window, click **Advanced**.
- ⇒ In the **Source WAN Port Address** window, enter the **IP Address** and its corresponding **Subnet Mask** and click **OK**.

Routing Information Protocol (RIP)

You can configure the router to send and receive RIP (Routing Information Protocol) packet information to and from the remote router. RIP is a protocol used by some routers to exchange IP routing information so that the local site will “learn” all about the routes beyond the remote router and the remote router will “learn” all about the local site’s routes.

Note 1: You may not want this to occur in some cases. For example, if you are connecting to a site outside of your company such as the Internet, you may want to keep knowledge about your local site’s routes private.

Note 2: With NAT (Network Address Translation) enabled, the local router cannot send RIP packets to the remote WAN link, but can, however, receive RIP packets from the remote site.

Default: The default is to restrict sending or receiving IP RIP packets or default routes. If RIP packets are not allowed to flow on the WAN link, you must seed the routing table. You can also advertise the remote site’s existence. The default is to keep the remote site’s existence private.

◇ RIP Options

RIP-1 Compatible

In RIP-1 Compatible mode, the router can broadcast RIP-1 packets and multicast RIP-2 packets. It can also receive and interpret RIP-1 and RIP-2 packets.

RIP-1

It is used when exchanging RIP packets when communicating with older routers that don’t have RIP-2. RIP-1 has the following two shortcomings: Since it uses broadcast for sending packets, every device on the LAN must receive and inspect every packet. RIP-1 has no way of communicating a subnet mask. This deficiency can lead to misinterpretation of IP networks by the router receiving the RIP-1 packets.

RIP-2

RIP-2 lets the routers exchange subnet mask information in the packets.

Since it uses multicast addresses, only devices supporting RIP-2 will listen to RIP-2 packets.

Note: If your network does not support RIP, then use the **RIP Off** option to disable RIP.

◇ Instructions to Enable RIP Options

It is advisable to only activate RIP options when instructed to do so by your network administrator. Make sure that IP routing is enabled by clicking **IP and IPX Routing** from the main menu.

Note: RIP options do not apply to Bridging.

To turn on LAN RIP Settings:

RIP-1 Compatible is enabled by default. To enable another RIP option:

- ⇒ From Configuration Manager's main menu, click **System Settings** and then **Ethernet IP Address**. Your current IP Address and Subnet Mask are displayed.
- ⇒ Select the appropriate RIP options under **LAN RIP Settings**.

To turn on WAN Settings:

RIP is disabled by default. To enable a RIP option:

- ⇒ From Configuration Manager's main menu, click **Remote Routers**. Select your remote router.
- ⇒ Click **TCP/IP Route Addresses**. In the **TCP/IP Route Addresses** window, click **Advanced**.
- ⇒ Select the appropriate RIP options under **WAN RIP Settings**.

Management Tools

This section describes tools designed to simplify file system management, software maintenance, and data traffic monitoring. These tools comprise:

- Terminal Window
- Upgrade/Backup
- Reboot from Network
- SNMP Options

⇒ To access these tools, click **Tools** from Configuration Manager's main menu.

Terminal Window

The **Terminal Window** lets you access the **Command Line Interface (CLI)** through **Configuration Manager ***.

◇ How to Access the Terminal Window

In order to access the Terminal Window, your PC or ASCII terminal must be connected to the **Console** port. Information needed to access to the CLI through Configuration Manager or through other utilities is explained in Appendix C, *Command Line Interface (CLI)*, page 118.

When using the Terminal Window from within Configuration Manager, the menu selection **Commands** provides shortcuts to most of the commands described in the Command Line Interface. These shortcuts will substantially reduce the amount of typing.

* The CLI can also be accessed from a terminal emulation session running under Windows, from an ASCII terminal, or through a TELNET session for remote access.

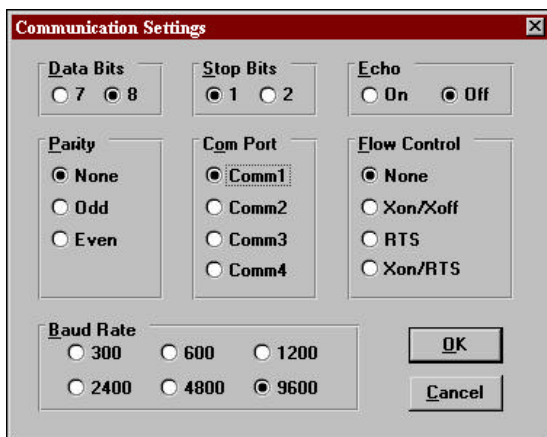
◇ How to Change the Router's IP Address Using the Terminal Window

The console cable allows you to access the Command Line Interface via Configuration Manager. The router's address will be changed to be in the same IP subnetwork as the PC. The PC's address will not change.

Note: Refer to Appendix C, *Command Line Interface*, page 116, for installation instructions.

◇ Instructions

1. Use the serial (console) cable to access the router through Configuration Manager.
2. Click the menu button **Tools** and then select **Terminal Window** to change the router's address.
3. From the Terminal Window menu, select **Commport** and **Settings** to verify that the communication settings are set as shown in the picture below and that the correct Communication Port (Com Port 1) is selected.



4. In the terminal window, enter the following commands to set, save, and verify the router's LAN address and enable IP routing:

login admin (admin is the default password)

eth ip addr x.x.x.x y.y.y.y

where:

x.x.x.x (IP address)

y.y.y.y (subnet mask for the router's LAN connection)

Ex: 192.168.254.254 255.255.255.0

Note: To determine which addresses are valid for your router, refer to Appendix E, *Subnetwork Tables*, page 121, or ask your network administrator.

eth list

This command lists the settings for the Ethernet LAN IP address and subnet mask as well as the port number.

save

reboot

5. Close the terminal window.
6. Click the **Connect** button in Configuration Manager.
7. Enter the same IP address you just assigned to the router.
8. Verify that you have set the router's LAN connection address and subnet mask correctly.

Upgrade/Backup

This menu gives you the options of performing backup or upgrade operations on the following files:

- Firmware files
- Configuration files
- DHCP settings files

Upgrade lets you upgrade or restore files from your PC to the router. With **Backup**, the files are downloaded from the router to your PC.

A **TFTP** utility needed to perform **Backup** and **Upgrade**, is integrated into Configuration Manager, but can also be used as a stand-alone application.

◇ Upgrade/Backup Options

Upgrade Firmware

Upgrading the Firmware should only be done when advised by Technical Support or when you are installing a new version/upgrade of the router's Firmware. You should back up the previous Firmware to a separate directory first.

Upgrade/Backup of the Configuration Files

A Backup or Upgrade operation on the configuration files will include all of the system files, but not the target DHCP settings files.

Upgrade/Backup of DHCP Setting Files

Backing up or upgrading the target system DHCP Settings files will involve only target systems DHCP files. The files will be copied to the directory C:/DSL by default.

Reset Defaults

This feature allows you to clear all of your configuration files (SYSTEM.CNF, DHCP.DAT) and to go back to the original factory default settings.

⇒ Click **Reset Defaults**. A message will ask you if you want to clear your configuration files.

⇒ If you answer **Yes**, the router will reboot.

Note: It is recommended that you back up all of your existing configuration files before resetting the defaults in your router.

◇ Instructions

⇒ Click **Tools** from the main menu and then click **Upgrade/Backup**.

⇒ Select one of the three options (Firmware, Configuration, DHCP Settings) and click **Backup** or **Upgrade**.

A **Select Backup File** or **Select Upgrade File** window will appear and give you the following default files in the name box:

- For Firmware, the default file is KERNEL.2K
- For Configuration, the default file is SYSTEM.CNF
- For DHCP, the default file is DHCP.DAT

⇒ Click **OK** if appropriate.

⇒ Otherwise select the proper file and directory from the list below the name box and click **OK**.

Reboot From Network

Reboot from Network is used in the following situations:

- To perform Beta testing (e.g., testing new router software before downloading to FLASH memory)
- To allow several routers to reboot from the same file on a server

Rebooting from the network will upload the file you have specified into the router and execute it.

Note 1: KERNEL.2K is the default file and is installed under the default directory C:\DSL or wherever you may have installed Configuration Manager.

Note 2: A Trivial File Transfer Protocol (TFTP) utility is built into Configuration Manager and is capable of reading from and writing to the network.

◇ Instructions

⇒ To reboot from the network, click **Tools** from Configuration Manager's main menu and then click **Reboot from Network**.

A new window will appear and let you select the file to boot from, in the file name box. KERNEL.2K is the default file.

⇒ Click **OK** to enable your choice.
Enter your login password and click **OK**.

SNMP Options

The router is preconfigured with the following SNMP default settings:

- **public** for the Community Name
- **161** for the UDP Port

You may, however, want to change the default settings for security reasons or to allow SNMP monitoring of a device located on the LAN while running NAT; both the device and the router can be monitored or managed at different UDP ports. Changing the settings will affect only the Windows configuration parameters but will not change the actual settings in the router.

The router values can only be changed with the Command Line Interface using the `system snmpport` or `system community` command.

◇ Instructions

- ⇒ Click **Tools** and **SNMP Options**.
- ⇒ You may set the **UDP Port** to any number between 1 and 65,535. Make sure that the port you select does not conflict with another defined port.
- ⇒ The **Community Name** can be a string of up to 40 characters. Special characters are allowed.

Chapter 5. Router Feature Descriptions

The FlowPoint supports the following industry standard protocols, security features, compression algorithms, and network management tools to ensure interoperability with other vendors' equipment.

- IEEE 802.3 Ethernet
- Point-to-Point Link Protocol (PPP)
- ADSL (Asymmetric Digital Subscriber Line)
- ATM (Asynchronous Transfer Mode)
- HDSL (High-Speed Digital Subscriber Line)
- SDSL (Symmetrical Digital Subscriber Line)
- RFC 1483 Link Protocol
- RFC 1483MER Link Protocol
- Password Authentication Protocol and Challenge Handshake Authentication Protocol (PAP/CHAP)
- Bridging, Routing, IPX Routing
- IEEE 802.1D Bridging
- Bridging and Routing Protocol Filtering
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)
- Software upgrade utilities
- TELNET
- Windows GUI Configurator
- Command Line Interface

IEEE 802.3 Ethernet

The router provides a standard 802.3 Media Access Control layer for CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Ethernet communications.

Point-To-Point Link Protocol (PPP)

PPP is a data link layer industry standard WAN protocol for transferring multi-protocol data traffic over point-to-point connections. It is suitable for both high-speed synchronous ports as well as lower speed asynchronous dial-up ports. With this protocol, options such as security and network protocols can be negotiated over the connection.

The FlowPoint router supports synchronous PPP over the ATM/DSL link. The STAC® Electronics Stacker LZS™ Compression Protocol is supported over PPP providing up to 4:1 data compression.

The Ascend and Microsoft variants are also supported.

Asymmetric Digital Subscriber Line (ADSL)

Asymmetric Digital Subscriber Line technology allows high-speed communication between two sites over the telephone wire. Normally the speed in one direction is higher than the speed in the other direction. This communication is performed using digital modems.

Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode allows the transmission of fixed-size cells over a network. The user's data is broken up into large chunks known as AAL5 PDUs. Each PDU is of variable size but is roughly equivalent in size to an Ethernet frame. Each AAL5 PDUs are then broken up into a number of fixed-length ATM cells for transmission. Reception is the reverse process.

High-Speed Digital Subscriber Line (HDSL)

HDSL is a DSL option that offers high-speed data rates of up to 1.1 Mbits/sec over existing copper wires. It uses HDLC frames on the line.

Symmetrical Digital Subscriber Line (SDSL)

This DSL service is similar to HDSL. It also allows for data rates of up to 1.1 Mbits/sec.

RFC 1483 Link Protocol

RFC 1483 is an IETF recommendation that describes the rules used to send IP, IPX, and bridging frames using AAL5 connections over ATM.

RFC 1483MER Link Protocol

Similar to RFC 1483 but with MAC Encapsulated Routing (MER) . This link protocol encapsulates routed Ethernet frames into bridged ATM cells (RFC 1483).

PAP And CHAP Security

The router supports the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) under PPP.

PAP provides verification of passwords between routers using a 2-way handshake:

One router (peer) sends the system name and password to the other router. Then the other router (known as the authenticator) checks the peer's password against the configured remote router's password and returns acknowledgment.

CHAP is more secure than PAP as unencrypted passwords are not sent across the network. CHAP uses a 3-way handshake:

One router (known as the authenticator) challenges the other router (known as the peer) by generating a random number and sending it along with its system name. The peer then applies a one-way hash algorithm to the random number and returns this encrypted information along with its own system name. The authenticator then runs the same algorithm and compares the result with the expected value. This authentication method depends upon a password or secret, known only to both ends.

Bridging And Routing

Bridging

Bridging connects two or more LANs together so that all devices share the same logical LAN segment and network number. The MAC layer header contains source and destination addresses used to transfer frames. An address table is dynamically built and updated with the location of devices when the frames are received. Transparent bridging allows locally connected devices to send frames to all devices as if they are local.

Bridging allows frames to be sent to all destinations regardless of the network protocols used. It allows protocols that cannot be routed (such as NETBEUI) to be forwarded and allows optimizing Internetwork capacity by localizing traffic on LAN segments. A bridge extends the physical reach of networks beyond the limits of each LAN segment. Bridging can increase network security with filtering.

Routing

Routing provides a way to transfer user data from source to destination over different LAN and WAN links using one or more network protocol formats. Routing relies on routing address tables to determine the best path for each packet to take.

Routing tables can be seeded; i.e., addresses for remote destinations are placed in the table along with network address masks and a metric for path latency.

Routing tables are also built dynamically; i.e., the location of remote stations, hosts and networks are updated from broadcast packet information.

Routing helps to increase network capacity by localizing traffic on LAN segments and reducing the amount of broadcasts that would result from bridged traffic. It also provides security by isolating traffic on segmented LANs. Routing extends the reach of networks beyond the limits of each LAN segment.

Bridging and Routing

The FlowPoint router can operate as a bridge, as a router, or as both (sometimes called a brouter). The router will operate as a router for network protocols that are supported when routing is enabled. The router will operate as a bridge when bridging is enabled. When both bridging and routing are enabled, routing takes precedence over bridging; i.e., the router uses the packet's protocol address information to route the packet; if the protocol is not supported, the router will use the MAC address information to bridge the packet.

Operation of the FlowPoint router is influenced by routing and bridging controls and filters set during router configuration as well as automatic spoofing and filtering performed by the router. General IP or IPX routing, and routing or bridging from/to specific remote routers are controls set during the configuration process.

Spoofing and filtering which minimize the number of packets that flow across the WAN, are performed automatically by the router. For example, RIP routing packets and certain NetBEUI packets are spoofed even if only bridging is enabled. For more detailed information on packet routing and bridging, refer to the section *Routing and Bridging Operation* in the *Command Line Interface* guide.

IEEE 802.1D Bridging

The FlowPoint router supports the IEEE 802.1D standard for LAN-to-LAN bridging. Bridging is provided over PPP as well as adjacent LAN ports. The bridging software uses transparent bridging. Configured as a bridge, the unit bridges data packets to the destination, regardless of the network protocols used.

Also included is the **Spanning Tree Protocol** allowing the FlowPoint router to interoperate with other vendors' bridge/routers. This is a learning bridge; i.e., the bridge builds and updates an address table with each MAC source address and associated information when the packets are received.

IP Routing

IP routing support provides the ability to process TCP/IP frames at the network layer for routing. IP routing support includes the Routing Information Protocol (RIP) which allows the exchange of routing information on a TCP/IP network. The router receives and broadcasts RIP messages to adjacent routers and workstations. Since IP sends out periodic RIP frames that could keep communication links permanently connected, filtering and spoofing are performed to minimize these broadcasts on the WAN links. The router uses the 'piggyback method' to send RIP update packets to the WAN port. The piggyback method means that RIP update packets are sent only when the communication link is established because of data traffic.

IPX Routing

Internetwork Packet Exchange (IPX) Routing support provides the ability to process IPX frames at the network layer. This support includes the Routing Information Protocol (RIP)* which allows the exchange of routing information on an Internetwork, and the Service Advertising Protocol (SAP) which provides a means of exchanging Internetwork service information. The router receives and broadcasts RIP and SAP messages to adjacent routers and workstations so that clients on the network can determine what services (file, print, etc.) are available on the network and obtain the Internetwork address of the servers.

Since IPX sends several types of control packets that could keep communication links permanently connected, control of updates and spoofing techniques are employed to reduce this traffic. Specifically, RIP, SAP, Watchdog, and serialization frames are filtered and spoofed. RIP and SAP update frames are only sent piggybacked with data packets. SAP requests for the nearest server are spoofed, serialization frames are dropped, and Watchdog frames are spoofed.

IPX-RIP is similar to IP-RIP except IPX-RIP includes a time delay in addition to a hop count.

Bridging And Routing Protocol Filtering

Filtering can be used to allow efficient usage of network resources and provide security for your network and hosts.

IP Internet Firewall

The FlowPoint router supports IP Internet Firewall filtering to prevent unauthorized access to your system and network resources from the Internet. A security violation can occur when a packet is received from a WAN link, typically connected from the Internet, which has the source IP address of a host on your LAN. This filter discards packets received from the WAN which have a source IP address recognized as a local LAN address.

Note: Most routers' Firewall implementations protect against one form of intrusion. The built-in protection Firewall of the FlowPoint router does not take the place of a professional Firewall system designed to protect against multiple violations.

Bridge Filtering

Bridge filtering allows a network administrator to control the flow of packets across the router. Bridge filtering can be used to 'deny' or 'allow' the transmission or reception of packets based on a 'matched pattern' using a

specified position and hexadecimal content within the packet. Common uses are to prevent access to remote networks, control unauthorized access to the local network and limit unnecessary traffic. (This feature can only be configured through the Command Line Interface.)

Simple Network Management Protocol (SNMP)

The FlowPoint router provides SNMP agent support and support for standard as well as Enterprise Specific MIBs. SNMP is also used internally for configuration of the router. The active SNMP agent within the router accepts SNMP requests for status, statistics, and configuration updates.

Communication with the SNMP agent occurs over the LAN or WAN connection. Any management application using SNMP over UDP/IP (User Datagram Protocol/Internet Protocol) has access to the local SNMP agent.

The following MIBs are supported:

- MIB II
- Bridge MIB
- Ethernet MIB
- IP Forwarding MIB
- PPP MIB For LCP
- Enterprise MIB for configuration

Dynamic Host Configuration Protocol (DHCP)

DHCP is used to acquire IP addresses and options (such as the subnet mask, DNS, gateway, etc.) automatically. On the practical level, acquiring these initialization parameters with DHCP translates into avoiding the more involved router/PC process (reconfiguration of router and/or PC addresses to be in the same network).

Network Address Translation (NAT)

NAT is an IP address conversion feature that translates a PC's local (internal) address into a temporary global (outside/Internet) IP address.

NAT is needed when a PC (or several PCs) on a Local Area Network wants to connect to the outside Internet to get to a remote network: NAT swaps the local IP address to a global IP address. Our version of NAT goes one step further by allowing several PCs to share one single IP address to the Internet, thus reducing connection costs. In effect, it allows a whole LAN to connect to the Internet as a Single User.

Software Upgrades

Software upgrades can be performed remotely using the TFTP protocol for the software download process. The router's file system is a DOS-compatible file system and any file contained within the system may be retrieved or replaced using the TFTP protocol. Specifically, configuration files and operating system upgrades can be updated. Chapter 5, *Management Tools*, describes how to upgrade software, boot the router from the network, make copies of configuration files, and perform other maintenance procedures. A TFTP server is provided with the FlowPoint software.

TELNET

TELNET access to the router is supported. TELNET allows you to log into the router as if directly connected through the console port. In this manner you can issue commands, using the Command Line Interface (the Command Line Interface guide is provided with the router), to configure the router and perform status monitoring from any remote location.

Any of the available TCP/IP packages containing the TELNET application can be utilized.

A special feature, **History Log**, described on page 99, allows the redirection of all console output (including notifications that would only appear at the console terminal) to any TELNET session.

Windows GUI Configurator

A Microsoft® Windows™-based program, the FlowPoint Configuration Manager, is provided for configuring the FlowPoint router. This Windows GUI point-and-click configurator is described in the chapter *Installing and Accessing Configuration Manager*. A Winsock-compliant TCP/IP stack must be installed on your PC to run Configuration Manager.

Command Line Interface

Configuration is also supported through the Command Line Interface. This interface provides the ability to configure the same basic features as the Windows GUI configurator, but through the console port or Telnet. It also gives you the following capabilities:

- Configuration of advanced features such as bridge filtering
- Online status commands and error message monitoring
- Statistics
- Unique PAP or CHAP authentication or system name passwords
- Additional DHCP options

These topics are discussed in the *Command Line Interface* guide.

Chapter 6. Troubleshooting

This chapter discusses diagnostic tools that are available to help identify and solve problems that may occur with your FlowPoint router. It also describes some common hardware and software problems and gives some suggestions to troubleshoot them.

Diagnostic Tools

Using LEDs

Most hardware problems can be diagnosed and solved by checking the LEDs on the front panel of your router.

The following table summarizes the normal LED sequence in the left column (5 consecutive states) from “Power On” to “Ready State”. The right column lists suggestions to problems reflected by an “abnormal” LED state (no progression to the next state).

Note that this normal progression involves:

- PWR LED (Power LED)
- TEST LED (Self test indicator LED)
- LINK LED (ATM modem link)

If the Power (PWR) light is off:

- Check that the power cord is firmly plugged into the back panel of the FlowPoint router and the other end into an active AC wall or power strip outlet.
- Check that the power switch is turned on.

Normal LED Sequence	State Length	Problem If the LED sequence stops at this stage:
State 1 Power ON PWR - green TEST - amber LINK - off	5 sec	A hardware problem has been detected. ⇒ Contact Technical Support.
State 2 All lights flash	1 sec	
State 3 PWR - green TEST - green LINK - off	5 sec	1. Check that the DIP switches are all up. 2. Check that the correct software was loaded.
State 4 PWR - green TEST - green LINK - amber	5 to 10 sec	1. Check your DSL cables. 2. Check the physical connection from your router to the DSLAM (Central Office). 3. Possible problem with DSLAM card.
State 5 PWR - green TEST - green LINK - green	Ready State	

Once the router is in “Ready State”, the other LEDs may indicate transmitting and receiving activity as follows:

The WAN LED indicates that the DSL WAN is transmitting activity.

The LANT LED indicates that the Ethernet LAN is transmitting activity.

The LANR LED indicates that the Ethernet LAN is receiving activity.

Troubleshooting Help File

Configuration Manager's **Help** file features an extensive troubleshooting section that is meant to help you diagnose and solve problems quickly through a logical process of elimination.

This **Troubleshooting** file is also available as a freestanding application in the FlowPoint directory.

⇒ To access it, click the **Start** your PC's desktop, click **Programs**, **FlowPoint DSL Tools**, and double-click **Troubleshooting Help**.

History Log

The **History Log** utility is a troubleshooting tool which displays the router's activity. It can be accessed from a terminal emulation session (including Configuration Manager) or from TELNET.

To access the logging utility through Configuration Manager:

1. Select **Tools** and **Terminal Window** (the console cable is required).
2. Log in with your administration password into the router (e.g. "admin").
3. Use the command **system history** to view the buffer contents.

To access the logging utility through TELNET:

1. Click **Connect** from the menu, and then **Remote System**.
2. Enter the router's IP address.

Other Logging Commands

- If you wish to monitor your router activity at all times, enter the command **system log start** to view a continuous log, using TELNET. (This command will not work in a Terminal Window session, but only from TELNET.)
- The command **system log status** is used to find out if other users, including yourself, are using this utility.

- To discontinue the log, use the command **system log stop**.

When you exit TELNET, you automatically stop any logging programs running in that session.

Note: History Log is preserved across reboots, but not across power outages or power down.

Ping Command

You can verify IP connectivity to the router by running a **ping** command. You will probably find a ping utility bundled with your TCP/IP stack. In Windows 95 and Microsoft's TCP/IP 32-bit stack for Windows for Workgroups, the command is called PING.EXE and can be found in your Windows directory.

Note: Before using the **ping** command to troubleshoot, make sure that the PWR, TEST, and LINK lights are green.

◇ Instructions

Start a DOS window

1. Select **Start** from the Windows 95 taskbar.
2. Select **Programs**.
3. Select **MS-DOS Prompt**.

Issue the Ping command

In the DOS window, type the command:

ping <IP address>

Example: ping 192.168.254.254

◇ Troubleshooting with Ping

To isolate a problem with the TCP/IP protocol, perform the following three tests:

1. Try to ping the IP address of your PC. If you get a response back, proceed directly with step 2. If you don't get a response back, check that:
 - The network adapter card is installed.
 - The TCP/IP protocol is installed.
 - The TCP/IP protocol is bound to the network adapter.
2. Try to ping the IP address of your router. If you get a response back, proceed directly with step 3. If you don't get a response back, the problem lies between your PC and router:
 - Check the cables.
 - Check the hub.
 - Make sure that your PC and the local router belong to the same IP subnetwork.
3. Try to ping the DNS server. Write the results down and call your Network Service Provider.

Investigating Hardware Installation Problems

Check the LEDs to Solve Common Hardware Problems

Please refer to this chapter's section entitled *Diagnostic Tools, Using LEDs*, for more information.

Problems with the Terminal Window Display

- Ensure that your console is plugged in and turned on.
- Verify that you are on the right communications port (Com1, Com2).
- Check the configuration parameters for speed, parity, etc. Make sure the console is not in an XOFF state. Try entering a 'ctrl q'.

- Verify that the RS232 device attached to the console is configured as a 'DTE'. If not, a crossover or null modem adapter is required.

Problems with the Factory Configuration

- Compare the FlowPoint router configuration with your FlowPoint router order.
- Verify that the model number is correct (displayed during the boot procedure). The model number (and serial number) is also displayed on the main window of Configuration Manager.

Investigating Software Configuration Problems

Problems Connecting to the Router

If you cannot connect your PC to the target router for configuration:

- For a LAN connection, verify that the router's IP address matches the IP address previously stored into the router's configuration.

You must have previously set the router's Ethernet LAN IP address and subnet mask, saved the Ethernet configuration changes, and rebooted the router for the new IP address to take effect.

- Check that your LAN cable is pinned correctly and each pin end is securely plugged in.

Note: If using a straight-through cable, the colors for pins 1, 2, 3, and 6 should match on both connectors.

If using a crossover cable, the colors for pins 1, 2, 3, and 6 on one connector should match respectively 3, 6, 1, and 2 on the other connector.

- Make sure the PC and target router are on the same IP subnetwork or the target router is reachable through a router on your LAN. They can, however, be on different networks if IP routing is off.

- Check Network TCP/IP properties under Windows 95 and the control panel of the TCP/IP driver installed under Windows 3.1.
- Check if the LAN LED on the router's front panel blinks when 'pinged'.
- Check your Ethernet board IRQ settings: the PC's table may become confused. If so, reboot your PC.

Problems with the Login Password

You have been prompted for the login password and received the following message: "Login Password is invalid".

- Re-enter the correct password and press enter. Remember that the password is case sensitive. Check that you are entering `admin` in lowercase and that the Caps key is not active.
- If you have forgotten the password, you must reset the login password. Refer to appendix D, *Changing Configuration Switches*, and perform the following procedure:
 1. Move switches **5** and **6** down.
 2. Type **login newpasswd**. Password checking is overridden.
 3. Move switches **5** and **6** up.
 4. Complete any configuration update that caused the prompt for login.
 5. Change your login password to a new password.
 6. Store the configuration and reboot the router.

Note: If you have not reset switches **5** and **6** up and have rebooted, you will place the router in maintenance mode. Set switches **5** and **6** up and turn the power off and then on.

Problems Accessing the Remote Network

◆ If Bridging

- Be sure to reboot if you have made any bridging destination or control changes.

- All IP addresses must be in the same IP subnetwork (IP is being bridged).

◇ **If TCP/IP Routing**

- Check that IP Routing is enabled at the local and the remote end.
- The IP addresses of the local and remote networks belong to different IP subnetworks.
- Make sure that there is an existing route to the remote network.
- Make sure that there is a route back from the remote network.
- There must be a Source WAN IP Address defined when using NAT.
- Check that, if required, the source and remote WAN IP addresses are on the subnetwork.
- Reboot if you have made any IP address, control, or protocol option changes.

◇ **If IPX Routing**

- Check that IPX Routing is enabled at the local and the remote end.
- Validate that the IPX WAN network number matches the remote router's WAN network number.
- Check that IPX SAPs correctly identify the servers and applications on the remote network and have valid network numbers, node numbers, etc.
- Check that every SAP has a router to its internal network.
- Check that the IPX Routes (network numbers, hops, and ticks) seeded into the routing table for network segments and servers beyond the remote router are correct.

How To Obtain Technical Support

Before contacting Technical Support, gather the following information:

- Description of the problem, onset, duration, and affected components.
- FlowPoint router's serial numbers, and the date you purchased the products.
- Level and success of the Power-On-Self-Test.
- List of other equipment such as personal computers, modems, and third party software you are using, including revision levels.
- Software version number.

Technical support, repair services, and spare parts are available through your FlowPoint Distributor. Otherwise, FlowPoint can provide assistance in the U.S. Warranty repairs must be accompanied by dated proof of purchase.

Contact FlowPoint at:

Phone number: **1-408-364-8530**

Fax number: **(408) 364-8301**

Email: **support@flowpoint.com.**

Appendix A. Software Specifications

ROUTING

Multi-user sharing via Ethernet LAN

TCP/IP with RIP1-Compatible, RIP1, RIP2, or static routing on the LAN and/or WAN

DHCP Relay Agent

DHCP Server – Automatic assignment of IP Address, Mask, Default Gateway, and DNS servers addresses to workstation (RFC 1541, RFC 1533)

Novell

IPX with RIP/SAP

DNS Relay

FlowPoint DHCP Client

Network Address Translation (NAT)

FlowPoint NAT Server Support

Network Renumbering

BRIDGING

Transparent Bridging (IEEE 802.1D)

Fully meshed or point-to-point topology support

Spanning Tree Protocol (802.1D)

Bridge Filters

BANDWIDTH OPTIMIZATION FEATURES

Data Compression, up to 4:1 (STAC LZS)

Van Jacobson Header Compression

Spoofing and filtering (IP-RIP packets, IPX-RIP, SAP, Watchdog, Serialization)

ATM

PPP & RFC 1483 over ATM transports

PPP-RFC 1661 (VC-Based/LLC Multiplexing)

ATM cell-based link layer

AAL5 adaptation using SAR

Up to 8 Virtual Circuits (VCs)

Virtual Circuit (VC) traffic shaping

NETWORK MANAGEMENT

Internet Quick Start Program

GUI-based Configuration Manager for local or remote management

Administration through SNMP, MIB-II, Telnet, or VT100 Terminal

TFTP download/upload of new software, configuration files, and scripts

Dynamic Host Configuration Protocol (DHCP) for simple installation and security

BootP Server

One RS232 asynchronous console port (RJ45)

SECURITY AND VPN OPTIONS

User authentication (PAP/CHAP) with PPP

Password control for Configuration Manager

L2TP Tunneling with DES encryption

Dynamic key exchange

Telnet/SNMP port management

SNMP community name reassignment

Telnet/SNMP management control features

PROTOCOL PERFORMANCE TESTING

RFC 1483 (Bay Networks, Cabletron, Cisco, RedBack)

PPP over ATM (ATML, Cisco, RedBack)

L2TP (Bay Networks, Ascend, IBM, Cisco, Novell)

Appendix B. Network Information Worksheets

To configure the target (local) router, you need to fill out one of the following blank worksheet(s) that applies to your Link Protocol/Network Protocol situation:

- PPP with IP Routing configuration
- PPP with IPX Routing configuration
- PPP with Bridging configuration
- RFC 1483 with IP Routing configuration
- RFC 1483 with IPX Routing configuration
- RFC 1483 with Bridging configuration
- RFC 1483MER with IP Routing configuration

If you are connecting to more than one remote router, you need to fill out one set of information for each remote router in the *Remote Routers* section of the worksheet.

If you are setting up both ends of the network:

You will need a mirror image of the information listed in your target router worksheet for configuring the router on the other end of the ATM/DSL link.

You will find the Network Information Worksheets for each Link Protocol/Network Protocol association on the following pages.

Note: You may want to review one of the sample configurations, page 41.

PPP with IP Routing		
STEP/BUTTON	ITEM	YOUR SETTINGS
System Settings		
System Name	Required	
System Message	Optional	
Authentication Password	Required	
Ethernet IP Address	As required	
DHCP Settings	Already enabled; additional settings may be required	
Change Login	Optional	
Remote Routers		
New Entry	Enter: Remote Name	
Link Protocol/PVC	Link Protocol	PPP
	Enter: VPI/VCI numbers	
Security Remote's Password	Choose security level	
	Enter: password	
Bridging On/Off	Select: OFF	OFF
TCP/IP Route Addresses	Enter required information	
If NAT is enabled: TCP/IP Route Addresses, Advanced	Enter: Source WAN Port Address (if required by ISP)	
If NAT is not enabled: TCP/IP Route Addresses, Advanced	Enter: Source WAN Port Address (if required by ISP)	
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Select: ON (Optional)	ON
IPX Routing	Select: OFF	OFF

Note: Don't forget to store your configuration and reboot the router.

PPP with IPX Routing		
STEP/BUTTON	ITEM	YOUR SETTINGS
System Settings		
System Name	Required	
System Message	Optional	
Authentication Password	Required	
Ethernet IP Address	As required	
DHCP Settings	Already enabled; additional settings may be required	
Change Login	Optional	
Ethernet IPX Network #	Enter: IPX Network # Frame Type	
Remote Routers		
New Entry	Enter: Remote Name	
Link Protocol/PVC	Select: PPP	PPP
	Enter: VPI/VCI Numbers	
Security Remote's Password	Choose security level	
	Enter: Password	
Bridging On/Off	Select: OFF	OFF
IPX Routes Add	Enter appropriate information	
IPX SAPs Add, Modify	Enter appropriate information Enter WAN Network #	
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Select: OFF Optional	OFF
IPX Routing	Select: ON	ON

Note: Don't forget to store your configuration and reboot the router.

PPP with Bridging

STEP/BUTTON	ITEM	YOUR SETTINGS
System Settings		
System Name	Required	
System Message	Optional	
Authorization Password	Required	
DHCP Settings	Already enabled; additional settings may be required	
Change Login	Optional	
Remote Routers		
New Entry	Enter: Remote Name	
Link Protocol/PVC	Select: PPP	PPP
	Enter: VPI/VCI	
Security	Choose security level	
Remote's Password	Enter: Password	
Bridging On/Off	Select: ON	ON
IP and IPX Routing		
IP Routing (Internet Firewall)	Select: OFF Optional	OFF
IPX Routing	Select: OFF	OFF

Note: Don't forget to store your configuration and reboot the router.

RFC 1483 with IP Routing		
STEP/BUTTON	ITEM	YOUR SETTINGS
System Settings		
System Message	Optional	
Ethernet IP Address	As required	
DHCP Settings	Already enabled; additional settings may be required	
Change Login	Optional	
Remote Routers		
New Entry	Enter: Remote Name	
Link Protocol/PVC	Select: RFC 1483	RFC 1483
	Enter: VPI/VCI Numbers	
Bridging On/Off	Select: OFF	OFF
TCP/IP Route Addresses Add	Enter: Explicit or default route	
If NAT is enabled: TCP/IP Route Addresses, Advanced	Enter: Source WAN Port Address	
If NAT is OFF: TCP/IP Route Addresses, Advanced	You may need to enter a Source WAN Port Address	
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Select: ON (Optional)	ON
IPX Routing	Select: OFF	OFF

Note: Don't forget to store your configuration and reboot the router.

RFC 1483 with IPX Routing

STEP/BUTTON	ITEM	YOUR SETTINGS
System Settings		
System Message	Optional	
Ethernet IP Address	As required	
DHCP Settings	Already enabled.; additional settings may be required	
Ethernet IPX Network #	Enter : IPX Network #	
	Frame Type	
Change Login	Optional	
Remote Routers		
New Entry	Enter: Remote Name	
Link Protocol/PVC	Select: RFC 1483	RFC 1483
	Enter: VPI/VCI Numbers	
Bridging On/Off	Select: OFF	OFF
IPX Routes Add	Enter appropriate information	
IPX SAPs Add	Enter appropriate information	
Modify	Enter WAN Network Number	
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Select: OFF (Optional)	OFF
IPX Routing	Select: ON	ON

Note: Don't forget to store your configuration and reboot the router.

RFC 1483 with Bridging

STEP/BUTTON	ITEM	YOUR SETTINGS
System Settings		
System Message	Optional	
DHCP Settings	Already enabled; additional settings may be required	
Change Login	Optional	
Remote Routers		
New Entry	Enter: Remote Name	
Link Protocol/PVC	Select: RFC 1483	RFC 1483
	Enter: VPI/VCI Numbers	
Bridging On/Off	Select: ON	ON
IP and IPX Routing		
IP Routing (Internet Firewall)	Select: OFF Optional	OFF
IPX Routing	Select: OFF	OFF

Note: Don't forget to store your configuration and reboot the router.

RFC 1483MER with IP Routing

STEP/BUTTON	ITEM	YOUR SETTINGS
Connect		
System Settings		
System Message	Optional	
Ethernet IP Address	As required	
DHCP Settings	Already enabled; additional settings may be required	
Change Login	Optional	
Remote Routers		
New Entry	Enter: Remote Name	
Link Protocol/PVC	Select: RFC1483MER Enter: VPI/VCI Numbers	RFC 1483MER
Bridging On/Off	Select: OFF	OFF
TCP/IP Route Addresses Add	Enter: explicit or default route with Remote Gateway	
If NAT is enabled: TCP/IP Route Addresses, Advanced	Enter: Source WAN Port Address and Mask	
If NAT is OFF: TCP/IP Route Addresses, Advanced	Enter: Source WAN Port Address and Mask	
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Select: ON (Optional)	ON
IPX Routing	Select: OFF	OFF

Note: Don't forget to store your configuration and reboot the router.

Appendix C. Command Line Interface

Why Use The Command Line Interface?

You will need to connect the router to the PC in order to access the Command Line Interface (CLI) when Configuration Manager is not compatible with certain platforms, cannot be used for complex configuration tasks, or if you initially experience trouble connecting to the router.

Non-Windows users have to configure their router using the CLI; Windows users may have to rely on it in specific situations, as is described below.

For Non-Windows Platforms (Macintosh, UNIX, etc.):

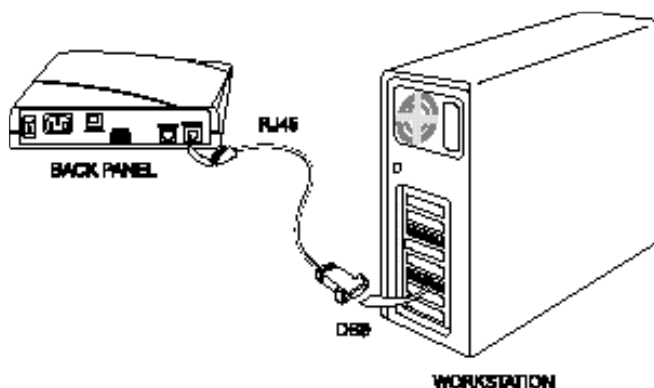
The CLI is the only configuration software available to non-Windows users. It is accessed from an ASCII terminal emulation or via Telnet to the router. It is needed to initialize the router's IP address manually and for all configuration matters.

For Windows-based Platforms:

The CLI is used selectively for a number of situations. It can be accessed from within Configuration Manager program or independently of it. It is specifically needed to:

- Change an existing IP address.
- Perform advanced configurations.
- Be used by network managers as the preferred management tool (for remote software management and maintenance and troubleshooting).

Connecting The Router To The PC



You will use the following cable and adapter:

- One 10-foot length of unshielded twisted pair cable with RJ45 connectors on either end. This cable has a green label marked “**Console**”.
- One RJ45 to DB9 adapter (console port to PC).

◇ Instructions

1. Plug the RJ45 connector at one end of the cable into the RJ45 jack marked **Console** on the back panel of the router.
2. If you are connecting directly to a workstation, attach the DB9 adapter to the other end of the cable and connect that end to your workstation.

Accessing The Command Line Interface

The Command Line Interface is available at all times once you have installed the router's hardware, connected the PC with a terminal emulation session (or ASCII) session, and powered the unit on. For specifics regarding the CLI commands, refer to the *Command Line Interface* guide (provided on diskette 3).

◇ Instructions

To Open a Terminal Window Emulation Program under Windows:

1. Click the **Start** button located on your PC desktop.
2. Click **Programs, Accessories, Hyper Terminal**.
3. Click **HYPERTERM.EXE**.
4. Assign the communications port connected to the console.
5. Set the terminal communications settings to the following configuration parameters:
 - 9600 bits per second
 - 8 bits
 - No parity
 - XON/XOFF support
 - 1 stop bit

To Open a Terminal Window Emulation from within Configuration Manager:

Use of Configuration Manager's Terminal Window is suitable for advanced configuration and file management. The communications settings are the same as described above.

1. Click **Tools**.
2. Click **Terminal Window**. You now have the ability to select a command using the **Commands** Menu function.

To Open a Terminal Window Emulation in a Macintosh or UNIX Environment:

Refer to your system documentation to determine which appropriate communications programs to use to communicate with the router's emulation mode.

To Access the Terminal Window via TELNET:

1. The PC address and the router address have to be in the same subnetwork.

Example:

Router address is: 192.168.254.254

PC address is: 192.168.254.253

2. Click the **Start** button located on the PC desktop, click **Programs**, click **Windows Explorer**, **Windows**, and **TELNET.EXE**.
3. Select **Connect** and **Remote System** from the menu.
4. In the **Connect** window, enter the router's IP address. Click **Connect**.

Appendix D. Changing Configuration Switch Settings

The configuration switches are located under the label CONFIG on the rear panel of the router. You might need to alter the configuration switches for:

- Upgrading software
- Troubleshooting with a qualified service representative
- Resetting the login password

Configuration Switch Settings

When you receive the router, switches 5 and 6 are set for the normal operation of the router. If these switches are not set in these positions when you receive the unit or you change the settings, reset them to continue normal operation.

Switches 1- 4 are not operational.

The following table describes the meaning of each configuration switch when in the **up (off)** or **down (on)** position.

Configuration Switch Settings		Description
Switch 5	UP (normal)	Normal router operation mode
	DOWN	Maintenance mode
Switch 6	UP (normal)	Automatic boot
	DOWN	Manual boot

With both switches 5 and 6 in the down (on) position after the router has booted, the login password is overridden allowing a forgotten password to be re-entered.

Appendix E. Subnetwork Tables

Numbers of Users	Mask in decimal	Mask in hexadecimal	Bits in mask	Range of valid addresses
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.1 - .6
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.9 - .14
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.17 - .22
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.25 - .30
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.33 - .38
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.41 - .46
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.49 - .54
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.57 - .62
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.65 - .70
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.73 - .78
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.81 - .86
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.89 - .94
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.97 - .102
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.105 - .110
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.113 - .118
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.121 - .126
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.129 - .134
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.137 - .142
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.145 - .150
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.153 - .158
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.161 - .166
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.169 - .174
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.177 - .182
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.185 - .190
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.193 - .198
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.201 - .206
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.209 - .214
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.217 - .222
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.225 - .230
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.233 - .238
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.241 - .246
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.249 - .254
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.1 - .14
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.17 - .30
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.33 - .46
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.49 - .62
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.65 - .78
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.81 - .94
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.97 - .110
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.113 - .126
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.129 - .142
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.145 - .158
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.161 - .174
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.177 - .190
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.193 - .206
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.209 - .222
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.225 - .238
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.241 - .254
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.1 - .30
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.33 - .62
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.65 - .94
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.97 - .126
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.129 - .158
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.161 - .190
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.193 - .222
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.225 - .254
61 (+ 1 router)	255.255.255.192	FFFFFFC0	26	.1 - .62
61 (+ 1 router)	255.255.255.192	FFFFFFC0	26	.65 - .126
61 (+ 1 router)	255.255.255.192	FFFFFFC0	26	.129 - .190
61 (+ 1 router)	255.255.255.192	FFFFFFC0	26	.193 - .254
125 (+ 1 router)	255.255.255.128	FFFFFF80	25	.1 - .126
125 (+ 1 router)	255.255.255.128	FFFFFF80	25	.129 - .254
254 (+ 1 router)	255.255.255.0	FFFFFF00	24	.1 - .254

Note 1: the router should be the lowest address in the given range.

Note 2: the mask 255.255.255.252 is legal, but it only provides for 2 addresses.

Glossary

10Base-T

IEEE 802.3 standard for the use of Ethernet LAN technology over unshielded twisted pair wiring, running at 10Mbps.

ADSL

Asymmetric Digital Subscriber Line - Technology that delivers high-speed data and voice connections over existing phone lines. Up to 6.2 MBits/sec can be sent downstream and 1.1 Mbits/sec upstream.

ARP

Address Resolution Protocol. An Internet protocol used to bind an IP address to Ethernet/802.3 addresses.

ASCII

American Standard Code for Information Interchange. 8-bit code for character representation.

ATM

Asynchronous Transfer Mode - Cell-relay broadband technology for high-speed transmission of video, audio, data over LAN/WAN, making use of fixed-size cells (53-byte cells).

AUI

Access Unit Interface. An IEEE 802.3 transceiver cable connecting the networked device (such as a router) to the MAU (Media Access Unit).

Bridge

A device that segments network traffic. A bridge maintains a list of each segment's nodes and only traffic destined for a node on the adjacent segment is passed across the bridge. A bridge operates at Layer 2 of the OSI reference model.

CHAP

Challenge Handshake Authentication Protocol. A security protocol supported under Point-to-Point Protocol (PPP) used to prevent unauthorized access to devices and remote networks. Uses encryption of password, device names, and random number generation.

Console

Device used by the network administrator to configure and monitor the router. The console employs an RS232 interface. Configuration Manager and Command Line Interface are used on the console.

DCE

Data Communicating Equipment. Equipment used within a network to transfer data from source to destination such as modems.

Data Compression

Techniques used to reduce the number of bits transferred across the communication links that represent the actual data bits. Compression is used to optimize use of WAN links and speed data transmission.

DHCP

Dynamic Host Configuration Protocol - Service that provides network information (such as IP addresses, masks, domain names) to PCs and other clients automatically.

Domain Name

Name given to a hierarchical structure or organization (such as the computing resources of a company). It is similar to an address at which you can be contacted.

DNS

Domain Name Service - Transmission Control Protocol/Internet Protocol (TCP/IP) service which translates a name that a person can remember into an IP address that a computer can use.

DSL

Digital Subscriber Line – Technology that improves the data capacity of the existing twisted-pair wire between the telephone company and most homes and businesses. There are different versions of DSL: ADSL, HDSL, SDSL, etc.

DTE

Data Terminating Equipment. DTE refers to equipment used in a network as the data source and/or destination, such as computers.

DTR

Data Terminal Ready. RS232 signal used for indicating to the DCE the readiness to transmit and receive data.

Dynamic IP Address

IP address that is assigned by the Internet provider and which may change with each connection.

EtherTalk

AppleTalk protocols running on Ethernet.

Filter

Feature to control the flow of data based on protocol or bridge information. Filters can be specific to allow data through or prevent transmission.

Firewall

A combination of techniques used to protect one network from unknown networks and users on the outside. Firewalls can filter or block traffic and act as a management and network security point where all traffic can be scrutinized.

GUI

The Graphical User Interface allows you to communicate with the computer through pull-down menus and icons.

High-Speed Digital Subscriber Line (HDSL)

HDSL is a DSL option that offers high-speed data rates of up to 1.1 Mbits/sec over existing copper wires. It uses HDLC frames on the line.

Hop Count

Represents the number of routers in a network through which the data packet has to pass to get to its destination.

IP address

Internet Protocol Address. A 32-bit address assigned to devices that participate in a network using TCP/IP. An IP address consists of four octets separated with periods defining network, optional subnetwork, and host sections.

IPX (Internet Packet Exchange)

A network layer protocol developed by Novell and used in NetWare and other networks.

Leased Line

A telecommunications line between two service points leased from a communications carrier for private use, usually incurring a monthly service rate.

LEDs

Light Emitting Diodes - Type of indicator lights on the panel of the router.

Link Protocol

Set of standards used over the communication link defining how different computers and other devices will communicate with each other. PPP and RFC 1483 are link protocols. These protocols provide a mechanism through which the network protocols are carried over the DSL/ATM link. Because of compatibility issues, it is essential to have the same Link Protocol selected on both ends of the connection.

Local Area Network (LAN)

A network connecting computers over a relatively small geographic area (usually within a single campus or building).

MAC layer/address

Media Access Control layer/address defined by the IEEE 802.3 specification which defines media access including framing and error detection. Part of the OSI reference model data link layer.

Metric

An algorithm used by routers to determine the best path for transmitting packets to a remote destination based on considerations such as time, delay, cost, etc.

MODEM

Modulator/Demodulator. A device that converts digital signals to/from analog signals for transmission over analog communications lines.

NetWare

A network operating system developed by Novell, Inc. providing shared access to files and other network services. IPX is the main protocol.

Network Layer

Layer 3 of the OSI reference model which provides the protocol routing function.

Node

Refers to a termination point for communication links; entity that can access a network.

NSP

Network Service Provider - Company from which you buy your network services.

OSI

Open System Interconnection. An international standard developed by ITU (formally CCITT) and ISO (International Standards Organization) to facilitate data networking multi-vendor interoperability. The OSI Reference Model defines seven layers, each providing specific network functions.

Packet

A piece of information sent across the network that includes a header and usually user data.

Ping

An echo message, available within the TCP/IP protocol suite, sent to a remote node and returned; used to test the accessibility of the remote node.

PPP (Point-to-Point Protocol)

A Data Link layer protocol that provides asynchronous and synchronous connectivity between computer/network nodes. It defines how packets of information are exchanged between computers or network nodes connect via a point-to-point connection (as opposed to multipoint or broadcast). Includes standardization for security and compression negotiation.

PVC

Permanent Virtual Circuit - Dedicated connection between end stations. The PVC is made up of 2 parts: the VPI and the VCI. In a PVC number of 0,32, 0 represents the Virtual Path Identifier (VPI) and 32 represents the Virtual Circuit Identifier (VCI).

RFC

Request for Comment. Documentation describing Internet communications specifications (e.g. Telnet, TFTP). Often these RFCs are used to achieve multi-vendor interoperability during implementation.

RFC 1483

Protocol that encapsulates ATM cells into logical data link frames.

RFC 1483MER

RFC 1483MER (MAC Encapsulated Routing) creates a virtual Ethernet-to-Ethernet environment by encapsulating IP routed packets into RFC 1483 bridged frames: IP packets are routed between the Ethernet interface and the

WAN interface and then formatted so that they can be understood in a bridged environment

RJ11

Standard 4-wire connectors for telephone lines.

RJ45

Standard 8-wire connectors used for DSL lines.

Router Information Protocol (RIP)

Protocols used in IP and IPX for broadcasting open path information between routers to keep routing tables current.

Routing

A network layer function that determines the path for transmitting packets through a network from source to destination.

RS-232

EIA standard specifying the physical layer interface used to connect a device to communications media.

Serialization Frames

Frames sent out by servers under IPX to check whether illegal copies of NetWare are in use on the network.

Service Advertising Protocol (SAP)

Protocol used in IPX for broadcasting information about services available on the network, such as file servers, CD-ROM drives, and modem pools.

SNMP

Simple Network Management Protocol. A widely implemented Internet network management protocol that allows status monitoring, getting/setting of parameters for configuration and control of network devices, such as routers and bridges.

Spoofing

Spoofing is a technique used to remove poll and update service frames from WAN links while ensuring that the network continues to operate normally. Spoofing is employed to minimize communication line connection time.

Subnet Address

An extension of the Internet 32-bit addressing scheme which allows the separation of physical or logical networks within the single network number

assigned to an organization. TCP/IP entities outside this organization have no knowledge of the internal ‘subnetting’.

Subnet Mask

A 32-bit Internet protocol address mask used to identify a particular subnetwork.

Symmetrical Digital Subscriber Line (SDSL)

This DSL service is similar to HDSL. It also allows for data rates of up to 1.1 Mb/s/sec. This technology uses ATM cells.

TCP/IP

Transmission Control Protocol/Internet Protocol. Refers to a set of Internetworking protocols developed by the U.S. Department of Defense that define a two-level-layered approach for interoperability. TCP provides a connection-oriented transport layer ensuring end-to-end reliability in data transmission. IP provides for network layer connectivity using connectionless datagrams.

TELNET

Internet standard protocol for remote terminal emulation that allows a user to remotely log in to another device and appear as if directly connected.

TFTP

Trivial File Transfer Protocol. A simplified version of the File Transfer Protocol (FTP) allowing for file transfer between computers over a network.

Ticks

The number of ticks represents how much time the packet takes to reach the destination in units of roughly 1/20th of a second.

TPE

Twisted pair Ethernet, also known as 10Base-T.

Transparent Bridging

Bridging technique used in Ethernet networks which allows transfer of frames across intermediate nodes using tables associating end nodes with bridging addresses. Bridges are unknown to the end nodes.

UDP

User Datagram Protocol. A connectionless protocol used to pass packets across an Internet network, requiring no handshaking between source and destination.

VCI

Virtual Channel Identifier - Number that identifies a channel within a virtual path in a DSL/ATM environment.

Virtual Channel

Refers to a logical connection between end stations in an DSL/ATM environment

Virtual Path

Refers to a bundle of virtual channels in a DSL/ATM environment.

VPI

Virtual Path Identifier - Number that identifies the link formed by the virtual path in a DSL/ATM environment.

Watchdog Frames

Frames sent out by servers to clients, under IPX, to verify that clients are still logged on.

Wide Area Network (WAN)

A communications network that is geographically dispersed, thus requiring links provided by communications carriers.

Workstation

Computer or terminal used by the systems administration or user.

Index

A

- ADSL, 88
- advanced features, 73
- ATM, 88
- authentication password, 56

B

- backing up files, 82
- backup tool, 83
- bridge filtering, 93
- bridging
 - general description, 90
 - IEEE 802.1D, 92
 - operation, 91
 - remote router, 63
 - Spanning Tree Protocol, 92
 - transparent, 92

C

- change IP address
 - using the Command Line Interface, 81
- CHAP, 15, 19, 22, 44, 45, 56, 89, 90, 123
- clear configuration files, 83
- Command Line Interface
 - access, 118
 - change IP address with, 81
 - feature description, 96
 - for non-Windows users, 116
 - reasons for using, 5, 116
- commands
 - system wan2wanforwarding, 69
- compression protocol
 - PPP, 88
- configuration
 - authentication password, 56
 - bridging, 91
 - Command Line Interface, 96
 - connecting to target, 53
 - Ethernet IP address, 57

- Ethernet IPX Network Number, 58
- example, 41, 48
- files, 83
- Internet firewall, 68
- IPX route hop count, 66
- IPX route ticks, 66
- IPX routes, 65
- IPX routing control, 68
- IPX SAPs, 67
- link protocols, 14
- login password, 58
- network protocols, 14
- remote router authentication
 - protocol, 62
- remote router bridging, 63
- remote router password, 62
- routing, 91
- saving, 69
- system message, 54
- system name, 54
- tables, 14
- TCP/IP protocol options, 78
- TCP/IP route addresses, 63
- TCP/IP routing control, 68
- TCP/IP WAN addresses, 65
- verifying, 70
- Windows configurator, 96

- Configuration Manager
 - access, 8
 - features, 5
 - general, 5
 - hardware/software prerequisites, 6
 - installation, 7
 - version, 55
- configuration switches
 - changing, 120
- configuration tables
 - general, 32
 - PPP with Bridging, 35
 - PPP with IP Routing, 33
 - PPP with IPX Routing, 34
 - RFC 1483 with Bridging, 38
 - RFC 1483 with IP Routing, 36
 - RFC 1483 with IPX Routing, 37

- RFC 1483MER with IP Routing, 39
- console
 - Command Line Interface, 117
 - connecting, 117

D

- DHCP
 - configuration, 73
 - configuration for the PC, 73
 - configuration for the router, 75
 - general, 58, 73, 94
- diagrams, 26

E

- Ethernet LAN
 - IP Address, 57
 - IP configuration parameters, 16, 24, 31

F

- factory defaults, 83
- file system, 95
- filtering
 - bridging and routing protocol, 93
 - Internet Firewall, 68
 - IP Routing, 92
 - IPX Routing, 93
 - piggyback method, 92

H

- hardware installation, 6
- HDSL, 89
- help file, 99
- history log, 99
- hop count, 66

I

- Internet Account Information, 16, 23, 24, 29, 30
- Internet connection, 2
- Internet Firewall, 68
- IP address, 82

- IP address change, 81
- IP address sharing, 77
- IPX Routing
 - control, 68
 - Ethernet IPX Network Number, 58
 - external network number, 20, 27
 - feature, 92
 - filtering and spoofing, 92
 - frame type, 20, 28
 - hop count, 66
 - internal network number, 20, 27
 - node number, 67
 - Routes, 65
 - SAPs, 67
 - servers, 67
 - socket number, 67
 - ticks, 66
 - WAN network number, 20

L

- LED sequence, 97
- Link Protocol, 60
- link protocol configuration
 - RFC 1483, 23
 - RFC 1483MER, 30
- Link protocol configuration
 - PPP, 15
- logging utility, 99
- login password, 54, 58
- reset, 103

M

- main menu, 54
- maintenance, 95
- management tools, 80
- mask, 82, 121
- multi-protocol encapsulation, 107

N

- names and passwords example, 46
- NetBEUI packets, 91
- Network address translation
 - general, 95
- Network Address Translation
 - enable, 64

- network diagrams, 26
- network information
 - example, 43, 50
 - sample worksheets, 43, 50
- network protocol configuration
 - Bridging (with PPP), 22
 - IP (with PPP), 15
 - IP (with RFC 1483MER), 30
 - IPX (with PPP), 19

P

- PAP, 15, 19, 22, 89, 90
- password
 - change login, 58
 - CHAP, 90
 - example, 46
 - PAP, 89
 - usage, 15, 19, 22
- passwords and names example, 46
- piggyback method
 - IP Routing, 93
- Point-to-Point Protocol
 - standard, 88
 - support for, 88

R

- reboot, 69
- Reboot from Network, 84
- remote router
 - authentication password, 62
 - bridging, 63
 - definition, 12
 - WAN IP addresses, 65
- remote router database, 59
 - add, delete, modify, enable, disable entry, 59
 - definition, 11
- remote WAN IP address, 65
- reset configuration files, 83
- resetting router's defaults, 83
- restoring files, 82
- RFC 1483, 89
- RFC 1483MER, 30, 89
- RIP
 - general, 78
 - IP Routing, 92

- LAN RIP settings, 79
- packets, 78, 91, 107
- WAN RIP settings, 65, 79
- router names
 - usage, 15, 19, 22
- routing
 - general description, 90

S

- sample configuration, 41
- SAP packets, 92
- SDSL, 89
- secret
 - CHAP, 90
- security
 - changing login password, 58
 - Internet firewall, 68
 - Internet Firewall, 93
 - login password, 54
 - remote router authentication
 - protocol, 62
 - remote router password, 62
- Security
 - CHAP, 90
 - PAP, 89
- serialization frames
 - spoofing, 93
- SNMP
 - features, 94
- SNMP MIB
 - databases, 94
- SNMP options, 85
- software level, 54
- software specifications, 107
- software updates, 95
- source WAN IP address, 65
- Spanning Tree Protocol, 92
- spoofing
 - IP Routing, 92
- subnetwork tables, 121
- system message, 54, 56
- system name, 54, 56

T

- target system settings, 55
- TCP/IP Routes, 63

- TCP/IP routing
 - control, 46, 51
- TCP/IP Routing
 - configuration parameters, 16, 24, 31
 - control, 68
 - default route, 17, 25, 31
 - filtering and spoofing, 92
 - protocol options, 78
 - route addresses, 17, 25, 31, 63
 - source and remote addresses, 17, 25, 31
 - stack requirements, 96
 - testing, 70
 - WAN IP addresses, 65
- Technical Support, 105
- TELNET, 95
- terminal emulation
 - communications settings, 118
 - establishing session, 118
- Terminal Window
 - access, 80
 - management tool, 80
- TFTP, 82, 95
- tools, 80
- troubleshooting
 - accessing the remote network, 103
 - console, 101
 - diagnosis tools, 98

- hardware, 97
- hardware configuration, 102
- Help file, 99
- history log, 99
- login password, 103
- PC connection, 102
- power light off, 97
- software configuration, 102
- terminal window display, 101
- using LEDs, 97

U

- upgrade tool, 82
- upgrading files, 82

V

- VPI/VCI numbers, 16, 19, 22, 24, 27, 29, 30, 127, 130

W

- WAN RIP settings, 65
- WAN-to-WAN forwarding, 69
- watchdog frames
 - spoofing, 93

