FlowPoint™

FlowPoint™ DSL Router Family

Command Line Interface

Second Edition (May, 1998)

Copyright

FlowPoint provides this publication “as is” without warranty of any kind, either expressed 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
Web site: www.flowpoint.com

Preface

About This Book

The *Command Line Interface* contains information on the syntax and use of the Command Line Interface for the family of DSL routers. It provides the steps and information needed to configure the Router software and troubleshoot problems using the Command Line Interface. Configuration of network connections, bridging, routing, and security features are essentially the same for all DSL routers (ADSL, ATM, SDSL, etc.), unless otherwise noted. The book also provides detailed information about the system's bridging, routing, addressing, and security operation.

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

How This Book Is Organized

This guide is intended to help you configure and manage the router using the Command Line Interface. The guide assumes that you have read the information about the router and installed the hardware using the *Internet Quick Start Guide*. The guide is divided into eight parts:

Introduction

Describes the features of the Command Line Interface.

Advanced Topics

Contains additional information on topics such as interoperability, routing and bridging operation, PAP/CHAP security negotiation, bandwidth management, protocol conformance, and the file system.

Planning for Router Configuration

Provides information unique to configuration using the Command Line Interface including tables for collecting required information.

Configuring Router Software

Describes how to configure the router using the Command Line Interface.

Configuring Special Features

Describes how to configure features such as IP Firewall, DHCP, NAT, and Management Security.

Command Line Interface Reference

Describes the syntax of each command and the results when the command is entered.

Managing the Router

Describes SNMP management capabilities, TELNET support and how to upgrade the system software, backup and restore configuration files, and recover FLASH memory.

Troubleshooting

Describes diagnostic tools used for identifying and correcting hardware and software problems.

Reference

User Guide
Contains an overview of the Router's software and hardware features and details on hardware installation and software configuration using the Windows-based Configuration Manager.

Internet Quick Start Guide
Describes the configuration process involved in setting up a Virtual Circuit connection to a Network Service Provider for s specific router model.

Typographic Conventions

The following figure summarizes the conventions used in this guide:

Item	Type Face	Example
Words defined in glossary, book titles, figure captions, command reference parameters.	Italics	Refer to *Installing the Hardware* system name *name*
Keywords in command reference instructions	Bold	Example: **save**
Examples showing you what to type and what is displayed on the terminal.	Mono-spaced font	Enter the following command: `remote setProtocol PPP rm1`
File names	Upper case	Copy file CFGMGR.EXE

Table of Contents

Preface **3**

Introduction **9**

Chapter 1. Advanced Topics **11**
- Interoperability 11
  - Routing 11
  - Bridging 12
- Bridging And Routing Operation 13
  - Bridging and Routing Configuration Settings 13
- Point-To-Point Protocol (PPP) 14
- PAP/CHAP Security Authentication 14
  - General Security Authentication Information 15
  - Security Configuration Settings 15
  - Authentication Process 16
- Protocol Conformance 17
  - Protocol Standards 17
  - IP Routing 17
  - IPX Routing 18
- Encapsulation Options 18
  - PPP 18
  - PPPLLC 18
  - RFC 1483 or RFC 1490 19
  - MAC Encapsulated Routing: RFC 1483MER (ATM) or RFC 1490MER (Frame Relay) 19
  - FRF8 19
  - rawIP 20
- System Files 20
- Advanced Command Line Interface Features 21
  - Bridging Filtering 21
  - Unique System Passwords 21

Chapter 2. Planning For Router Configuration **23**
- Important Terminology 23
- Collect Your Configuration Information 24
  - PPP Link Protocol (over ATM or Frame Relay) 26
  - RFC 1483 / RFC 1490 Link Protocols 31
  - MAC Encapsulated Routing: RFC 1483MER / RFC 1490MER Link Protocols 35
  - FRF8 Link Protocol 37

Chapter 3. Configuring Router Software **39**
- Configuration Tables 40
  - Configuring PPP with IP Routing 41
  - Configuring PPP with IPX Routing 42
  - Configuring PPP with Bridging 43
  - Configuring RFC 1483 / RFC 1490 with IP Routing 44
  - Configuring RFC 1483 / RFC 1490 with IPX Routing 45
  - Configuring RFC 1483 / RFC 1490 with Bridging 46
  - Configuring MAC Encapsulated Routing: RFC 1483MER / RFC 1490MER with IP Routing 47
  - Configuring FRF8 with IP Routing 48
  - Mixed Network Protocols Configuration 49
- Verify The Router Configuration 49
  - Test IP Routing 49
  - Test Bridging to a Remote Destination 50
  - Test IPX Routing 50
- Sample Configurations 51
  - Sample Configuration 1 — PPP with IP and IPX 51
  - Sample Configuration 2 — RFC 1483 with IP and Bridging 59

Chapter 4. Configuring Special Features **65**
- IP Firewall Bridging Filtering 65

Enable/Disable Internet Firewall Filtering 65
Configure Bridging Filtering 65
DHCP (Dynamic Host Configuration Protocol) 66
General Information 66
Manipulating Subnetworks and Explicit Client Leases 67
Setting Option Values 70
BootP 72
Defining Option Types 73
Other Information 74
NAT (Network Address Translation) 75
General NAT Rules 75
Masquerading (one single NAT IP address shared by many PC IP addresses) 75
Classic NAT (one NAT IP address assigned per one PC IP address) 78
Management Security 80
Disable Telnet and SNMP 80
Restore Telnet and SNMP 80
Validation of Telnet and SNMP clients 80
Restrict Remote Access 81
Changing the SNMP Community Name 81
Disable WAN Management 81

Chapter 5. Command Line Interface Reference 82
Command Line Interface Conventions 82
Command Input 82
Command Output 82
Command Organization 82
? or HELP 83
System Level Commands 84
Router Configuration Commands 91
Target Router System Configuration Commands (SYSTEM) 91
Target Router Ethernet LAN Bridging and Routing (ETH) 100
Remote Router Access Configuration (REMOTE) 106
Asymmetric Digital Subscriber Line Commands (ADSL) 121
Asynchronous Transfer Mode Commands (ATM) 123
High-Speed Digital Subscriber Line Commands (HDSL) 125
ISDN Digital Subscriber Line (IDSL) 128
Symmetric Digital Subscriber Line Commands (SDSL) 130
Dynamic Host Configuration Protocol Commands (DHCP) 133
Bridging Filtering Commands (FILTER BR) 143
Save Configuration Commands (SAVE) 145
Erase Configuration Commands (ERASE) 147
File System Commands 149

Chapter 6. Managing The Router 153
Simple Network Management Protocol (SNMP) 153
TELNET Remote Access 153
Client TFTP Facility 154
Software Boot Options 154
Manual Boot Mode 154
Booting from the Network 155
Other Manual Boot Options 157
Software Kernel Upgrades 158
Booting and Upgrading from the LAN 158
Upgrading from the WAN Line 159
Backup And Restore Configuration Files 160
FLASH Memory Recovery Procedures 160
Batch File Command Execution 161

Chapter 7. Troubleshooting 164
Diagnostic Tools 164

Using LEDs 164
History Log 165
Ping Command 166
Investigating Hardware Installation Problems 167
Check the LEDs to Solve Common Hardware Problems 167
Problems with the Terminal Window Display 167
Problems with the Factory Configuration 167
Investigating Software Configuration Problems 167
Problems Connecting to the Router 167
Problems with the Login Password 168
Problems Accessing the Remote Network 168
Problems Accessing the Router via TELNET 170
Problems Downloading Software 170
System Messages 171
Time-Stamped Messages 171
History Log 174
How To Obtain Technical Support 175

Appendix A. Network Information Worksheets 176
Configuring PPP with IP Routing 177
Configuring PPP with IPX Routing 178
Configuring PPP with Bridging 179
Configuring RFC 1483 / RFC 1490 with IP Routing 180
Configuring RFC 1483 / RFC 1490 with IPX Routing 181
Configuring RFC 1483 / RFC 1490 with Bridging 182
Configuring RFC 1483MER / RFC 1490MER with IP Routing 183
Configuring FRF8 with IP Routing 184

Appendix B. Configuring IPX Routing 185
IPX Routing Concepts 185
Configure IPX Routing 185
Step 1: Collect Your Network Information for the Target (Local) Router 186
Step 2: Review Your Settings 187

Index 188

Introduction

This guide provides steps and information needed to configure the DSL Router software, using the **Command Line Interface**[1].

It covers the following basic configuration topics:

- Setting of names, passwords PVC numbers, and link and network parameters
- Configuration of specific details within a protocol, such as IP or IPX addresses and IP protocol controls
- Activation of bridging and routing protocols
- Enabling of the Internet Firewall filter with IP routing

The Command Line Interface also provides the following advanced features:

- Manage the router's file system
- Set bridging filters
- Configure the type of DSL technology specific to your router (ADSL, SDSL, etc.)
- Issue online status commands
- Monitor error messages
- Set RIP options
- Configure DHCP
- Configure NAT

Command Line Interface Access

You can access the Command Line Interface from:

- A terminal session running under Windows (for local access)
- The terminal window from the Configuration Manager (for local access) (see note 2)
- An ASCII terminal (for local access)
- A TELNET session (for remote access)

NOTE 1: For local access, the PC or ASCII terminal is connected to the **Console** port. This connection and the required communications settings are thoroughly described in the *User Guide*, Appendix D, *Accessing the Command Line Interface*.

NOTE 2: If you wish to access the terminal window from within the Configuration Manager, click **Tools** and **Terminal Window** from the main menu. The menu selection Commands provides shortcuts to most of the commands described in this manual. These shortcuts will substantially reduce the amount of typing.

[1] The Microsoft® Windows™-based **Configuration Manager** (featuring an easy-to-use, point-and-click GUI interface) provides another way to configure the router's software. Please refer to the *User Guide* if you intend to use the Configuration Manager as your primary configuration tool.

Chapter 1. Advanced Topics

This chapter provides information on advanced topics useful to network administrators. Refer to the *User Guide* for a general overview of the router basic features.

Interoperability

The router uses industry-wide standards to ensure compatibility with routers and equipment from other vendors. To interoperate, the router supports standard protocols on the physical level, data link level for frame type or encapsulation method, and network level. For two systems to communicate directly, they must use the same protocol at each level. Most protocols do not support negotiable options, except for PPP.

The physical protocol level includes hardware and electrical signaling characteristics. This support is provided by the router Ethernet and modem hardware interfaces.

The data link protocol level defines the transmission of data packets between two systems over the LAN or WAN physical link.

The frame type or encapsulation method defines a way to run multiple network-level protocols over a single LAN or WAN link. The router supports the following WAN encapsulations:

- PPP (VC multiplexing)
- PPP (LLC multiplexing)
- RFC 1483 (for ATM)
- RFC 1483 with MAC Encapsulation Routing (for ATM)
- FRF8 (for ATM)
- RFC 1490 (for Frame Relay)
- RFC 1490 with MAC Encapsulated Routing (for Frame Relay)

Routing

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

The routing tables can be seeded; i.e., addresses for remote destinations are placed in the table along with path details and the associated costs (path latency).

The 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. It also provides security by isolating traffic on segmented LAN. Routing extends the reach of networks beyond the limits of each LAN segment.

Numerous network protocols have evolved and within each protocol are associated protocols for routing, error handling, network management, etc. The following chart displays the networking and associated protocols supported by the router.

Network Protocol	Associated Protocol	Description
Internet Protocol (IP)	Routing Information Protocol (RIP)	Protocol used to maintain a map of the network
	Address Resolution Protocol (ARP)	Maps IP addresses to datalink addresses
	Reverse Address Resolution Protocol (RARP)*	Maps data link addresses to IP addresses
	Internetwork Control Message Protocol (ICMP)	Diagnostic and error reporting/recovery
	Simple Network Management Protocol (SNMP)	Network Management
Internet Packet Exchange (IPX)	Routing Information Protocol (RIP)**	Protocol used to maintain a map of the network
	Service Advertising Protocol (SAP)	Distributes information about service names and addresses

* Used only during a network boot
** IPX-RIP is a different protocol from IP-RIP and includes time delays

Most of the router's operation on each protocol level is transparent to the user. Some functions are influenced by configuration parameters and these are described in greater details in the following sections.

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 NETBIOS) 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.

The router bridging support includes the IEEE 802.1D standard for LAN-to-LAN bridging and the Spanning Tree Protocol for interoperability with other vendor's bridge/routers. Bridging is provided over PPP as well as adjacent LAN ports.

Most of the router's bridging operation is transparent. Some functions are influenced by configuration parameters and these are described in greater detail in the following sections.

Bridging And Routing Operation

The 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 enabled for routing (IP or IPX).
- The router will operate as a bridge for protocols that are not supported for routing.
- Routing takes precedence over bridging; i.e., when routing is active, 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 forward the packet.

Operation of the 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. For example, general IP or IPX routing, and routing or bridging from 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.

Bridging and Routing Configuration Settings

The router can be configured to perform general routing and bridging while allowing you to set specific controls.

One remote router is designated as the outbound default bridging destination. All outbound bridging traffic, with an unknown destination, is sent to the default bridging destination. Bridging from specific remote routers can be controlled by enabling/disabling bridging from individual remote routers.

Routing is performed to all remote routers entered into the remote router database. All routing can be enabled/disabled with a system-wide control.

The following charts describe the operational characteristics of the router, based on configuration settings.

IP/IPX Routing ON **Bridging To/From Remote Router OFF**

Data Packets Carried	IP (TCP, UDP), IPX
Operational Characteristics	Basic IP, IPX connectivity
Typical Usage	When only IP/IPX traffic is to be routed and all other traffic is to be ignored. For IP, used for Internet access. **Note:** This is the most easily controlled configuration.

IP/IPX Routing ON **Bridging To/From Remote Router ON**

Data Packets Carried	IP/IPX routed; all other packets bridged
Operational Characteristics	IP/IPX routing and allows other protocols, such as NetBEUI (that can't be routed), to be bridged.
Typical Usage	When only IP/IPX traffic is to be routed but some non-routed protocol is required. Used for client/server configurations.

IP/IPX Routing OFF **Bridging To/From Remote Router ON**

Data Packets Carried	All packets bridged
Operational Characteristics	Allows protocols, such as NetBEUI (that can't be routed) to be bridged.
Typical Usage	Peer-to-peer bridging and when the remote end supports only bridging.

Point-To-Point Protocol (PPP)

PPP is an industry standard WAN protocol for transporting multi-protocol datagrams over point-to-point connections. PPP defines a set of protocols, such as security and network protocols, that can be negotiated over the connection. PPP includes the following protocols:

- Link Control Protocol (LCP) to negotiate PPP; i.e., establish, configure and test the datalink connection.
- Network Control Protocols (NCPs), such as:
  TCP/IP routing Internet Protocol Control Protocol (IPCP)
  IPX routing Control Protocol (IPXCP)
  Bridge Control Protocol (BNCP)
- Security Protocols including PAP and CHAP

For a more detailed description of the router's implementation of some of these protocols, please read the following section. A list of PPP protocol conformance is included in the section *Protocol Conformance*.

PAP/CHAP Security Authentication

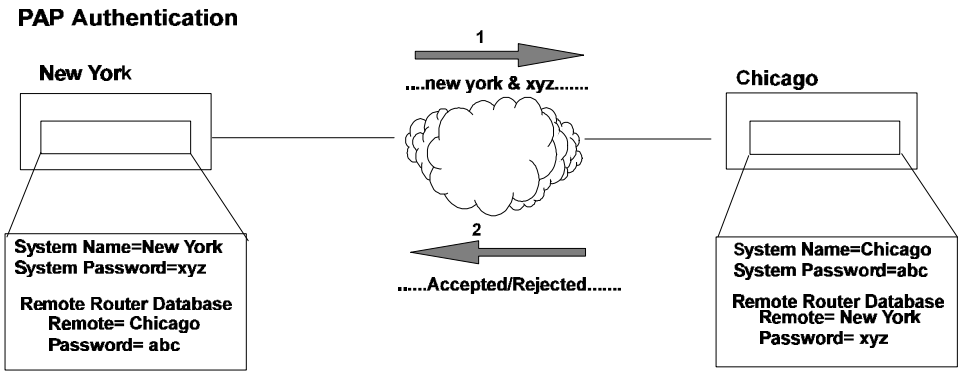
Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) under PPP are supported by the router. However, security authentication may or may not be needed depending on the requirements of the remote end.

The nature of the connection in a DSL environment (traffic occurs on a dedicated line/virtual circuit) does not require authentication unless specifically required by the remote end, the ISP, or the NSP. When not required, security is disabled with the command `remote disauthen`.

General Security Authentication Information

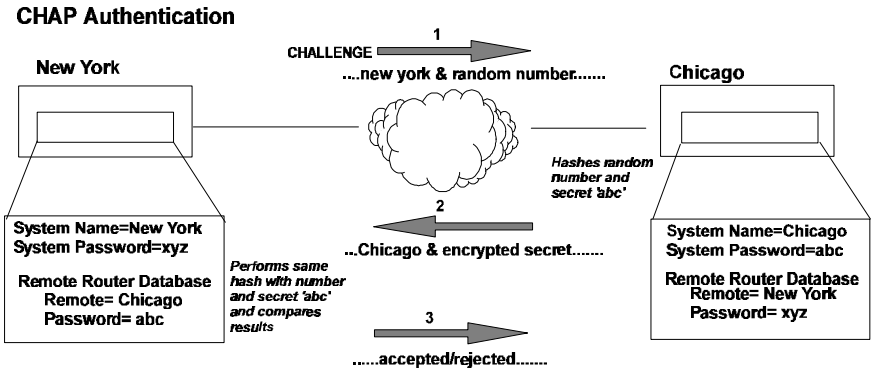
Security authentication may be required by the remote end. The following information describes how authentication occurs.

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 the system name. The peer then applies a one-way hash algorithm to the random number and returns this encrypted information along with the 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.



Security Configuration Settings

The router has one default system password used to access any remote router. This 'system authentication password' is utilized by remote sites to authenticate the local site. The router also allows you to assign a unique 'system override password' used only when connecting to a specific remote router for authentication by that remote site. Each remote router entered in the remote router database has a password used when the remote site

attempts to gain access to the local router. This ‘remote authentication password’ is utilized by the router to authenticate the remote site.

Each remote router entered in the remote router database also has a minimum security level, known as the ‘remote authentication protocol’, that must be negotiated before the remote router gains access to the local router. In addition, a system-wide control, ‘system authentication protocol’, is available for overriding the minimum security level in the entire remote router database.

Authentication Process

The authentication process occurs regardless of whether a remote router connects to the local router or vice versa, and even if the remote end does not request authentication. It is a bi-directional process, where each end can authenticate the other using the protocol of its choice (provided the other end supports it).

During link negotiation (LCP), each side of the link negotiates what protocol is to be used for authentication during the connection. If both the system and the remote router have PAP authentication, then PAP authentication is negotiated.

Otherwise, the router *always* requests CHAP authentication first; if refused, PAP will be negotiated. If the remote end does not accept either PAP or CHAP, the link is dropped; i.e., the router does not communicate without a minimum security level. On the other hand, the router will accept any authentication scheme required by the remote node, including no authentication at all.

During the authentication phase, each side of the link can request authentication using the method they negotiated during LCP.

For CHAP, the router issues a CHAP challenge request to the remote side. The challenge includes the system name and random number. The remote end, using a hash algorithm associated with CHAP, transforms the name and number into a response value. When the remote end returns the challenge response, the router can validate the response challenge value using the entry in the remote router database. If the response is invalid, the call is disconnected. If the other end negotiated CHAP, the remote end can, similarly, request authentication from the router. The router uses its system name and secret to respond to CHAP challenge.

For PAP, when a PAP login request is received from the remote end, the router checks the remote router PAP security using the remote router database. If the remote router is not in the remote router database or the remote router password is invalid, the call is disconnected. If the router and password are valid, the router acknowledges the PAP login request.

If PAP was negotiated by the remote end for the remote-side authentication, the router will issue PAP login requests *only* if it knows the identity of the remote end. The identity is known if the call was initiated from the router or the remote end returned a successful CHAP challenge response. For security reasons, the router will *never* identify itself using PAP without first knowing the identity of the remote router.

If PAP was negotiated by the remote end for the local side of the authentication process and the minimum security level is CHAP, as configured in the remote router database, the link is dropped for a security violation.

Protocol Conformance

Protocol Standards

The router conforms to RFCs designed to address performance, authentication, and multi-protocol encapsulation. The following RFCs are supported:

- RFC 1058 Routing Information Protocol (RIP)
- RFC 1144 Compressing TCP/IP headers (Van Jacobson)
- RFC 1220 Bridging Control Protocol (BNCP)
- RFC 1332 IP Control Protocol (IPCP)
- RFC 1334 Password Authentication Protocol & Challenge Handshake Authentication Protocol (PAP/CHAP)
- RFC 1483 Multiprotocol Encapsulation over ATM Adaptation Layer 5
- RFC 1490 Multiprotocol Interconnect over Frame Relay
- RFC 1552 Novell IPX Control Protocol (IPXCP)
- RFC 1661 Point-to-Point Protocol (PPP)
- RFC 1577 Classical IP and ARP over ATM
- RFC 1723 RIP Version 2
- RFC 1962 PPP Compression Control Protocol (CCP)
- RFC 1973 PPP in Frame Relay
- RFC 1974 Stac LZS compression protocol
- RFC 1990 Multi-Link Protocol (MLP)
- RFC 2131 and 2132 Dynamic Host Configuration Protocol (DHCP)

IP Routing

IP routing support, in conformance with RFC 791, provides the ability to process TCP/IP frames at the network layer for routing. IP routing support includes the Routing Interface Protocol (RIP), in conformance with RFC 1058 (RIP v.1) and RFC 1723 (RIP v.2).

IPX Routing

IPX routing conforms to the Novell® NetWare™ IPX Router Development Guide, Version 1.10.

Encapsulation Options

This section describes in technical terms the format of each packet associated with a particular encapsulation option supported by the FlowPoint router.

The encapsulation type for each remote entry is defined using the `remote setprotocol` command.

PPP

Each packet begins with a one or two-byte protocol ID. Typical IDs are:

0xc021 -- LCP

0x8021 -- IPCP

0x0021 -- IP

0x002d -- Van Jacobson compressed TCP/IP

0x002f -- Van Jacobson uncompressed TCP/IP

0x8031 -- Bridge NCP

0x0031 -- Bridge Frame

The command for this encapsulation option is:

```
remote setprotocol PPP <remoteName>
```

Note: With PPP over ATM, the address and control fields (i.e. FF03 are never present, including in LCP packets).

PPPLLC

This protocol (LLC-multiplexed) allows PPP traffic to be carried simultaneously with other traffic on a single virtual circuit (as opposed to the PPP method of encapsulation – VC multiplexing - which dedicates a virtual circuit to PPP traffic only).

Each PPP packet is prepended with the sequence 0xFEFE03CF. Thus, a LCP packet has the format: 0xFEFE03CF 0xC021.

The command for this encapsulation option is:

```
remote setprotocol PPPLLC <remoteName>
```

RFC 1483 or RFC 1490

Bridging

User data packets are prepended by the sequence 0xAAAA0300 0x80c20007 0x0000 followed by the Ethernet frame containing the packet.

802.1D Spanning Tree packets are prepended with the header 0xAAAA0300 0x80C2000E.

Routing

IP packets are prepended with the header 0xAAAA0300 0x00000800.
IPX packets are prepended with the header 0xAAAA0300 0x00008137.

The commands for this encapsulation option are:

`remote setprotocol rfc1483 <remoteName>` (for ATM)

`remote setprotocol FR <remoteName>` (for Frame Relay)

MAC Encapsulated Routing: RFC 1483MER (ATM) or RFC 1490MER (Frame Relay)

MER encapsulation allows IP packets to be carried as bridged frames, but does not prevent bridged frames from being sent as well, in their normal encapsulation format: RFC 1483 (ATM) or RFC 1490 (Frame Relay).

If IP routing is enabled, then IP packets are prepended with the sequence 0xAAAA0300 0x80c20007 0x0000 and sent as bridged frames. If IP routing is not enabled, then the packets appear as bridged frames (see below).

The commands for this encapsulation option are:

`remote setprotocol rfc1483MER <remoteName>` (for ATM)

`remote setprotocol MER` (for Frame Relay)

FRF8

IP Packets have prepended to them the following sequence 0x03CC.

The command for this encapsulation option is:

`remote setprotocol frf8 <remoteName>`

rawIP

IP packets do not have any protocol headers prepended to them; they appear as IP packets on the wire. Only IP packets can be transported since there is no possible method to discriminate other types of packets (bridged frames or IPX).

The command for this encapsulation option is:

```
remote setprotocol rawIP <remoteName>
```

System Files

The router's file system is a DOS-compatible file system. The following list describes the contents of the file system:

- **SYSTEM.CNF**
  Configuration files containing:

  DOD Remote Router Database
  SYS System Settings: name, message, authentication method, and passwords
  ETH Ethernet LAN Configuration settings

- **DHCP.DAT**
  DHCP files

- **FILTER.DAT**
  Bridge filters

- **KERNEL.F2K**
  Router system software (KERNEL.FP1 for IDSL routers)

- **ETH.DEF**
  File used by the manufacturer to set a default Ethernet configuration

- **ASIC.AIC**
  Firmware for the xDSL modem or ATM interface

- **ATM.DAT**
  ATM configuration file

Any file contained within the system may be retrieved or replaced using the TFTP protocol. Specifically, configuration files and the operating system upgrades can be updated. Only one copy for the router software is allowed in the router's FLASH memory.

Refer to Chapter 5. *Managing the Router* or the *User Guide* for details on software upgrades, booting router software, copying configuration files, and restoring router software to FLASH.

Advanced Command Line Interface Features

Bridging Filtering

You can control the flow of packets across the router using bridging filtering. Bridging filtering lets you 'deny' or 'allow' packets to cross the network based on position and hexadecimal content within the packet. This enables you to restrict or forward messages with a specified address, protocol, or data content. Common uses are to prevent access to remote networks, control unauthorized access to the local network, and limit unnecessary traffic.

For example, it might be necessary to restrict remote access for specific users on the local network. In this case, bridging filters are defined using the local MAC address for each user to be restricted. Each bridging filter is specified as a 'deny' filter based on the MAC address and position of the address within the packet. Deny filtering mode is then enabled to initiate bridge filtering. Every packet with one of the MAC addresses would not be bridged across the router until the deny filtering mode was disabled.

Similarly, protocol filtering can be used to prevent a specific protocol from being bridged. In this case, the protocol ID field in a packet is used to deny or allow a packet. You can also restrict, for example, the bridging of specific broadcast packets.

Unique System Passwords

As described in the section *Security Configuration Settings* of this chapter, you can specify a unique system override password for a remote router with the command `remote setOurPasswd`. This 'system override password' is used instead of the general system password *only* when connecting to a specific remote router. This allows you to set a unique CHAP or PAP authentication password for authentication of the local site by the remote site *only* when the router connects to that remote site.

A common use would be to set a password assigned to you by Internet Service Providers (ISPs). Similarly, the system name of the local router can be overridden when connecting to a specific remote with the command `remote setoursysname`.

Chapter 2. Planning For Router Configuration

This chapter describes the terminology and the information that you need to collect before configuring the router. The information needed to configure the router is contingent on the chosen Link Protocol. It is therefore important 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.

When configuring the router using the Command Line Interface, planning is similar to the process described for Configuration Manager with very few exceptions.

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.

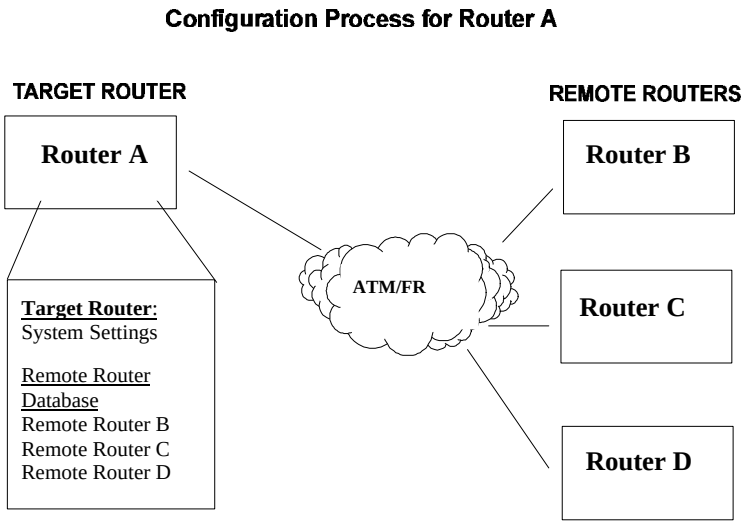
Remote routers
All the routers to which the target (local) router may connect.

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.



Collect Your Configuration Information

This section describes the configuration information associated with each Link Protocol/Network Protocol combination. It is organized as follows:

- PPP Link Protocol with IP, or IPX, or Bridging Network Protocol
- RFC 1483 or RFC 1490 Link Protocol with IP, or IPX, or Bridging Network Protocol
- MAC Encapsulated Routing: RFC 1483MER or RFC 1490MER Link Protocol with IP Network Protocol
- FRF8 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 listing:

   PPP with:

   - IP Routing Network Protocol, page 26.
   - IPX Routing Network Protocol, page 28.
   - Bridging Network Protocol, page 30.

   RFC 1483 or RFC 1490 with:

   - IP Routing Network Protocol, page 31.
   - IPX Routing Network Protocol, page 33.
   - Bridging Network Protocol, page 34.

   MAC Encapsulated Routing: RFC 1483MER or RFC 1490MER with:

   - IP Routing Network Protocol, page 35.

FRF8 Link Protocol with:

- IP Routing Network Protocol, page 37.

3. Collect the information applicable to your Link/Network Protocol association. This information will be used later in conjunction with the *Configuration Tables* for easy configuration of your router based on your Link/Network protocol. These configuration tables provide step-by-step instructions for a basic configuration for each your Link/Network protocol.

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

PPP Link Protocol (over ATM or Frame Relay)

The PPP Link Protocol is an encapsulation method that can be used over ATM (for ATM routers) or Frame Relay (for Frame Relay routers)

Combined with the IP, IPX, or Bridging Network Protocols, PPP over ATM and PPP over Frame Relay share the same configuration characteristics, except for the connection identifiers: VPI/VCI numbers are used for ATM and a DLCI number is used for Frame Relay.

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 the Command Line Interface commands (see *Configuration Tables*, chapter 3).

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. Please refer to the diagram on page 14 to see how this information is used.

NOTE 1: A sample configuration containing Names and Passwords is provided in the section *Sample Configuration, Configuration 1*, in chapter 3.

NOTE 2: If the ISP does not support the authentication of the ISP system by the caller, use the command `remote disauthen <remoteName>` to disable the authentication.

VPI and VCI Numbers (for ATM routers)

Your router may have been preconfigured with VPI/VCI numbers. If not, you will have to obtain these numbers from your Network Service Provider and then configure them.

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

DLCI (for Frame Relay routers)

The DLCI number applies to Frame Relay routers only.

Your Network Service Provider or your Network Access Provider will provide you with a DLCI (Data Link Connection Identifier). The DLCI is an address identifying your connection.

DNS Internet Account Information (optional)

This information is obtained from your Network Service Provider.

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

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

IP Routing Addresses

For the Ethernet Interface

This information is defined by the user or your 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 which cannot exchange routing information between them. This feature is normally not used except in very special circumstances.

For the WAN Interface

This information is defined by the Network Service Provider.

Source (Target/Local) WAN Port Address
If Network Address Translation (NAT) 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.

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. Please refer to the diagram on page 14 to see how this information is used.

NOTE 1: A sample configuration containing Names and Passwords is provided in the section *Sample Configuration, Configuration 1*, chapter 3.

NOTE 2: If the ISP does not support the authentication of the ISP system by the caller, use the command `remote disauthen <remoteName>` to disable the authentication.

VPI and VCI Numbers

Your router may have been preconfigured with VPI/VCI numbers. If not, you will have to obtain these numbers from your Network Service Provider and then configure them.

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

DLCI (for Frame Relay routers)

The DLCI number applies to Frame Relay routers only.

Your Network Service Provider or your Network Access Provider will provide you with a DLCI (Data Link Connection Identifier). The DLCI is an address identifying your connection.

IPX Routing Entries

These numbers are defined by the Network Administrator.

You will need to obtain the following information (most likely from your network administrator) for IPX Routing.

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.

NOTE: Appendix B provides step-by-step information on how to configure IPX routing.

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. Please refer to the diagram on page 14 to see how this information is used.

NOTE 1: A sample configuration containing Names and Passwords is provided in the section *Sample Configuration, Configuration 1*, chapter 3.

NOTE 2: If the ISP does not support the authentication of the ISP system by the caller, use the command `remote disauthen <remoteName>` to disable the authentication.

VPI and VCI Numbers

Your router may have been preconfigured with VPI/VCI numbers. If not, you will have to obtain these numbers from your Network Service Provider and then configure them.

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

DLCI (for Frame Relay routers)

The DLCI number applies to Frame Relay routers only.

Your Network Service Provider or your Network Access Provider will provide you with a DLCI (Data Link Connection Identifier). The DLCI is an address identifying your connection.

DNS Internet Account Information (optional)

This information is obtained from the Network Service Provider.

Consult with you 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 / RFC 1490 Link Protocols

The Link Protocol RFC 1483 is a multiprotocol encapsulation method over ATM and is used by ATM routers. RFC 1490 is a multiprotocol encapsulation method over Frame Relay and is used by Frame Relay routers.

RFC 1483 and RFC 1490 combined with the IP, IPX, or Bridging Network Protocols share the same configuration characteristics, except for the connection identifiers: VPI/VCI numbers are used for RFC 1483 and a DLCI number is used for RFC 1490.

Collect the information as described in the appropriate section. This data will be later used to configure your router using the Command Line Interface (see *Configuration Tables*, chapter 3).

IP Routing Network Protocol

VPI and VCI Numbers (for RFC 1483)

The VPI and VCI numbers apply to ATM routers only.

Your router may have been preconfigured with VPI/VCI numbers. If not, you will have to obtain these numbers from your Network Service Provider and then configure them.

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

DLCI (for RFC 1490)

The DLCI number applies to Frame Relay routers only.

Your Network Service Provider or your Network Access Provider will provide you with a DLCI (Data Link Connection Identifier). The DLCI is an address identifying your connection.

DNS Internet Account Information (optional)

This information is obtained from the Network Service Provider.
Consult with you Network Service Provider to find out if you need to enter the following information:

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

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 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.

IPX Routing Network Protocol

VPI and VCI Numbers (for RFC 1483)

The VPI and VCI numbers apply to ATM routers only.

Your router may have been preconfigured with VPI/VCI numbers. If not, you will have to obtain these numbers from your Network Service Provider and then configure them.

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

DLCI (for RFC 1490)

The DLCI number applies to Frame Relay routers only.

Your Network Service Provider or your Network Access Provider will provide you with a DLCI (Data Link Connection Identifier). The DLCI is an address identifying your connection.

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: 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 (with RFC 1483)

The VPI and VCI numbers apply to ATM routers only.

Your router may have been preconfigured with VPI/VCI numbers. If not, you will have to obtain these numbers from your Network Service Provider and then configure them.

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

DLCI (with RFC 1490)

The DLCI number applies to Frame Relay routers only.

Your Network Service Provider or your Network Access Provider will provide you with a DLCI (Data Link Connection Identifier). The DLCI is an address identifying your connection.

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

MAC Encapsulated Routing: RFC 1483MER / RFC 1490MER Link Protocols

MAC Encapsulated Routing (MER) allows IP packets to be carried as bridged frames (bridged format). The Link Protocol RFC 1483 with MER (referred to as RFC 1483MER) is a multiprotocol encapsulation method over ATM used by ATM routers. RFC 1490 with MER (referred to as RFC 1490MER) is a multiprotocol encapsulation method over Frame Relay used by Frame Relay routers.

RFC 1483MER and RFC 1490MER combined with the IP, IPX, or Bridging Network Protocols share the same configuration characteristics, except for the connection identifiers: VPI/VCI numbers are used for RFC 1483MER and a DLCI number is used for RFC 1490.

Collect the information as described in the appropriate section. This data will be later used to configure your router using the Command Line Interface (see *Configuration Tables*, chapter 3).

IP Routing Network Protocol

VPI and VCI Numbers (for RFC 1483MER)

The VPI and VCI numbers apply to ATM routers only.

Your router may have been preconfigured with VPI/VCI numbers. If not, you will have to obtain these numbers from your Network Service Provider and then configure them.

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

DLCI (for RFC 1490MER)

The DLCI number applies to Frame Relay routers only.

Your Network Service Provider or your Network Access Provider will provide you with a DLCI (Data Link Connection Identifier). The DLCI is an address identifying your connection.

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 ATM 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 RFC1483MER or RFC 1490MER, 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.

FRF8 Link Protocol

The FRF8 Link Protocol is an encapsulation method, which allows an ATM router to interoperate with a Frame Relay network.

FRF8 is only used in conjunction with the IP Network Protocol. Collect the information described below. This data will be later used to configure your router using the Command Line Interface (see *Configuration Tables*, chapter 3).

IP Routing Network Protocol

VPI and VCI Numbers

Your router may have been preconfigured with VPI/VCI numbers. If not, you will have to obtain these numbers from your Network Service Provider and then configure them.

If you are connecting to multiple remote sites, you will need to obtain additional VPI and VCI numbers from your Network Service Provider and/or Network Access 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 ATM 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 FRF8, the IP route includes an IP address, subnet mask, metric (a number representing the perceived cost in reaching the remote network or station. 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.

Chapter 3. Configuring Router Software

This chapter covers the following configuration topics:

Configuration Tables

Configuration commands are outlined for each Link Protocol/Network Protocol supported by the router. The information needed to configure the router is contingent on the chosen Link Protocol. It is therefore important 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.

Verify the Router Configuration

This section describes how to test IP, IPX, or Bridging.

Sample Configurations

This chapter provides two configuration examples with diagrams, commands, and list outputs.

Note 1: For usage conventions and a complete description of the commands mentioned in this chapter, refer to Chapter 4, *Command Line Interface Reference*.

Note 2: Command Line Interface

To configure the router software, the Command Line Interface is available to you at all times after you have installed the router hardware, connected a PC with a terminal emulation session (or ASCII terminal), and powered the unit on. This chapter assumes that you have successfully installed the router hardware as described in the User Guide.

If you intend to use the Command Line Interface through the Configuration Manager, it is assumed that you have installed the Configuration Manager software and can access the terminal window (refer to the *User Guide*, chapter 2, *Installing and Accessing the Configuration Manager*).

Note 3: Network Information Worksheets

Worksheets are provided in Appendix A so that you can enter details about your target router and remote routers. The worksheets list the commands associated with setting the features.

To configure the **target router**, you need to fill out one Target Router chart for the target router and one Remote Router chart for each remote router to be entered into the remote router database.

If you are setting up both ends of the network, you will need a mirror image of the information listed below for configuring the router on the other end of the ATM or ADSL link.

Important — Changing any the of the following settings requires a “reboot and save” of the router to take effect:

Ethernet LAN: Ethernet IP or IPX Address, TCP/IP Routing, IPX Routing

Bridging: Bridging, Filters

Remote Router: TCP/IP Route Addresses, IPX Routes, IPX SAPs and Bridging control, enable, disable or add remote routers

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
- PPP Link Protocol with IPX Routing Network Protocol
- PPP Link Protocol with Bridging Network Protocol
- RFC 1483/RFC 1490 Link Protocols with IP Routing Network Protocol
- RFC 1483/RFC 1490 Link Protocols with IPX Routing Network Protocol
- RFC 1483/RFC 1490 Link Protocols with Bridging Network Protocol
- RFC 1483MER/RFC 1490MER Link Protocols with IP Network Protocol
- FRF8 Link Protocol with IP Routing Network Protocol
- Combinations of two or more of the preceding Link Protocols/Network Protocols

NOTE: Blank Network Configuration Worksheets are available in Appendix A.

How to use the tables

1. Find the configuration table that fits your particular Network Protocol/Link Protocol association. These tables are designed to provide easy step-by-step instructions.

2. Use the blank Network Configuration Worksheets provided at the end of the chapter to enter the commands in the order that they are given in the Configuration tables' ***commands*** column.

3. You may want to refer to the sample configurations at the end of the chapter.

Configuring PPP with IP Routing

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

PPP with IP Routing		
STEPS	**SETTINGS**	**COMMANDS**
System Settings		
System Name	Required	system name <name>
System Message	Optional	system msg <message>
Authentication Password	Required	system passwd <password>
Ethernet IP Address	As required	eth ip addr <ipAddr> <ipNetMask>
DHCP Settings	Already enabled; additional settings may be required	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver <IpAddr>
Change Login	Optional	system admin <password>
Remote Routers		
New Entry	Enter: Remote Name	remote add <remoteName>
Link Protocol/PVC* (for ATM routers)	Select: PPP Enter: VPI/VCI numbers	remote setProtocol PPP <remoteName> remote setPVC <vpi number>*<vci number> <remoteName>
Link Protocol/DLCI** (for Frame Relay routers)	Select: PPP Enter: DLCI number	remote setProtocol PPP <remoteName> remote setDLCI <number> <remoteName>
Security *** Remote's Password	Choose security level Enter: password	remote setAuthen <protocol> <remoteName> remote setPasswd <passwd> <remoteName>
Bridging On/Off	Must be OFF	remote disBridge <remoteName>
TCP/IP Route Address	Enter: Explicit or default route	remote addiproute <ipNet> <ipNetMask> <hops> <remoteName>
If NAT is enabled:	To enable NAT, use: Enter: You may need to enter a Source WAN Port Address	remote setIpTranslate on <remoteName> remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>
If NAT is not enabled:	Enter: You may need to enter a Source WAN Port Address	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Must be enabled (Optional)	eth ip enable eth firewall < on | off>
IPX Routing	Must be disabled	eth ipx disable
Store **Reboot**		save reboot

* Enter this information if you are using PPP in an ATM environment.
** Enter this information if you are using PPP in a Frame Relay environment.
*** If the ISP does not support the authentication of the ISP system by the caller, use the command `remote disauthen <remoteName>` to disable the authentication.

Configuring PPP with IPX Routing

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

NOTE: Appendix B provides step-by-step information on how to configure IPX routing.

PPP with IPX Routing		
STEPS	**SETTINGS**	**COMMANDS**
System Settings		
System Name	Required	system name <name>
System Message	Optional	system msg <message>
Authentication Password	Required	system passwd <password>
Ethernet IP Address	As required	eth ip addr <ipAddr> <ipNetMask>
DHCP Settings	Already enabled; addit. settings may be required	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver < IpAddr >
Change Login	Optional	system admin <password>
Ethernet IPX Network #	Enter: IPX Network #	eth ipx addr <ipxNet#>
	Frame Type (default: 802.2)	eth ipx frame <type>
Remote Routers		
New Entry	Enter: Remote Name	remote add <remoteName>
Link Protocol/PVC* (for ATM routers)	Select: PPP Enter: VPI/VCI numbers	remote setProtocol PPP <remoteName> remote setPVC <vpi number>*<vci number> <remoteName>
Link Protocol/DLCI** (for Frame Relay routers)	Select: PPP Enter: DLCI number	remote setProtocol PPP <remoteName> remote setDLCI <number> <remoteName>
Security *** Remote's Password	Choose security level Enter: Password	remote setAuthen <protocol> <remoteName> remote setPasswd <passwd> <remoteName>
Bridging On/Off	Must be OFF	remote disBridge <remoteName>
IPX Routes Add	Enter appropriate info	remote addIpxroute <ipxNet> <metrics> <ticks> <remoteName>
IPX SAPs Add	Enter appropriate info	remote addIpxsap <service_name> <ipxNet> < ipxNode> <socket> <type> <hops> <remoteName>
WAN Network #	Enter appropriate info	remote setIpxaddr <ipxNet> <remoteName>
IP and IPX Routing		
TCP/IP Routing IPX Routing	Must be disabled Must be enabled	eth ip disable eth ipx enable
Store **Reboot**		save reboot

* Enter this information if you are using PPP in an ATM environment.
** Enter this information if you are using PPP in a Frame Relay environment.
** If the ISP does not support the authentication of the ISP system by the caller, use the command: `remote disauthen <remoteName>` to disable the authentication.

Configuring PPP with Bridging

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

PPP with Bridging		
STEPS	**SETTINGS**	**COMMANDS**
System Settings		
System Name	Required	system name <name>
System Message	Optional	system msg <message>
Authorization Password	Required	system passwd <password>
DHCP Settings	Already enabled; additional settings may be required	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver < IpAddr >
Change Login	Optional	system admin <password>
Remote Routers		
New Entry	Enter: Remote Name	remote add <remoteName>
Link Protocol/PVC* (for ATM routers)	Select: PPP Enter: VPI/VCI	remote setProtocol PPP <remoteName> remote setPVC <vpi number>*<vci number> <remoteName>
Link Protocol/DLCI** (for Frame Relay routers)	Select: PPP Enter: DLCI number	remote setProtocol PPP <remoteName> remote setDLCI <number> <remoteName>
Security *** Remote's Password	Choose security level Enter: Password	remote setAuthen <protocol> <remoteName> remote setPasswd <passwd> <remoteName>
Bridging On/Off	Must be ON	remote enaBridge <remoteName>
IP and IPX Routing		
IP Routing	Must be disabled	eth ip disable
IPX Routing	Must be enabled	eth ipx disable
Store **Reboot**		save reboot

* Enter this information if you are using PPP in an ATM environment.

** Enter this information if you are using PPP in a Frame Relay environment.

*** If the ISP does not support the authentication of the ISP system by the caller, use the command `remote disauthen <remoteName>` to disable the authentication.

Configuring RFC 1483 / RFC 1490 with IP Routing

This table outlines configuration commands for the RFC 1483 and the RFC 1490 Link Protocols with the IP Routing Network Protocol.

RFC 1483 / RFC 1490 with IP Routing		
STEPS	**SETTINGS**	**COMMANDS**
System Settings		
System Message	Optional	system msg <message>
Ethernet IP Address	As required	eth ip add <ipNet> <ipNetMasK>
DHCP Settings	Already enabled; additional settings may be required	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver < IpAddr >
Change Login	Optional	system admin <password>
Remote Routers		
New Entry	Enter: Remote Name	remote add <remoteName>
Link Protocol/PVC* (for ATM routers)	Select: RFC 1483 Enter: VPI/VCI Numbers	remote setProtocol RFC1483 <remoteName> remote setPVC <vpi number>*<vci number> <remoteName>
Link Protocol/DLCI** (for Frame Relay routers)	Select: FR Enter: DLCI number	remote setProtocol FR <remoteName> remote setDLCI <number> <remoteName>
Bridging On/Off	Must be OFF	remote disBridge <remoteName>
TCP/IP Route Address	Enter: Explicit or default route with remote gateway	remote addiproute <ipNet> <ipNetMask> <hops> <remoteName>
If Address Translation (NAT) is enabled: TCP/IP Route Addresses	To enable NAT, use: Enter: Source WAN Port Address	remote setIpTranslate on <remoteName> remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>
If NAT is OFF: TCP/IP Route Addresses	You may still need to enter a Source WAN Port Address	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Must be enabled (Optional)	eth ip enable eth firewall < on | off >
IPX Routing	Must be disabled	eth ipx disable
Store **Reboot**		save reboot

* Enter this information if you are using RFC 1483 in an ATM environment.
** Enter this information if you are using RFC 1490 in a Frame Relay environment.

Configuring RFC 1483 / RFC 1490 with IPX Routing

This table outlines configuration commands for the RFC 1483 and RFC 1490 Link Protocols with the IPX Routing Network Protocol.

NOTE: Appendix B provides step-by-step information on how to configure IPX routing.

RFC 1483 / RFC 1490 with IPX Routing		
STEPS	**SETTINGS**	**COMMANDS**
System Settings		
System Message	Optional	system msg <message>
Ethernet IP Address	As required	eth ip addr <ipAddr> <ipNetMask>
DHCP Settings	Already enabled; additional settings may be required	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver < IpAddr >
Ethernet IPX Network #	Enter: IPX Network # Frame Type (default is 802.2)	eth ipx addr <ipxNet> eth ipx frame <type>
Change Login	Optional	system admin <password>
Remote Routers		
New Entry	Enter: Remote Name	remote add <remoteName>
Link Protocol/PVC (for ATM routers)	Select: RFC 1483 Enter: VPI/VCI Numbers	remote setProtocol RFC1483 <remoteName> remote setPVC <vpi number>*<vci number> <remoteName>
Link Protocol/DLCI** (for Frame Relay routers)	Select: FR Enter: DLCI number	remote setProtocol FR <remoteName> remote setDLCI < number> <remoteName>
Bridging On/Off	Must be OFF	remote disBridge <remoteName>
IPX Routes Add	Enter appropriate info	remote addIpxroute <ipxNet> <metrics> <ticks> <remoteName>
IPX SAPs Add	Enter appropriate info	remote addIpxsap <service_name> <ipxNet> < ipxNode> <socket> <type> <hops> <remoteName>
WAN Network Number	Enter appropriate info	remote setIpxaddr <ipxNet> <remoteName>
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Must be disabled (Optional)	eth ip disable eth firewall <on | off >
IPX Routing	Must be enabled	eth ipx enable
Store **Reboot**		save reboot

* Enter this information if you are using RFC 1483 in an ATM environment.
** Enter this information if you are using RFC 1490 in a Frame Relay environment.

Configuring RFC 1483 / RFC 1490 with Bridging

This table outlines configuration commands for the RFC 1483 and RFC 1490 Link Protocols with the Bridging Network Protocol.

RFC 1483 / RFC 1490 with Bridging		
STEPS	**SETTINGS**	**COMMANDS**
System Settings		
System Message	Optional	system msg <message>
DHCP Settings	Already enabled; additional settings may be required	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver < IpAddr >
Change Login	Optional	system admin <password>
Remote Routers		
New Entry	Enter: Remote Name	remote add <remoteName>
Link Protocol/PVC (for ATM routers)	Select: RFC 1483 Enter: VPI/VCI Numbers	remote setProtocol RFC1483 <remoteName> remote setPVC <vpi number>*<vci number> <remoteName>
Link Protocol/DLCI** (for Frame Relay routers)	Select: FR Enter: DLCI number	remote setProtocol FR <remoteName> remote setDLCI <number> <remoteName>
Bridging On/Off	Must be ON	remote enaBridge <remoteName>
IP and IPX Routing		
IP Routing	Must be disabled	eth ip disable
IPX Routing	Must be disabled	eth ipx disable
Store **Reboot**		save reboot

*Enter this information if you are using RFC 1483 in an ATM environment.
**Enter this information if you are using RFC 1490 in a Frame Relay environment.

Configuring MAC Encapsulated Routing: RFC 1483MER / RFC 1490MER with IP Routing

This table outlines configuration commands for the RFC 1483MER and RFC 1490MER Link Protocols with the IP Routing Network Protocol.

RFC 1483MER / RFC 1490 MER with IP Routing		
STEPS	**SETTINGS**	**COMMANDS**
System Settings		
System Message	Optional	system msg <message>
Ethernet IP Address	As required	eth ip add <ipNet> <ipNetMasK>
DHCP Settings	Already enabled; additional settings may be required	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver < IpAddr >
Change Login	Optional	system admin <password>
Remote Routers		
New Entry	Enter: Remote Name	remote add <remoteName>
Link Protocol/PVC* (for ATM routers)	Select: RFC 1483MER Enter: VPI/VCI Numbers	remote setProtocol RFC1483MER <remoteName> remote setPVC <vpi number>*<vci number> <remoteName>
Link Protocol/DLCI** (for Frame Relay routers)	Select: MER Enter: DLCI number	remote setProtocol MER <remoteName> remote setDLCI <number> <remoteName>
Bridging On/Off	Must be OFF	remote disBridge <remoteName>
TCP/IP Route Address	Enter: Explicit or default route with remote gateway	remote addiproute <ipNet> <ipNetMask> <hops> <ipGateway> <remoteName>
If Address Translation (NAT) is enabled:	To enable NAT, use:	remote setIpTranslate on <remoteName>
	Enter: Source WAN Port Address + mask of the remote network	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>
If NAT is OFF: TCP/IP Route Addresses	Enter a Source WAN Port Address + mask of the remote network's mask	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Must be enabled (Optional)	eth ip enable eth firewall < on | off >
IPX Routing	Must be disabled	eth ipx disable
Store **Reboot**		save reboot

*Enter this information if you are using RFC 1483 in an ATM environment.
**Enter this information if you are using RFC 1490 in a Frame Relay environment.

Configuring FRF8 with IP Routing

This table outlines configuration commands for the FRF8 Link Protocol with the IP Routing Network Protocol.

FRF8 with IP Routing		
STEPS	**SETTINGS**	**COMMANDS**
System Settings		
System Message	Optional	system msg <message>
Ethernet IP Address	As required	eth ip add <ipNet> <ipNetMasK>
DHCP Settings	Already enabled; additional settings may be required	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver < IpAddr >
Change Login	Optional	system admin <password>
Remote Routers		
New Entry	Enter: Remote Name	remote add <remoteName>
Link Protocol/PVC	Select: FRF8 Enter: VPI/VCI Numbers	remote setProtocol FRF8 <remoteName> remote setPVC <vpi number>*<vci number> <remoteName>
Bridging On/Off	Must be OFF	remote disBridge <remoteName>
TCP/IP Route Address	Enter: Explicit or default route	remote addiproute <ipNet> <ipNetMask> <hops> <remoteName>
If Address Translation (NAT) is enabled:	To enable NAT, use:	remote setIpTranslate on <remoteName>
	Enter: Source WAN Port Address + mask of the remote network	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>
If NAT is OFF: TCP/IP Route Addresses	Enter a Source WAN Port Address + mask of the remote network	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	Must be enabled (Optional)	eth ip enable eth firewall < on | off >
IPX Routing	Must be disabled	eth ipx disable
Store **Reboot**		save reboot

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 Link Protocol 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.

Verify The Router Configuration

Test IP Routing

Test IP Routing over the Local Ethernet LAN (from PC)

- Use the TCP/IP `ping` command or a similar method to contact the configured target router specifying the Ethernet LAN IP address.
- If you cannot contact the router, verify that the Ethernet IP address and subnet mask are correct and check cable connections.
- Make sure that you have saved and rebooted after setting the IP address.
- Check Network TCP/IP properties under Windows 95. If you are running Windows 3.1, check that you have a TCP/IP driver installed.

Test IP Routing To a Remote Destination

- Using the TCP/IP `ping` command, contact a remote router from a local LAN-connected PC. When you enter the ping command, the router will connect to the remote router using the ATM or ADSL line.

- If remote or local WAN IP Addresses are required, verify that they are valid.
- Use the **`iproutes`** command to check the contents of the IP routing table and that you have specified a default route as well.

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 located on the network beyond a remote router to verify the TCP/IP route addresses entered in the remote router database.
- Verify that you configured correct static IP routes.
- Use the **`iproutes`** command to check the contents of the IP routing table.

Test Bridging to a Remote Destination

Use any application from a local LAN-attached station that accesses a server or disk using a protocol that is being bridged on the remote network beyond the remote router. If you cannot access the server:

- Verify that you have specified a default destination remote router.
- Make sure that you have enabled bridging to the remote router.
- Check that bridging filtering does not restrict access from the local station.

Test IPX Routing

One way to test IPX Routing is to check for access to servers on the remote LAN. Under Windows, use the "NetWare Connections" selection provided with NetWare User Tools. Under DOS, use the command "**pconsole**" or type **`login`** on the login drive (usually F:)**.** Select the printer server and verify that the server you have defined is listed. When you attempt to access the server, the router will connect to the remote router using the ATM or ADSL line.

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.
- List the contents of the routing and services tables using the **`ipxroutes`** and **`ipxsaps`** commands, respectively.
- Make sure that the security authentication method and password that you configured matches the remote router.

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
- Several “list” commands outputs that are used to check the information entered for this particular configuration.
- 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 A.

Scenario

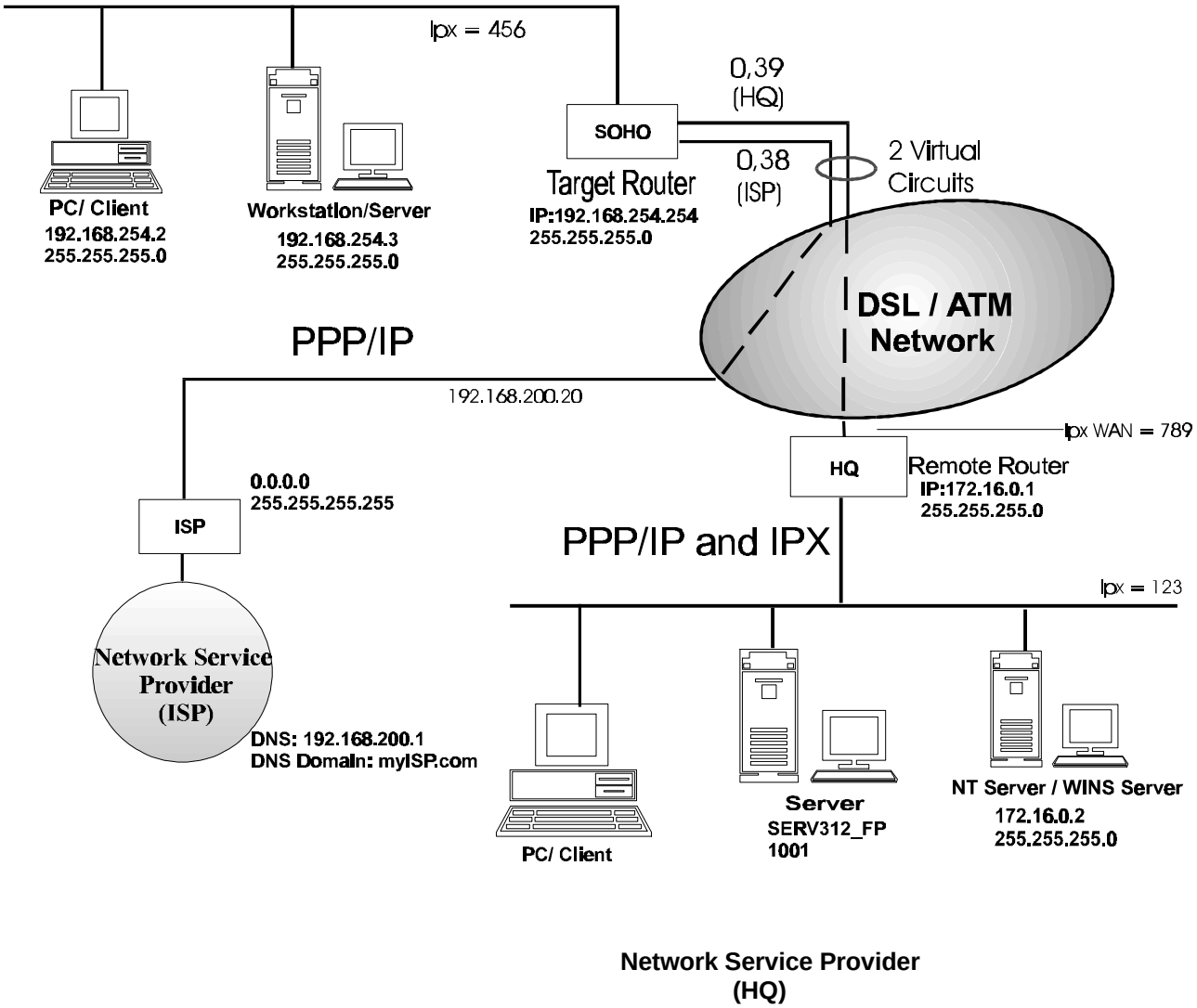
In this configuration example of a hypothetical network, a small office/home office **(SOHO)** will access:

- 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) through a Network Service Provider (NSP provides access to the DSL/ATM Wide Area Network); 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**	**Commands**
System Settings Name	System Name	**system name SOHO**
System Settings Message	Message (optional)	**system msg Configured_Dec_1997**
System Settings Authentication Password	Authentication Password	**system passwd SOHOpasswd**
System Settings Ethernet IP Address Ethernet IPX Network	Ethernet IP Address and Subnet Mask (default IP address) Ethernet IPX Network Number	**eth ip addr 192.168.254.254 255.255.255.0** **eth ipx addr 456**
System Settings DHCP Settings	DNS Domain Name DNS Server WINS Server Address	**dhcp set valueoption domainname myISP.com** **dhcp set valueoption domainnameserver 192.168.200.1** **dhcp set valueoption winsserver 172.16.0.2**

SOHO REMOTE ROUTER DATABASE ENTRY: HQ		
Configuration Section	**Item**	**Commands**
Remote Routers New Entry	Remote Router's Name	**remote add HQ**
Remote Routers Link Protocol PVC	Link Protocol VPI Number/VCI Number	**remote setProtocol PPP HQ** **remote setPVC 0*39 HQ**
Remote Routers Security	Minimum Authentication (PAP is the default) Remote Router's Password	**remote setauthen PAP HQ** **remote setpasswd HQpasswd HQ**
Remote Routers Bridging	Bridging On/Off **(**Bridging is OFF by default)	**remote disbridge HQ**
Remote Routers TCP/IP Route Addresses	Remote Network's IP Addresses, Subnet Masks, and Metric	**remote addiproute 172.16.0.0 255.255.255.0 1 HQ**
Remote Routers IPX Address	Network #, Hop Count, Ticks	**remote addipxroute 1001 1 4 HQ**
Remote Routers IPX SAPs	SAPS: Server Name, Server Type, Network #, Node #, Sockets, type, hops WAN Network #	**remote addipxsap SERV312_FP 4 1001 00-00-00-00-00-01 451 3 1 HQ** **remote setipxaddr 789 HQ**

NOTE: One chart for each remote router in the Remote Router Database

SOHO REMOTE ROUTER DATABASE ENTRY: ISP		
Configuration Section	**Item**	**Commands**
Remote Routers New Entry	Remote Router's Name	**remote add ISP**
Remote Routers Link Protocol PVC	Link Protocol VPI Number/VCI Number	**remote setProtocol PPP ISP** **remote setPVC 0*38 ISP**
Remote Routers Security	Minimum Authentication (PAP is the default) Remote Router's Password	**remote setauthen PAP ISP** **remote setpasswd ISPpasswd ISP**
Remote Routers Bridging	Bridging On/Off **(**Bridging is OFF by default)	**remote disbridge ISP**
Remote Routers TCP/IP Route Addresses	Remote Network's IP Addresses, Subnet Masks, and Metric Network Address Translation In Advanced: Source WAN IP Address and Subnet Mask*	**remote addiproute 0.0.0.0 255.255.255.255 1 ISP (Default Route)** **remote setiptranslate on ISP** **remote setSrcIpAddr 192.168.200.20 255.255.255 255 ISP**

* This is needed only if the ISP does not assign an IP address automatically.
NOTE: One chart for each remote router in the remote router database

SOHO ROUTING CONTROLS		
Configuration Section	**Item**	**Commands**
IP and IPX Routing	TCP/IP Routing On/Off IPX Routing On/Off Internet Firewall On/Off (Firewall is ON by default)	**eth ip enable** **eth ipx enable** **eth ip firewall on**

Sample Configuration 1 - Check the Configuration with the “list” Commands

system list

```
GENERAL INFORMATION FOR <SOHO>
  System started on..................... 12/1/1997 at 17:41
  Authentication override.............. NONE
 WAN to WAN Forwarding................ yes
  BOOTP/DHCP Server address............ none
  Telnet Port.......................... default (23)
SNMP Port............................ default (161)
  System message: configured Dec-1997
```

remote list

```
INFORMATION FOR <HQ>
  Status............................... enabled
  Protocol in use...................... PPP
  Authentication....................... enabled
  Authentication level required........ PAP
  Connection Identifier (VPI*VCI)...... 0*39
  IP address translation............... off
  Compression Negotiation.............. off
  Source IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Remote IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Send IP RIP to this dest............. no
    Send IP default route if known..... no
  Receive IP RIP from this dest........ no
    Receive IP default route by RIP.... no
  Keep this IP destination private..... yes
  Total IP remote routes............... 1
           172.16.0.0/255.255.255.0/1
  IPX network number................... 00000789
  Total IPX remote routes.............. 1
           00001001/1/4
  Total IPX SAPs....................... 1
    SERV312_FP 00001001 00:00:00:00:00:01 0451 0003 1
  Bridging enabled..................... no
    Exchange spanning tree with dest... yes

INFORMATION FOR <ISP>
  Status............................... enabled
  Protocol in use...................... PPP
  Authentication....................... enabled
  Authentication level required........ PAP
  Connection Identifier (VPI*VCI)...... 0*38
  IP address translation............... on
  Compression Negotiation.............. off
  Source IP address/subnet mask........ 192.168.200.20/255.255.255.255
  Remote IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Send IP RIP to this dest............. no
    Send IP default route if known..... no
  Receive IP RIP from this dest........ no
```

```
    Receive IP default route by RIP.... no
  Keep this IP destination private..... yes
  Total IP remote routes............... 1
           0.0.0.0/255.255.255.255/1
  IPX network number................... 00000000
  Total IPX remote routes.............. 0
  Total IPX SAPs....................... 0
  Bridging enabled..................... no
    Exchange spanning tree with dest... yes
```

dhcp list

```
       bootp server ................. none
       bootp file ................... n/a

       DOMAINNAMESERVER (6) ......... 192.168.200.1
       DOMAINNAME (15) .............. myISP.com
       WINSSERVER (44) .............. 172.16.0.2

Subnet 192.168.254.0, disabled - other DHCP servers detected
       When DHCP servers are active . stop
       Mask ......................... 255.255.255.0
       first ip address ............. 192.168.254.2
       last ip address .............. 192.168.254.20
       lease ........................ default
       bootp ........................ not allowed
       bootp server ................. none
       bootp file ................... n/a
```

eth list

```
ETHERNET INFORMATION FOR <ETHERNET/0>
  Hardware MAC address................. 00:20:6F:02:A1:BF
  Bridging enabled..................... no
  IP Routing enabled................... yes
    Firewall filter enabled ........... yes
    Send IP RIP to the LAN............. rip-1 compatible
      Advertise me as default router... yes
    Process IP RIP packets received.... rip-1 compatible
      Receive default route by RIP..... yes
  RIP Multicast address................ default
  IP address/subnet mask............... 192.168.254.254/255.255.255.0
  IP static default gateway............ none
  IPX Routing enabled.................. yes
    External network number............ 00000456
    Frame type......................... 802.2
```

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: If you have trouble with passwords, we recommend 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
- Several "list" commands outputs that are used to check the information entered for this particular configuration.

Note 1: Names and Passwords are not required 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 A.

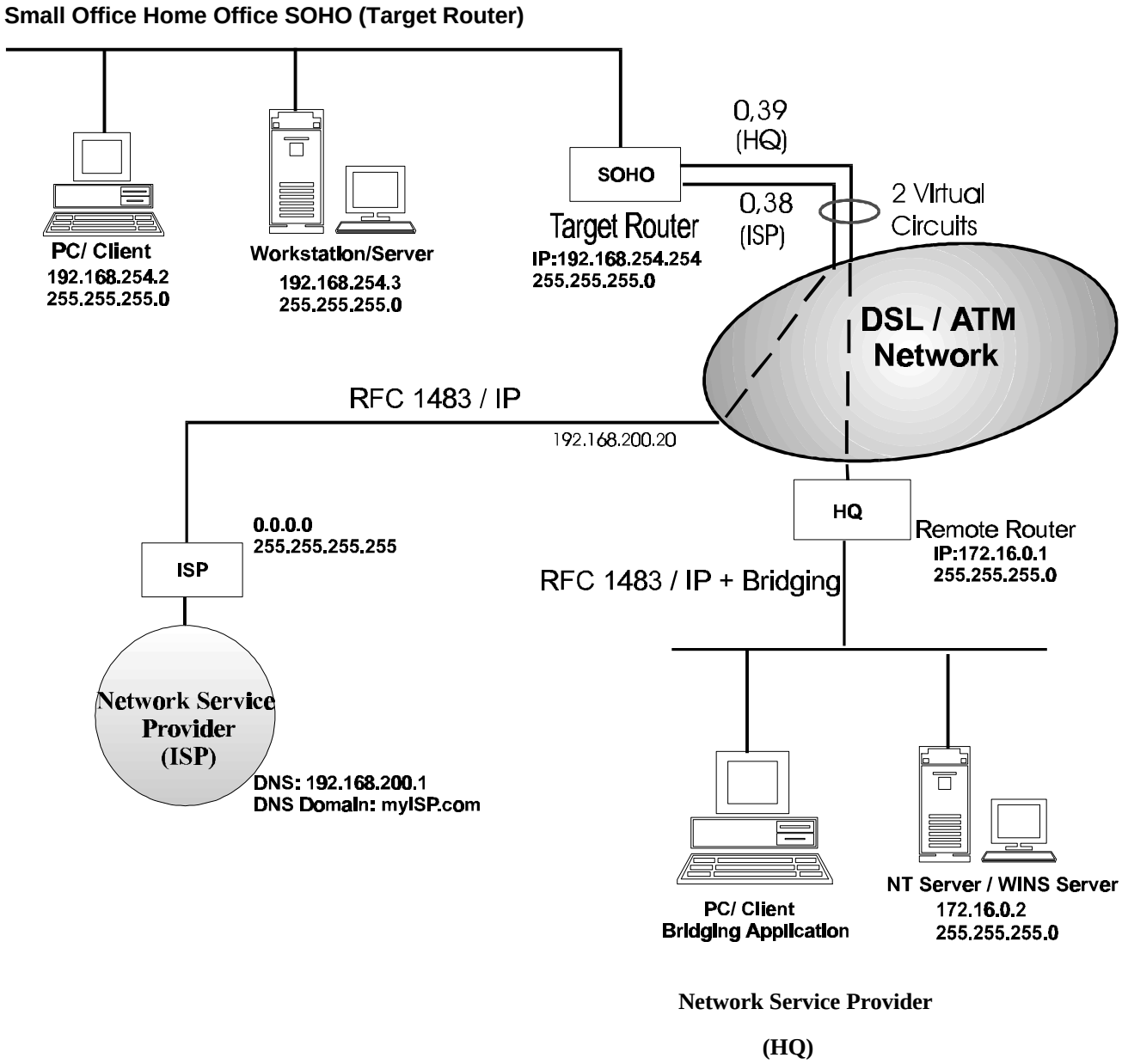
Scenario

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) through a Network Service Provider (NSP provides access to the DSL/ATM Wide Area Network); 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



Sample Configuration 2 — Tables For Target Router (SOHO)

SOHO SYSTEM SETTINGS		
Configuration Section	**Item**	**Commands**
System Settings Message	Message (optional)	**system msg RFC1483_dec97**
System Settings Ethernet IP Address	Ethernet IP Address and Subnet Mask (default IP address)	**eth ip addr 192.168.254.254 255.255.255.0**
System Settings DHCP Settings	DNS Domain Name DNS Server WINS Server address	**dhcp set valueoption domainname myISP.com** **dhcp set valueoption domainnameserver 192.168.200.1** **dhcp set valueoption winsserver 172.16.0.2**

SOHO REMOTE ROUTER DATABASE ENTRY: HQ		
Configuration Section	**Item**	**Commands**
Remote Routers New Entry	Remote Router's Name	**remote add HQ**
Remote Routers Link Protocol PVC	Link Protocol VPI Number/VCI Number	**remote setProtocol RFC1483 HQ** **remote setPVC 0*39 HQ**
Remote Routers Bridging	Bridging On/Off	**remote enabridge HQ**
Remote Routers TCP/IP Route Addresses	Remote Network's IP Addresses, Subnet Masks, and Metric	**remote addiproute 172.16.0.0 255.255.255.0 1 HQ**

SOHO REMOTE ROUTER DATABASE ENTRY: ISP		
Configuration Section	**Item**	**Commands**
Remote Routers New Entry	Remote Router's Name	**remote add ISP**
Remote Routers Link Protocol PVC	Link Protocol VPI Number/VCI Number	**remote setProtocol RFC1483 ISP** **remote setPVC 0*38 ISP**
Remote Routers Bridging	Bridging On/Off (Bridging is Off by default)	**remote disbridge ISP**
Remote Routers TCP/IP Route Addresses	Remote Network's IP Addresses, Subnet Masks, and Metric Network Address Translation (NAT) In Advanced: Source WAN IP Address and Subnet Mask	**remote addiproute 0.0.0.0 255.255.255.255 1 ISP** **remote setIpTranslate on ISP** **remote setSrcIpAddr 192.168.200.20 255.255.255.255 ISP**

SOHO ROUTING CONTROLS		
Configuration Section	**Item**	**Commands**
IP and IPX Routing	TCP/IP Routing On/Off IPX Routing On/Off (IPX routing is OFF by default) Internet Firewall On/Off (Firewall is ON by default)	**eth ip enable** **eth ipx disable** **eth ip firewall on**

Sample Configuration 2 - Check the Configuration with the “list” Commands

system list

```
GENERAL INFORMATION FOR <SOHO>
  System started on..................... 12/1/1997 at 17:48
  Authentication override............... NONE
WAN to WAN Forwarding................ yes
  BOOTP/DHCP Server address............ none
  Telnet Port.......................... default (23)
SNMP Port............................ default (161)
  System message: ADSL RCF1483 sample
```

eth list

```
ETHERNET INFORMATION FOR <ETHERNET/0>
  Hardware MAC address................. 00:20:6F:02:A1:BF
  Bridging enabled..................... yes
  IP Routing enabled................... yes
    Firewall filter enabled ........... yes
    Send IP RIP to the LAN............. rip-1 compatible
      Advertise me as default router... yes
    Process IP RIP packets received.... rip-1 compatible
      Receive default route by RIP..... yes
  RIP Multicast address................ default
  IP address/subnet mask............... 192.168.254.254/255.255.255.0
    IP static default gateway............ none
  IPX Routing enabled.................. no
    External network number............ 00000000
    Frame type......................... 802.2
```

remote list

```
INFORMATION FOR <HQ>
  Status............................... enabled
  Protocol in use...................... RFC1483 (SNAP)
  Connection Identifier (VPI*VCI)...... 0*39
  IP address translation............... off
  Compression Negotiation.............. off
  Source IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Remote IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Send IP RIP to this dest............. no
    Send IP default route if known..... no
  Receive IP RIP from this dest........ no
    Receive IP default route by RIP.... no
  Keep this IP destination private..... yes
  Total IP remote routes............... 1
           172.16.0.0/255.255.255.0/1
  IPX network number................... 00000000
  Total IPX remote routes.............. 0
  Total IPX SAPs....................... 0
  Bridging enabled..................... yes
    Exchange spanning tree with dest... yes
```

```
INFORMATION FOR <ISP>
  Status............................. enabled
  Protocol in use.................... RFC1483 (SNAP)
  Connection Identifier (VPI*VCI)..... 0*38
  IP address translation............... on
  Compression Negotiation.............. off
  Source IP address/subnet mask........ 192.168.200.20/255.255.255.255
  Remote IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Send IP RIP to this dest............ no
    Send IP default route if known..... no



Receive IP RIP from this dest........ no
    Receive IP default route by RIP.... no
  Keep this IP destination private..... yes
  Total IP remote routes............... 1
           0.0.0.0/255.255.255.255/1
  IPX network number................... 00000000
  Total IPX remote routes.............. 0
  Total IPX SAPs....................... 0
  Bridging enabled..................... no
    Exchange spanning tree with dest... yes
```

dhcp list

```
       bootp server ................. none
       bootp file ................... n/a

       DOMAINNAMESERVER (6) ......... 192.168.200.1
       DOMAINNAME (15) .............. myISP.com
       WINSSERVER (44) .............. 172.16.0.2

Subnet 192.168.254.0, disabled - other DHCP servers detected
       When DHCP servers are active . stop
       Mask ......................... 255.255.255.0
       first ip address ............. 192.168.254.2
       last ip address .............. 192.168.254.20
       lease ........................ default
       bootp ........................ not allowed
       bootp server ................. none
       bootp file ................... n/a
```

Chapter 4. Configuring Special Features

IP Firewall Bridging Filtering

Enable/Disable Internet Firewall Filtering

The router supports 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. You can set Internet Firewall Filtering using the command:

`eth ip firewall on|off|list`

The Internet Firewall defaults to ON during initial configuration and is active *only* when Ethernet LAN IP routing is on.

As described earlier, Ethernet LAN IP routing is controlled by the commands:

```
eth ip enable
eth ip disable
```

Therefore, at initial configuration, you need only enable IP routing to activate the Internet Firewall Filter. If you do not wish the router to perform IP Internet Firewall Filtering while IP routing, you must turn OFF the Firewall Filter. Remember to save and reboot if you alter IP routing status.

Configure Bridging Filtering

Bridging filtering allows you to control the packets transferred across the router. This feature can be used to enhance security or improve performance. Filtering occurs based on matched patterns within the packet at a specified offset. Two filtering modes are available:

- "Deny" mode will discard any packet matched to the "deny" filters in the filter database and let all other packets pass.
- "Allow" mode will only pass the packets that match the "allow" filters in the filter database and discard all others.

Up to 40 "allow" filters or 40 "deny" filters can be activated from the filter database.

You enter the filters, including the pattern, offset, and filter mode, into a filter database. If you intend to restrict specific stations or subnetworks from bridging, then add the filters with a "deny' designation. Then enable filtering for deny. If you wish to allow only specific stations or subnetworks to bridge, then add the filters with an "allow" designation and enable filtering for "allow". Add each filter with the following command:

`filter br add` *`pos dataPattern`* **`deny|allow`**

where *`pos`* is the byte offset within a packet (number from 0-127) to a *`dataPattern`* (a hex number up to 6 bytes). This data and offset number can be used to identify an address, protocol id or data content. After you have entered all of the filters, verify your entries with the following command:

`filter br list`

If you have entered an incorrect filter, delete the filter using the **`filter br del`** command. When you are satisfied with the filter list, save the filtering database with the **`save filter`** command. You must reboot the router to load the filtering database. Then enable bridging filtering with the following command:

`filter br use none|deny|allow`

Test the filtering configuration by accessing a remote destination identified in the filter.

DHCP (Dynamic Host Configuration Protocol)

This section describes how to configure DHCP using the Command Line Interface. Configuring DHCP can be a complex process; this section is therefore intended for network managers. Please refer to Chapter 4 for a complete list of the DHCP commands.

General Information

The router supports DHCP and acts as the DHCP server. DHCP is a service that allocates IP addresses automatically to any DHCP client (any device attached to your network such as your PC) requesting an IP address.

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 manual initialization process (reconfiguration of router and/or PC addresses to be in the same network).

To configure DHCP for a network, the network administrator defines a range of valid IP addresses to be used in the subnetwork as well as options and other parameters. Once DHCP is configured for the network, each DHCP client (your PC for example) can easily request an IP address from the pool of valid IP addresses. The DHCP client will learn part or all of the network parameters automatically. IP addresses and options assigned to a client are collectively called the lease. The lease is only valid for a certain period of time and is automatically renewed by the client. Note that **Internet Quick Start** configurator does a basic configuration of the DHCP server by asking for some common options.

DHCP administration and configuration is divided into the following parts:

- Manipulating subnetworks and explicit client leases
- Setting option values
- BootP
- Defining option types
- Other information

Note 1: The TCP/IP stack has to be installed on the PCs for DHCP to work.

Note 2: In Windows, DHCP is enabled by selecting it on your PC (under Settings, Control Panel, Network, and TCP/IP in the Configuration tab page).

Note 3: To save the DHCP configuration or changes to FLASH in the router, make sure to use the command:
dhcp save

Manipulating Subnetworks and Explicit Client Leases

A) Enabling/disabling a subnetwork or a client lease

To enable/disable a subnetwork or a client lease, use the commands:

```
dhcp enable <net> <ipAddr>
dhcp disable <net> <ipAddr>
```

Examples:

To enable the subnetwork 192.168.254.0 if that subnetwork exists, type:

```
dhcp enable 192.168.254.0
```

To enable the client lease 192.168.254.17 if that client lease exists, enter:

```
dhcp enable 192.168.254.17
```

To disable the client lease 192.168.254.18 if that client lease exists, type:

```
dhcp disable 192.168.254.18
```

To check the results of these commands, use:

```
dhcp list
```

If the client lease does NOT exist, it must be explicitly created.

B) Adding subnetworks and client leases

Adding a subnetwork

The following commands are used to add/delete subnetworks. Only one subnetwork with one pool of IP addresses may be defined for a subnet.

To add a subnetwork, use:

```
dhcp add <net> <mask>
```

To remove a subnetwork, use:

```
dhcp del <net>
```

Note: All client leases associated with this subnetwork are automatically deleted.

Examples:

The following command will create a subnetwork 192.168.254.0 with a subnet mask of 255.255.255.0:

```
dhcp add 192.168.254.0 255.255.255.0
```

The following command will delete the subnetwork 192.168.254.0 and will delete all client leases associated with that subnetwork:

```
dhcp del 192.168.254.0
```

Adding explicit or dynamic client leases

Client leases may either be created dynamically or explicitly. Usually client leases are created dynamically when PCs boot and ask for IP addresses.

Explicit client leases

To add an explicit client lease, a subnetwork MUST already exist (use **dhcp add <net> <mask>** to add the subnetwork) before the client lease may be added. Use the command:

```
dhcp add <ipAddr>
```

To remove a client lease, type:

```
dhcp del <ipAddr>
```

NOTE: An administrator MAY create a client lease that is part of a subnet but does not fall within the pool of IP addresses.

Examples:

To explicitly add the client lease 192.168.254.31, use:

```
dhcp add 192.168.254.31
```

To delete the client lease 192.168.254.31, use:

```
dhcp del 192.168.254.31
```

Dynamic Client Leases

Dynamic client leases are created from the pool of IP addresses associated with that subnetwork. To set or change the pool, use:

```
dhcp set addresses <firstipAddr> <lastipAddr>
```

To clear the values from the pool, use:

```
dhcp clear addresses <net>
```

Note: Any client leases that currently exist will NOT be affected.

To remove a client lease that was dynamically created, use:

```
dhcp del <ipAddr>
```

Caution: If <ipAddr> is a subnet, you will delete the entire subnet.

C) Setting the lease time

Concepts

The information given by the DHCP server (router) to your PC is leased for a specific amount of time.

The client lease has already been selected. The DHCP server will select the lease time based on the option defined for the client lease as described by this algorithm:

1) If the client lease option is a specific number or is infinite, then the server uses the specified lease time associated with this client lease.

2) If the client lease option is "default", then the server goes up one level (to the subnetwork) and uses the lease time explicitly specified for the subnetwork.

3) If the client and subnetwork lease options are both "default", then the server goes up one level (global) and uses the lease time defined at the global level (server).

4) Lease time:
   The minimum lease time is 1 hour.
   The global default is 168 hours.

Commands

The following commands are used by network administrators to control lease time.

To set the lease time explicitly for the client lease, use:

```
dhcp set lease <ipAddr> <hours>
```

To set the lease time explicitly for the subnetwork lease, use:

```
dhcp set lease <net> <hours>
```

To set the lease time explicitly for the global lease, use:

```
dhcp set lease <hours>
```

Examples:

To set the lease time to "default" for the client 192.168.254.17, use:

```
dhcp set lease 192.168.254.17 default
```

To set the subnetwork lease time to infinite for the subnet 192.168.254.0, use:

```
dhcp set lease 192.168.254.0 infinite
```

To set the global lease time to 2 hours, use:

```
dhcp set lease 2
```

D) Manually changing client leases

Administrators will generally NOT need to change client leases manually. However, if the need arises to do so, use the following commands.

WARNING: The client will not be aware that the administrator has changed or released a client lease!

This command will change the client lease expiration time to a given value:

```
dhcp set expire <ipAddr> <hours>
```

Setting the expiration time to “default” will cause the server to compute the lease time using the algorithm as described in section C, *Setting the lease time.*

Use this command to release the client lease so it becomes available for other assignments:

```
dhcp clear expire <ipAddr>
```

Setting Option Values

Administrators will want to set the values for global options, for options specific to a subnetwork, or for options specific to a client lease.

NOTE: See RFC 2131/2132 for the description of various options.

A. Concepts

The server returns values for options explicitly requested in the client request. It selects the values to return based on the following algorithm:

1) If the value is defined for the client, then the server will return the requested value for an option.

2) If the value for the option has not been set for the client, then the server returns the value option if it has been defined for the subnetwork.

3) If the valueoption does not exist for the client AND does not exist for the subnetwork, then the server returns the value option if it has been defined globally.

4) If the value option is not defined anywhere, the server will NOT return any value for that option in its reply to the client request.

IMPORTANT: When replying to a client request, the server does:

- Not return any option values NOT requested by the client.
- Not support the definition of a "class" of clients.
- Not return any non-default option values UNLESS the client requests the option value AND the server has a value defined for that option.
- Not return any non-default values on the clients subnet UNLESS the client requests the value for that option.

B. Commands for global option values

To set the value for a global option, use:

`dhcp set valueoption <code> <value> ...`
The code can be a number between 1 and 61 or a keyword.

To see the list of predefined and user-defined options, type:

`dhcp list definedoptions`

To clear the value for a global option, use:

`dhcp clear valueoption <code>`

Example:

To set the global value for the domain name server option, enter:

```
dhcp set valueoption domainnameserver 192.168.254.2 192.168.254.3
```

C. Commands for specific option values for a subnetwork

To set the value for an option associated with a subnetwork, type:

```
dhcp set valueoption <net> <code> <value>...
```

To clear the value for an option associated with a subnetwork, use:

```
dhcp clear valueoption <net> <code>
```

Examples:

```
dhcp set valueoption 192.168.254.0 gateway 192.168.254.254
dhcp set valueoption 6 192.84.210.75 192.84.210.68
```

D. Commands for specific option values for a client lease:

To set the value for an option associated with a specific client, use:

```
dhcp set valueoption <ipAddr> <code> <value>...
```

To clear the value for an option associated with a specific client, type:

```
dhcp clear valueoption <ipAddr> <code>
```

Example:

```
dhcp set valueoption 192.168.254.251 winserver 192.168.254.7
```

E. Commands for listing and checking option values:

To list the values for global options as well as subnet and client lease information, use:

```
dhcp list
```

To list options that are set for that subnet/client lease as well as subnet/client lease information, type:

```
dhcp list <net>|<ipAddr>
```

This command lists all available options (predefined and user-defined options):

```
dhcp list definedoptions
```

This command lists all available options starting with the string "name".

```
dhcp list definedoptions name
```

To list the lease time use:

```
dhcp list lease
```

Example:

This command lists the subnet 192.168.254.0 including any options set specifically for that subnet:

```
dhcp list 192.168.254.0
```

BootP

Administrators may wish to specify that certain client leases AND certain subnetworks can satisfy BootP requests.

A. About BootP and DHCP

BootP and DHCP provide services that are very similar. However, as an older service, BootP offers only a subset of the services provided by DHCP.

The main difference between BootP and DHCP is that the client lease expiration for a BootP client is always INFINITE.

Caution: Remember that when BootP is enabled, the client assumes that the lease is infinite.

By default, the DHCP server will NOT satisfy BootP requests unless the administrator has explicitly enabled BootP (at the subnetwork or lease level).

B. Enable/Disable BootP

To allow BootP request processing for a particular client/subnet, use the command:

```
dhcp bootp allow <net>|<ipAddr>
```

To disallow BootP request processing for a particular client/subnet, type:

```
dhcp bootp disallow <net>|<ipAddr>
```

C. Use BootP to specify the boot server

The following commands let the administrator specify the TFTP server (boot server) and boot file name. The administrator will first configure the IP address of the TFTP server and file name (kernel) from which to boot. This is particularly useful if the kernel in the router's flash is corrupt or does not exist.
To set the IP address of the server and the file to boot from, enter:

```
dhcp bootp tftpserver[<net>|<ipAddr>] <tftpserver ipAddr>
dhcp bootp file [<net>|<ipAddr>] <file name>
```

To clear the IP address of the server and the file to boot from, type:

```
dhcp bootp tftpserver [<net>|<ipAddr>] 0.0.0.0
```

Examples:

To set the global BootP server IP address to 192.168.254.7:

```
dhcp bootp tftpserver 192.168.254.7
```

To set the subnet 192.168.254.0 server IP address to 192.168.254.8:

```
dhcp bootp tftpserver 192.168.254.0 192.168.254.8
```

To set the client 192.168.254.21 server IP address to 192.168.254.9

```
dhcp bootp tftpserver 192.168.254.21 192.168.254.9
```

To set the subnet 192.168.254.0 boot file to "kernel.100":

```
dhcp bootp file 192.168.254.0 kernel.100
```

To clear the global BootP server IP address and file name:

```
dhcp bootp tftpserver 0.0.0.0
```

To clear the subnet 192.168.254.0 server IP address and file name:

```
dhcp bootp tftpserver 192.168.254.0 0.0.0.0
```

Defining Option Types

A. Concepts

A DHCP option is a code, length, or value. An option also has a "type" (byte, word, long, longint, binary, IP address, string).

The subnet mask, router gateway, domain name, domain name servers, NETBIOS name servers are all DHCP options. Please refer to RFC 1533 if you require more information.

Usually users will not need to define their own option types. The list of predefined option types based on RFC 1533 can be shown by typing :

```
dhcp list definedoptions
```

B. Commands

The following commands are available for adding/deleting option types:

```
dhcp add <code> <min> <max> <type>
```

To list option types that are currently defined, type:

```
dhcp list definedoptions ...
```

To list the definitions for all known options, use:

```
dhcp list definedoptions
```

To get help information, enter:

```
dhcp list definedoptions ?
```

To list the definition for option 1 if option 1 is defined, use:

```
dhcp list definedoptions 1
```

To list the definition for all options that are well-known AND have a name starting with 'h', type:

```
dhcp list definedoptions h
```

Example:

To define a new option with a code of 128, a minimum number of IP addresses of 1, a maximum number of IP addresses of 4, of type “IP address”, enter:

```
dhcp add 128 1 4 ipAddress
```

This information implies that:

- Some DHCP client will know about the option with code 128.
- Option 128 allows IP addresses.
- The server can have a minimum of 1 IP address.
- The server can have up to 4 IP addresses.

- The administrator will still need to set the option value either globally, specific to a subnetwork, or specific to a client for the option to have any meaning.

To delete the definition of the option with code 128, use:

```
dhcp del 128
```

The values for this option that have been set globally, specific to a subnetwork, or specific to a client will NOT be removed. The administrator must remove those values explicitly.

Well-known type option codes CANNOT be changed or deleted.

Other Information

DHCP information is kept in the file DHCP.DAT. This file is self contained.

This file contains ALL of the DHCP information including:

- the option definitions
- the subnetwork that have been added
- the client lease information
- the option values that have been set

This file can be uploaded/downloaded from one router to another.

NAT (Network Address Translation)

The router supports classic NAT (one NAT IP address assigned to one PC IP address) and a NAT technique known as masquerading (one single NAT IP address assigned to many PC IP addresses).

General NAT Rules

1. IP Routing must be enabled.

2. NAT can be run on a per-remote-router basis.

3. Any number of PCs on the LAN may be going to the same or different remote routers at the same time. In reality, the number of PCs on the LAN that can be supported is limited by how much memory the router consumes maintaining table information -AND- by how many connections are currently active.

4. Some operations will NOT work. Specifically, services that place IP address/port information in the data MAY NOT WORK until the router examines their packets and figures out what information in the data needs to be changed. Remember that the router is remapping both IP addresses and ports.

5. When using NAT with a remote router, either the remote ISP MUST supply the IP address for NAT translation -or- the user MUST configure the IP address for NAT translation locally.

Masquerading (one single NAT IP address shared by many PC IP addresses)

With this form of NAT, multiple local (PC) IP addresses are mapped to a single global IP address. Many local (PCs) IP addresses are therefore hidden behind a single global IP address. The advantage of this type of NAT is that users only need one global IP address, but the entire local LAN can still access the Internet. This NAT technique requires not only remapping IP addresses but also TCP and UDP ports.

Each PC on the LAN side has an IP address and mask. When the router connects to an ISP, the router appears to be a HOST with one IP address and mask. The IP address that the router uses to communicate with the ISP is obtained dynamically (with PPP/IPCP or DHCP) or is statically configured. When the PC connects to the ISP, the IP address and Port used by the PC are remapped to the IP address assigned to the router. This remapping is done dynamically.

Client Configuration

Enable NAT

To enable NAT, use the commands:

```
remote setIPTranslate <remoteName>
save
```

The `save` command makes the above changes persistent across boots which turn NAT on when connected to this remote router.

Obtain an IP Address for NAT Translation

The IP address (the IP address "known" by the remote ISP) used for this type of NAT translation can be assigned in two ways.

The ISP dynamically assigns the IP address. Use the commands:

```
remote setSrcIpAddr 0.0.0.0 0.0.0.0 <remoteName>
save
```

The IP address is assigned locally. Use the commands:

```
remote setSrcIpAddr ww.xx.yy.zz 255.255.255.255 <remoteName>
save
```

Note: ww.xx.yy.zz is the IP address the user on the local LAN is assigning.

Server Configuration

This section is intended for users and network administrators who wish to allow WAN access to a Web server, FTP server, SMTP server, etc., on their local LAN, while using NAT.

NAT needs a way to identify which local PC (local IP address(es)) should receive these server requests. The servers can be configured on a per-remote-router basis as well as globally.

Remote Commands

The following two commands are used to enable/disable a local IP address (on your LAN) as the server for a particular protocol for the remote router <*remoteName*>.

```
remote addserver <ipaddr> <protocol> <port> <remoteName>
remote delserver <ipaddr> <protocol> <port> <remoteName>
```

This command is used to view all of the remote entries, including the changes.
remote list <remoteName>

Remember to type `save` to make the changes persistent across boots.

Example 1:

Assume that the local LAN network is 192.168.1.0 255.255.255.0. The following commands are used to enable a Telnet server on the local LAN with the IP address 192.168.1.3, and an FTP server with the IP address 192.168.1.2.

```
remote addserver 192.168.1.3 tcp telnet router1
remote addserver 192.168.1.2 tcp ftp router1
```

When receiving a request from *router1* to communicate with the local Telnet server, the local router will send the request to 192.168.1.3. If *router1* asks to talk to the local FTP server, the local router will send the request to 192.168.1.2.

Example 2:

Assume that the local LAN network is 192.168.1.0 255.255.255.0. When the port value of 0 (zero) is used, it directs all ports of the specified protocol to the IP address specified.

```
remote addserver 192.168.1.4 tcp 0 router1
```

Note: `addserver` commands using specific port numbers take priority over the port # 0 setting. 192.168.1.4 will be asked to serve requests coming from *router1* to the local router. If the local router also has the same Telnet and FTP entries from the previous example, 192.168.1.3 will serve the Telnet request, 192.168.1.2 will serve the FTP request, and 192.168.1.4 will serve any other request, including HTTP, SMTP, etc.

System Commands

The following two commands are used to globally enable/disable a local IP address (on your LAN) as the server for that particular protocol.

```
system addserver <ipaddr> <protocol> <port>
system delserver <ipaddr> <protocol> <port>
```

This command is used to view all of the global system entries, including the changes.

`system list`

Remember to type `save` to make the changes persistent across boots.

Examples:

```
system addserver 192.168.1.5 tcp smtp
system addserver 192.168.1.6 tcp 0
system addserver 192.168.1.6 udp 0
```

The router sends a server request for SMTP to 192.168.1.5 when such a request comes from any remote router running NAT. The router sends any other server request (tcp or udp) to 192.168.1.6.

Server Request Hierarchy

When handling a request from a remote router (to which the local router has NAT enabled), the local router selects a server based on the following priority (order) algorithm:

1) `remote addserver` — The local router selects a server for the remote router that handles that particular protocol/port .

2) `system addserver` — The local router selects a global server that handles that particular protocol/port.

3) `remote addserver` with port 0 — The local router selects a server for the remote router that handles that particular protocol (such as tcp/udp) and ANY port.

4) `system addserver` with port 0 — The local router selects a global server that handles that particular protocol and ANY port.

5) Router's IP address — The local router selects itself (the local router) as the server.

Classic NAT (one NAT IP address assigned per one PC IP address)

With classic NAT, one PC IP address is translated to one NAT IP address. This NAT technique is primarily used to make certain hosts on a private LAN globally visible and give them the ability to remap these IP addresses as well.

Client Configuration

Classic NAT requires that you first enable NAT Masquerading as described in the previous section; thus, for the Classic and Masquerading forms of NAT, the clients are configured in the same way. Please refer to the Client Configuration section, page 75.

Host Remapping

Remote Commands

Use these commands to enable or disable host remapping on a-per-remote basis:

`remote addHostMapping <first private addr> <second private addr> <first public addr> <remoteName>`

`remote delHostMapping <first private addr> <second private addr> <first public addr> <remoteName>`

Use `remote addHostMapping` when a host on the local LAN is known by different IP addresses to different remotes.

System Commands

Use these commands to enable or disable host remapping systemwide:

`system addHostMapping <first private addr> <second private addr> <first public addr>`
`system delHostMapping <first private addr> <second private addr> <first public addr>`

Use the `system addHostMapping` when a host on the local LAN is known by the same IP address on all remotes.

IP Address Range

The range of local LAN IP addresses to be remapped is defined by <first private addr> to <second private addr> inclusive. These addresses are mapped one-to-one to the public addresses.

The range of public IP addresses is defined by <first public addr> only. The rest of the range is computed automatically (from <first public addr> to <first public addr> + number of addresses remapped - 1) inclusive.

Multiple Host Remapping Entries

Users may have as many host remapping entries as they wish.

Example:

```
remote addHostMapping 192.168.207.40 192.168.207.49 10.0.20.11  <remoteName>
remote addHostMapping 192.168.207.93 192.168.207.99 10.0.20.4   <remoteName>
remote addHostMapping 192.168.209.71 192.168.209.80 10.12.14.16 <remoteName>
```

The above entries create three mappings:

```
192.168.207.40 through 192.168.207.49 are mapped to 10.0.20.11 through 10.0.20.20
192.168.207.93 through 192.168.207.99 are mapped to 10.0.20.4 through 10.0.20.10
192.168.209.71 through 192.168.209.80 are mapped to 10.12.14.16 through 10.12.14.25
```

Range Overlap Rules

With `remote addHostMapping,` private IP address ranges cannot overlap for a remote router.
With `remote addHostMapping`, public IP address ranges cannot overlap for a remote router.

With `system addHostMapping`, private IP address ranges cannot overlap for a system.
With `system addHostMapping`, public IP address ranges cannot overlap for a system.

If a private IP address range for a remote router and a private IP address range for the system overlap, the private IP address range for the remote has precedence.

If a public IP address range for a remote and the public IP address range for the system overlap, the public IP address range for the remote has precedence.

Private IP addresses and public IP addresses can be the same. For example, to enable IP/port translation to a remote router and make the IP addresses 10.1.1.7 through 10.1.1.10 globally visible, it is permissible to use either one of the following commands:

```
remote addHostMapping 10.1.1.7 10.1.1.10 10.1.1.7 <remote>
system addHostMapping 10.1.1.7 10.1.1.10 10.1.1.7
```

If the remapped host's IP address (classic NAT, one-to-one IP address translation) and the "masquerading" IP address (many-to-one IP address translation) are the same, then NAT masquerading has precedence over classic NAT.

Management Security

With the following security control features, the user can prevent the router from being remotely managed via Telnet and/or SNMP. Disabling SNMP will stop the Configuration Manager from accessing the router. In some environments this is desirable.

Disable Telnet and SNMP

To completely disable remote management, the following commands should be entered from the command line.

```
login admin
system telnetport disable
system snmpport disable
save
reboot
```

Restore Telnet and SNMP

In order to reestablish the Telnet and SNMP services, you should restore the default values with the commands:

```
system telnetport default
system snmpport default
```

Validation of Telnet and SNMP clients

This feature is used to validate Telnet or SNMP clients. The following commands are used to define a range of IP addresses that are allowed to access the router via Telnet or SNMP. Only the IP addresses in the range specified for Telnet or SNMP can access the router via Telnet or SNMP. This validation feature is **off** by default.

```
System addtelnetFilter <first ip addr> [<last ip addr>]
System addsnmpFilter <first ip addr> [<last ip addr>]
```

Where:

first ip addr	First IP address of the client range
last ip addr	Last IP address of the client range. May be omitted if the range contains only one IP address.

Example: `system addsnmpfilter 192.168.1.5  192.168.1.12`

Multiple range can be specified for Telnet and SNMP clients. If no range is defined, then access to the router is through the LAN or WAN.

Note 1: These commands do not require a reboot and are effective immediately.

Note 2: To list the range of allowed clients, use the command `system list` when logged in with read and write permission (log in with password).

Restrict Remote Access

To allow management via SNMP or Telnet, while making it more difficult for non-authorized personnel to access the router, the Telnet and SNMP ports may be redefined to a non well-known value. When Network Address Translation (NAT) is used, this port redefinition feature also allows to continue using the standard Telnet and SNMP ports with another device on the LAN (provided the appropriate NAT server ports commands are issued), while simultaneously managing the router (with non-standard ports). The following commands show how this is done:

```
login admin
system telnetport 4321
system snmpport  3214
```

Changing the SNMP Community Name

Changing the SNMP community name from its default value of “public” to another string may further enhance SNMP security. This string then acts like a password, but this password is sent in the clear over the WAN/LAN, in accordance with the SNMP specification.

The SNMP community name is changed using the following commands:

```
login admin
system community <snmp community name>  --  eg: system community fred
save
reboot
```

Disable WAN Management

It may be desirable to allow management of the router on the local LAN, but not over the WAN Network. If the router has been configured to use NAT, then by defining two servers, that DO NOT exist, on the LAN side to handle WAN SNMP and Telnet requests, WAN management of the router cannot occur. The following commands show how this could be done.

```
login admin
system addServer 192.168.254.128 udp snmp  - no computer at 192.168.254.128
system addServer 192.168.254.128 tcp telnet
save
reboot
```

Chapter 5. Command Line Interface Reference

Command Line Interface Conventions

Command Input

The router Command Line Interface follows these conventions:

- Command line length may be up to 120 characters long.
- The Command Line Interface is not case-sensitive except for passwords and router names.
- Items that appear in bold type must be typed exactly as they appear.
  However, commands can be shortened to just those characters necessary to make the command unique.
- Items that appear in italic are placeholders representing specific information that you supply.
- Parameters in between characters < and > must be entered.
- Parameters in between characters [and] are optional.
- All commands are positional; i.e. each keyword/parameter must be entered in the order displayed.

Command Output

After execution of most commands, the system will return either of the following command prompts:

when you are logged in as an administrator, to indicate the end of command execution.

> to indicate the end of command execution when not logged in

Sample responses are shown in this chapter. In many cases, only the command prompt is returned. If you have not entered the correct parameters, the syntax of the command is displayed.

Command Organization

The commands are organized as follows:

- **System-level commands**
- **Router configuration commands:**
  System
  Eth

Remote
ADSL
ATM
HDSL
ISDN
SDSL
DHCP
Filters
Save
Erase

- **File system commands**

? or HELP

Lists the commands at the current level as well as subcommands. At the lowest level of the subcommand, entering a **?** may return the syntax of the command. Note that some commands require a character string and the **?** will be taken as the character string if entered in that position.

? or **HELP**

Example: **# ?**

Top-level commands:

```
?                   help                version
filter              login               logout
exit                reboot              mem
ps                  copy                dir
delete              rename              format
sync                msfs                ifs
ipifs               iproutes            ipxroutes
ipxsaps             bi                  system
eth                 save                erase
remote              call                ping
dhcp                atm
```

System Level Commands

These commands are online action and status commands. They allow you to perform the following functions:

- log into and log out of configuration update mode
- display the router's configuration, the version and level numbers
- list running tasks, memory, communication interfaces
- connect to a remote router to test the line
- list IP routes, and IPX routes and SAPs, root bridge
- save the new configuration image
- reboot the system

BI

Lists the root bridge.

bi

Response:

```
# bi
GROUP 0Our ID=8000+00206f0249fc Root ID=8000+00206f0249fc
Port ETHERNET/0       00+00 FORWARDING
```

BI LIST

Lists MAC addresses and corresponding bridge ports as learned by the bridge function. This list includes several flags and the number of seconds elapsed since the last packet was received by the MAC address.

bi list

Response:

```
# bi list
BRIDGE GROUP 0:
00206F0249FC: P     US    SD A
0180C2000000: P              A        MC
FFFFFFFFFFFF: P FLD          A        BC
00206F024A4F: ETHERNET/0         1                  FWD
00A024C6C594: ETHERNET/0         1                  FWD
00206F200008: ETHERNET/0         1                  FWD
0020AFC5697F: ETHERNET/0        11                  FWD
```

EXIT

Has the same function as Logout, but will disconnect you from a Telnet session.

exit

IFS

Lists the communications interfaces installed in the router and the status of the interfaces.

ifs

Response:

```
# ifs
Interface   Speed      In %     Out % Protocol     State      Connection
ETHERNET/0 10.0mb     0%/0%     0%/0% (Ethernet)   OPENED
ATM_VC/1   25.6mb     0%/0%     0%/0% (CLEAR)      OPENED     to HQ
ATM-25/0   25.6mb     0%/0%     0%/0% (ATM)        OPENED
CONSOLE/0  9600 b     0%/0%     0%/0% (TTY)        OPENED
>
```

IPIFS

Lists the IP interface.

ipifs

Response:

```
ATM_VC/1      192.168.254.1 (FFFFFF00) dest 192.168.254.2 sub 192.168.254.0
              net 192.168.254.0 (FFFFFF00) P-2-P
ETHERNET/0    192.84.210.12 (FFFFFF00) dest 0.0.0.0 sub 192.84.210.0
              net 192.84.210.0 (FFFFFF00) BROADCAST
```

IPROUTES

Lists the current entries in the IP routing table.

iproutes

Response:

```
# iproutes
    IP route   /  Mask   --> Gateway         Interface    Hops Flags

0.0.0.0        /ffffffff --> 0.0.0.0         [none]       0 NW PRIV
192.84.210.0   /ffffff00 --> 0.0.0.0         ETHERNET/0   1 NW FW DIR PERM
192.84.210.12  /ffffffff --> 0.0.0.0         ETHERNET/0   0 ME
192.168.254.0  /ffffff00 --> 0.0.0.0         [none]       0 NW PRIV
192.168.254.1  /ffffffff --> HQ              ATM_VC/1     0 ME
192.168.254.2  /ffffffff --> HQ              ATM_VC/1     1 FW DIR PRIV
224.0.0.9      /ffffffff --> 0.0.0.0         [none]       0 ME
255.255.255.255/ffffffff --> 0.0.0.0         [none]       0 NW PERM
```

where:

```
NW      Network
PERM    Permanent (static)
DOD     Initiate Link dial-up
FW      Forward
DIR     Direct
ME      his Router
```

IPXROUTES

Lists the current entries in the IPX routing table.

ipxroutes

Response:

```
# ipxroutes
Network      Gateway      Interface      Hops Ticks Flags
00001001:    HQ              [down]       1     4    STATIC FORWARD DOD
00000456:   (DIRECT)      ETHERNET/0      0     1    FORWARD
```

where:

```
STATIC   Static Route
DOD      Initiate Link dial-up
FORWARD
DIRECT
```

IPXSAPS

Lists the current services in the IPX SAPs table.

ipxsaps

Response:

```
# ipxsaps
Service Name                          Type  Node number  Network Skt  Hops
SERV312_FP                             4   000000000001:00001001:045   1
```

LOGIN

Login is required whenever you intend to change any configuration settings or save an entire new configuration.

login <*password*>

password Mandatory password set using the ‘system admin’ command or default (`admin`). If not specified, you will be shown the command syntax. The password is case-sensitive.

Response:

```
Logged in successfully!
     or
Wrong password!  Try logging in again.
```

After successfully logging in, the ‘#’ is used as the prompt character to indicate that you are logged in as an administrator.

LOGOUT

Logs out to reinstate administrative security after you have completed changing the router’s configuration.

logout

MEM

Lists memory and buffer usage.

mem

Response:

```
# mem
Small buffers used.......  18 (7% of 256 used)
Large buffers used.......  41 (16% of 256 used)
Buffer descriptors used..  59 (7% of 768 used)
Number of waiters s/l....   0/0

Table memory allocation statistics:
Sizes     16    32    64   128   256   512  1024  2048
Used      34    18    12     3     8     9     8     7
Free       3     1     4     0     1     1     1     1

Sizes   4096  8192
Used       3     1
Free       1     0
Total in use: 51936, total free: 857368 (8272 + 849096)
```

MLP SUMMARY

Lists the status of the any protocols negotiated for an active remote connection. The following lists the most common protocols:

- MLP (PPP Link Protocol)
- IPNCP (IP routing Network Protocol)
- CCP (Compression Network Protocol)
- BNCP (Bridging Network Protocol)
- IPXCP (IPX Network Protocol)

"Open" indicates that the protocol is in ready state.
"Stopped" means that the protocol is defined but did not successfully negotiate with the remote end.
No message means that that the link is not active.

mlp summary

Example: `mlp summary`

PING

An echo message, available within the TCP/IP protocol suite, sent to a remote node and returned; it is used to test connectivity to the remote node and is particularly useful for locating connection problems on a network. By default, the router will try to "ping" the remote device for five consecutive times and will issue status messages.

ping [**-c count**] [**-i wait**] [**- s size** (or **-l size**)] *<ipAddr>*

Options are:

-c count Number of packets; count is a value between 1 and 10.

-i wait Wait period in seconds between packets; wait is a value between 1 and 10.

-s size Packet data length “size” bytes; size is a value between 0 and 972.
-l size Same as -s size

ipAddr IP address in the format of 4 decimals separated by periods.

Example: ping -c 8 -i 7 -s 34 192.168.254.2

Response:

```
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: packets sent 8, packets received 8
```

PS

Lists all of the tasks (processes) running in the system and the status of the tasks.

ps

Response:

```
# ps
TID:          NAME                FL P BOTTOM CURRENT SIZE
  1:IDLE                          02 7 1208f0  121008 2032
  3:MSFS_SYNC                     03 6 1224a0  122ba8 2032
  4:SYSTEM LOGGER                 03 5 122cd0  1233d8 2032
  5:LL_PPP                        03 5 126750  126e58 2032
  6:NL_IP                         03 5 126fe0  1272e0 1000
  7:TL_IP_UDP                     03 3 127460  127768 1000
  8:TL_IP_TCP                     03 3 1278c0  127fd0 2032
  9:IP_RIP                        03 4 128120  128420 1000
 10:TELNETD                       03 5 128550  128838 1000
 11:DUM                           03 5 12b580  12bc88 2032
 12:ATM25                         03 1 12c0a0  12c790 2032
 13:SNMPD                         03 5 124b60  125a70 4080
 14:BOOTP                         03 5 12e3d0  12e6c0 1000
 15:CMD                           01 6 12cba0  12d9f8 4080
```

TID: task ID field
NAME: name of the task
FL: flag field
P: number from 1 to 7 with the highest priority equal to 1.
BOTTOM : address of the task stack
CURRENT: current stack pointer
SIZE: stack size in byte

REBOOT

This command causes a reboot of the system. You must perform a reboot after you have configured the router the first time or when you modify the configuration. Reboot is *always* required when the following configuration settings are modified:

- System Settings Ethernet IP Address
- Ethernet IPX Network Number
- TCP/IP and IPX Routing
- Remote Router Default Bridging Destination
- TCP/IP Route Addresses
- IPX Routes
- SAPs and Bridging

Reboot is also required when adding a new remote entry in the remote database.

Reboot also ensures that all file system updates are completed. There is a time lag between the '**`save...`**' commands and the time the data is safely stored in FLASH memory. If the power goes off during this time, data can be lost. Always reboot before powering off the router. Alternatively, use the **sync** command.
CAUTION: This command erases all of the configuration data in the router.

reboot <*default*>

default This option deletes the system configuration file, and restores the router to its original defaults (before any configuration was entered).

NOTE: *Default* must be fully spelled out.

Response:

```
# reboot

Syncing filesystems.....done.FlowPoint-2000 BOOT/POST V3.0.0 (12-Dec-97 18:10)
Copyright (c) 1994-1998, FlowPoint Corporation.
Copyright (c) 1985-1995, MPX Data Systems, Inc.
All rights reserved.

Board revision:................. 2
General Purpose timers:......... OK
CRC check (75FF4BF2):........... OK
Amount of FLASH installed:...... 1024 Kbytes
Amount of RAM installed:........ 2048 Kbytes
RAM address test:............... OK
RAM running 1111s test:......... OK
RAM pattern test:............... OK
RAM Byte/Word access:........... OK
Real-Time Clock:................ OK
Battery-backed RAM ............. OK
SCC ports in HDLC loopback mode: OK
Ethernet loopback mode:......... OK
Interrupts:..................... OK
Detecting Optional Hardware .... Type 8 Rev 0

POST summary: successful
```

```
Initializing the system RAM ... done
Initializing optional hardware: "lock_idreg"
Hardware Type 8 Rev 0 successfully initialized -- ID: DAD7
Today is Wednesday January 7, 1998; the time is 13:29:36
My MAC address is: 00:20:6F:02:AC:0D
Reason for this reset: reboot command

Trying to boot from flash memory

loading ..................................done.
Verifying CRC (2515443C).....................done.

FlowPoint Model 2025-O (P/N 901-20038-01), Rev 1 (S/N 175117)
Now 1355k free before buffers
Interfaces detected
   LAN: Ethernet (10BASE-T)   WAN: ATM-25 (00000001)


FlowPoint/2025 ATM25 Router
Copyright (c) 1995-1998 FlowPoint Corp.
Copyright (c) 1985-1996 MPX Data Systems, Inc.
All Rights Reserved

INIT: buffer pool is 485424 bytes
ETHERNET/0 interface started, MAC=00:20:6F:02:AC:0D
01/07/1998-13:29:40:DOD: connecting to HQ @ 0*38 over ATM_VC/1

FlowPoint/2025 ATM25 Router.
```

VERS

Displays the software version level, source, and amount of elapsed time the router has been running.

vers

Response:

```
FlowPoint/2025 ATM25 Router
FlowPoint-2000 BOOT/POST V3.0.0 (12-Dec-97 18:10)
Software version1.1.2 (10 built Wed Jan 7 13:17:37 PST 1998
Options: ATM25, IP, IPX, IP TRANS, DHCP

Up for 0 days 0 hours 20 minutes (started 1/7/1998 at 13:29)
```

Router Configuration Commands

Configuration commands are used to set configuration information for each functional capability of the router. Each functional capability has a specific prefix for its associated commands:

- **system**: target router system commands
- **eth ip**: Ethernet IP routing commands
- **remote**: remote router database commands
- **adsl** Asymmetric Digital Subscriber Line commands (ADSL routers only)
- **atm:** Asynchronous Transfer Mode commands (ATM routers only)
- **hdsl** High-speed Digital Subscriber Line commands (HDSL routers only)
- **isdn** ISDN Digital Subscriber Line (IDSL routers only)
- **sdsl** Symmetric Digital Subscriber Line commands (SDSL routers only)
- **dhcp:** Dynamic Host Configuration Protocol commands
- **save**: save configuration to FLASH memory commands
- **filter**: filtering commands
- **? or help**: summary of available commands

Target Router System Configuration Commands (SYSTEM)

The following commands set basic router configuration information:

- name of the router
- optional system message
- authentication password
- security authentication protocol
- management security
- system administration password
- translate IP address
- NAT configuration

SYSTEM ?

Lists the supported keywords.

system ?

Response:

```
?                   msg                 name
passwd              authen              community
list                admin               history
log                 addServer           delServer
bootpServer         supportTrace        telnetport
snmpport            wan2wanforwarding   addUDPrelay
delUDPrelay
```

SYSTEM ADMIN

Sets the administration password used to control write access to the target router configuration.

system admin <*password*>

password Write-enable login password

Example: `system admin adx1lp`

SYSTEM ADDSERVER

This Network Address Translation (NAT) command is used to configure a local IP address as the particular server on the LAN (FTP, SMTP, etc.) for the global configuration.

system addServer <*ipAddr*> <*protocolid*>|*tcp*|*udp* <*port*>|*ftp*|*telnet*|*smtp*|*snmp*|*http*

ipAddr IP address of the host selected as server in the format in the format of 4 decimals separated by periods

protocolid Protocol used by the selected server.
Can be **tcp** or **udp,** or a numeric value.

port Port used by the selected server.
Can be a string such as **ftp, telnet, smtp, snmp,** or **http**, or a numeric value between 0 and 65,535.
A numeric value of 0 will match any port

Example: `system addServer 192.168.1.5 tcp smtp`

SYSTEM ADDSNMPFILTER

This command is used to validate SNMP clients by defining a range of IP addresses that are allowed to access the router via SNMP. This validation feature is **off** by default.

Note 1: This command does not require a reboot and is effective immediately.

Note 2: To list the range of allowed clients, use the command `system list` when logged in with read and write permission (log in with password).

system addsnmpFilter *<first ip addr>* [*<last ip addr>*]

first ip addr First IP address of the client range
last ip addr Last IP address of the client range. May be omitted if the range contains only one IP address.

Example: `system addsnmpfilter 192.168.1.5  192.168.1.12`

SYSTEM ADDTELNETFILTER

This command is used to validate Telnet clients by defining a range of IP addresses that are allowed to access the router via Telnet. This validation feature is **off** by default.

Note 1: This command does not require a reboot and is effective immediately.

Note 2: To list the range of allowed clients, use the command `system list` when logged in with read and write permission (log in with password).

system addtelnetFilter *<first ip addr>* [*<last ip addr>*]

first ip addr First IP address of the client range
last ip addr Last IP address of the client range. May be omitted if the range contains only one IP address.

Example: `system addtelnetfilter 192.168.1.5  192.168.1.12`

SYSTEM ADDUDPRELAY

This command is used to create a UDP port range for packet forwarding. You can specify a port range from 0 to 65535. 137 to 139 are reserved for Netbios ports. Overlap of UDP ports is not allowed.

system addUDPrelay *<ipaddr> <first port>|all [<last port>]*

ipAddr IP address of the server to which the UDP packet will be forwarded.
first port First port in the UDP port range to be created.

all Incorporates all the available UDP ports in the new range

last port Last port in the UDP port range to be created

Example: `system addudprelay 192.168.1.5 all`

SYSTEM AUTHEN

Forces the target router authentication protocol used for security negotiation with the remote routers when setting the local side authentication. You should not need to issue this command as the best security possible is provided with the **none** default.

system authen none | pap | chap

none When set to **none** (the default), the authentication protocol is negotiated, with the minimum best security level as defined for each remote router in the database.

pap When set to **pap**, negotiation will begin with PAP (instead of CHAP) for those entries that have PAP in the remote database and only when the call is initiated locally.

chap Overrides all the remote database entries with **chap**; i.e., only CHAP will be performed.

Example: `system authen CHAP`

SYSTEM BOOTPSERVER

Lets the router relay BootP or DHCP requests to a DHCP server on the WAN, when a PC attempts to acquire an IP address using DHCP. This command disables the router's DHCP server.

system bootpserver <*ipAddr*>

ipAddr IP address of the target router in the format of 4 decimals separated by periods.

Example: `system bootpserver 128.1.210.64`

SYSTEM COMMUNITY

This command is used to enhance SNMP security. It allows the user to change the SNMP community name from its default value of "public" to a different value. Refer to chapter 3, *Advanced Features - Management Security*.

Note: The command `system community` (with no value) will display the current community name.

system community [<*SNMP community name*>]

SNMP community name String of up to 40 characters

Example 1: `system community fred`
Example 2: `system community`

SYSTEM DELSERVER

This Network Address Translation (NAT) command is used to delete an entry created by the `system addServer` command.

system delServer <*ipAddr*> <*protocolid*>|*tcp*|*udp* <*port*>|*ftp*|*telnet*|*smtp*|*snmp*|*http*

ipAddr IP address of the host selected as server in the format of 4 decimals separated by periods

protocolid Protocol used by the selected server;
Can be **tcp** or **udp** or a numeric value.

port Port used by the selected server;
Can be a string such as **ftp, telnet, smtp, snmp,** or **http,** or a numeric value between 0 and 65,535.

Example: `system delServer 192.168.1.5 tcp smtp`

SYSTEM DELSNMPFILTER

This command deletes the client range previously defined by the command system `addsnmpfilter`.

Note 1: This command does not require a reboot and is effective immediately.

Note 2: To list the range of allowed clients, use the command system list when logged in with read and write permission (log in with password).

system delsnmpFilter <*first ip addr*> [<*last ip addr*>]

first ip addr First IP address of the client range
last ip addr Last IP address of the client range. May be omitted if the range contains only one IP address.

Example: `system delsnmpfilter 192.168.1.5  192.168.1.12`

SYSTEM DELTELNETFILTER

This command deletes the client range previously defined by the command system `addtelnetfilter`.

Note 1: This command does not require a reboot and is effective immediately.

Note 2: To list the range of allowed clients, use the command system list when logged in with read and write permission (log in with password).

system deltelnetFilter <*first ip addr*> [<*last ip addr*>]

first ip addr First IP address in the client range
last ip addr Last IP address in the client range. May be omitted if the range contains only one IP address.

Example: `system deltelnetfilter 192.168.1.5  192.168.1.12`

SYSTEM DELUDPRELAY

This command deletes the port range that was previously enabled by the command: `system addUDPrelay.`

system delUDPrelay <*ipaddr*> <*first port*>| *all [*<*last port*>*]*

ipAddr IP address of the server

first port First port in the UDP port range to be deleted

all Deletes all existing UDP ports

last port Last port in the UDP port range to be deleted

Example: `system deludprelay 192.168.1.5 all`

SYSTEM HISTORY

Displays the router's most recent console log.

system history

Example: `system history`

SYSTEM LIST

Lists the target router's system name, security authentication protocol, callerID and 'data as voice' status, and system message.

system list

Example: `system list`

Response:

```
GENERAL INFORMATION FOR <SOHO>

System started on..................... 1/7/1998 at 13:29
  Authentication override............. NONE
WAN to WAN Forwarding................ yes
  BOOTP/DHCP Server address........... none
  Telnet Port......................... default (23)
SNMP Port........................... default (161)
System message: Configured January 1998
```

SYSTEM LOG

Allows to log the router's activity in a TELNET session.

system log start | stop | status

start Used to monitor the router activity at all time

Example: `system log start`

status Used to find out if other users (yourself included) are using this utility

Example: `system log status`

stop Use to discontinue the logging utility at the console

Example: `system log stop`

SYSTEM MSG

Sets a message that is saved in the target router you are configuring.

system msg <*message*>

Message Message (character string) — Space characters are not allowed within the message; you may use underscore characters instead. If you do not enter a message, the current message is displayed. The message must be no more than 255 characters.

Example: `system msg Configured _on_ 1/21/98`

SYSTEM NAME

Sets the name for the target router that you are configuring. You are required to assign a name to the target router. This name is sent to a remote router during PAP/CHAP authentication.

system name <*name*>

name Name of the target router (character string). Space characters are not allowed within the name; you may use underscore characters instead. (The system name is a 'word' when exchanged with PAP/CHAP.) If you do not enter a name, the current name of the router is displayed. If you type anything after **system name**, the characters will be taken as the new name.

NOTE: the system name is case-sensitive and must be no more than 50 characters.

Example: `system name Router1`

SYSTEM PASSWD

Sets the target router system authentication password used when the router connects to other routers or is challenged by them. This password is a default password used for all remote sites, unless a unique password is explicitly defined for connecting to a remote router with the **remote setOurPasswd** command.

system passwd <*password*>

password Authentication password of the target router.
NOTE: The password is case-sensitive and should be no more than 40 characters.

Example: `system passwd chwgn1`

SYSTEM TELNETPORT

The router has a built-in Telnet server. This command is used to specify which router's TCP port is to receive a Telnet connection. Refer to *Advanced Features - Management Security* in Chapter 3.

NOTE: This command requires a save and reboot to take effect.

system telnetport *default* | *disabled* | *<port>*

default The default value is 23.

disabled The router will not accept any incoming TCP request.

port Port number of the Ethernet LAN. It is recommended that this number be > 2048 if not 0 (disabled) or 23 (default).

Examples:
```
system telnetport default
system telnetport disabled
system telnetport 3333
```

SYSTEM SNMPPORT

This command is used to manage SNMP port access; this includes disabling SNMP, reestablishing SNMP services, or redefining the SNMP port for security reasons. Refer to *Advanced Features - Management Security* in Chapter 3.

NOTE: This command requires a save and reboot to take effect.

system snmpport *default* | *disabled* | *<port>*

default Restores the default values to 161

disabled Disables remote management.

port Used to definea new SNMP port number.
Use this option to redefine the SNMP port to a non well-known value to restrict remote access.

Examples:
```
system snmpport default
system snmpport disabled
system snmpport 3333
```

SYSTEM SUPPORTTRACE

This command lets you capture to a file all of the configuration data that Technical Support may need to investigate configuration problems. This exhaustive list command incorporates the following commands:

- system history
- vers
- mem
- system list
- eth list
- dhcp list (if DHCP is enabled)
- remote list
- ifs
- bi (if bridging)
- ipifs
- iproutes
- ipxroutes

system supporttrace

Example: `system supporttrace`

SYSTEM WAN2WANFORWARDING

This command allows the user to manage WAN-to-WAN forwarding of data from one WAN link to another. For example, if the router is used at home to access both a company network and the Internet at the same time, and it is desirable that company information not pass to the Internet, then disable WAN-to-WAN forwarding.

system wan2wanforwarding on|off

on Used to allow data to be forwarded from one WAN link to another link.

off Used to stop the data from being forwarded fron one WAN link to another WAN link.

Example: `system wan2wanforwarding on`

Target Router Ethernet LAN Bridging and Routing (ETH)

The following commands allow you to:

- Set the Ethernet LAN IP address
- List the current contents of the IP routing table
- Enable and disable IP routing
- List or save the current configuration settings

All of these commands will require a reboot.

ETH ?

Lists the supported keywords.

eth ?

Examples: `eth ?`
`eth ip ?`

Response:

```
Eth commands:
?                   ip                  ipx
list


eth ip sub-commands
?                   addr
ripmulticast        options             enable
disable             firewall            addroute
delroute            defgateway
```

ETH IP ADDR

Sets the IP address, subnet mask, and port number for the Ethernet LAN connection. After entering this command, Ethernet LAN IP routing is disabled.

eth ip addr <*ipAddr*> <*ipNetMask*> [*port#*]

ipAddr Ethernet LAN IP address, in the format of 4 decimals separated by periods.

ipNetMask IP network mask, in the format of 4 decimals separated by periods.

port# Port number of the Ethernet LAN. This number must be 0 (default) or may be omitted.

Example: `eth ip 128.1.2.0 255.255.255.0`

ETH IP ADDROUTE

Allows to define IP routes reached via the LAN interface. It is only needed if the system does not support RIP.

NOTE: This command requires a reboot.

eth ip addRoute <*ipAddr*> <*ipNetMask*> <*gateway*> <*hops*> [<port#>]

ipAddr Ethernet LAN IP address in the format of 4 decimals separated by periods.

IpNetMask IP network mask in the format of 4 decimals separated by periods.

gateway IP address in the format of 4 decimals separated by periods.

hops Number of routers through which the packet must go to get to its destination.

port# Port number of the Ethernet LAN; must be zero or omitted.

Example: `eth IP AddRoute 128.1.2.0 255.255.255.0 128.1.1.17 1`

ETH IP DEFGATEWAY

Lets you assign an Ethernet default gateway for packets that do not have a destination specified. This setting is most useful when IP routing is not enabled, in which case the system acts as an IP host (i.e. an end system, as opposed to an IP router).

NOTE: This command requires a reboot; it is also an alternative to:

```
eth IP AddRoute 0.0.0.0 255.255.255.0 <gateway> 1
```

eth ip defgateway <*ipAddr*>

ipAddr Ethernet Lan IP address in the format of 4 decimals separated by periods.

Example: `eth ip defgateway 128.1.210.65`

ETH IP DISABLE

Disables IP routing across the Ethernet LAN. This acts as a master switch allowing you to disable IP Routing for testing or control purposes.

NOTE: A reboot is required after this command.

eth ip dis(**able**) [*port#*]

port# Port number of the Ethernet LAN. This number must be 0 or may be omitted.
Example: `eth ip disable`

ETH IP ENABLE

Enables IP routing across the Ethernet LAN. This acts as a master switch allowing you to enable IP routing.

eth ip enable [*port#*]

port# Port number of the Ethernet LAN. This number must be 0 or may be omitted.

Example: `eth ip enable`

ETH IP FIREWALL

The router supports 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 that have a source IP address recognized as a local LAN address. This command requires a reboot.
This command sets Ethernet Firewall Filtering ON or OFF and allows you to list the active state.

NOTE: To perform Firewall Filtering, IP routing must be enabled.

eth ip firewall on | off | list

on Sets firewall filtering on. IP routing must also be enabled for filtering to be performed.

off Sets firewall filtering off.

list Lists the current status of firewall filtering.

Example: `eth ip firewall list`

Response:
```
The Internet firewall filter is currently on.
0 offending packets were filtered out.
```

ETH IP OPTIONS

RIP is a protocol used for exchanging IP routing information among routers. The following RIP options allow you to set IP routing information protocol controls on the local Ethernet LAN.

NOTE: This command requires a reboot.

eth ip options <*option*> on | off <port#>

option Must be one of the following:

rxrip Receive and process IP RIP-1 compatible and RIP-2 broadcast packets from the Ethernet LAN. Also receive and process RIP-2 packets that are multicast as defined by the **`eth ip ripmulticast`** command.

Set this option if the local router is to discover route information from the Ethernet LAN. This defaults to **ON**.

rxrip1 Receive and process RIP-1 packets only.

rxrip2 Receive and process RIP-2 packets only.

rxdef Receive the default route address from the Ethernet LAN. This defaults to **ON**. This option is useful if you do not want to configure your router with a default route.

txrip Transmit RIP-1 compatible broadcast packets and RIP-2 multicast packets over the Ethernet LAN. This defaults to **ON**.

txrip1 Transmit broadcast RIP-1 packets only.

txrip2 Transmit multicast RIP-2 packets only.

txdef/avdfr Advertise this router as the default router over the Ethernet LAN (provided it has a default route!). This default is set to ON. Set this to OFF if another router on the local LAN is the default router.

Example: `eth ip options avdfr off`

ETH IP RIPMULTICAST

This commands lets you change the multicast address for RIP-1 compatible and RIP-2 packets. The default address is 224.0.0.9.

eth ip ripmulticast <*IpNet*>

IpNet IP address of the remote network or station, in the format of 4 decimals separated by periods.

Example: `eth ip ripmulticast 128.1.210.64`

ETH IPX ADDR

Sets the IPX network number for the Ethernet LAN connection.

eth ipx addr <*ipxNet#*> [*port#*]

ipxNet# IPX network number represented by 8 hexadecimal characters.

port# Port number of the Ethernet LAN. This number must be 0 or may be omitted.

Example: `eth ipx 123`

ETH IPX DISABLE

Disables IPX routing across the Ethernet LAN. This acts as a master switch allowing you to disable IPX Routing for testing or control purposes.

NOTE: This command requires a reboot.

eth ipx disable [*port#*]

port# Port number of the Ethernet LAN. This number must be 0 or may be omitted.

Example: `eth ipx disable`

ETH IPX ENABLE

Enables IPX routing across the Ethernet LAN. This acts as a master switch allowing you to enable IPX routing.

NOTE: This command requires a reboot.

eth ipx enable [*port#*]

port# Port number of the Ethernet LAN. This number must be 0 or may be omitted.

Example: `eth ipx enable`

ETH IPX FRAME

Sets the frame encapsulation method. The default is 802.2.

eth ipx frame <*type*>

type Choice of:

802.2 (DEC standard)
802.3 (Intel standard)
dix (Xerox/Ethernet II standard)

Example: `eth ipx frame 802.3`

ETH LIST

Lists the Ethernet LAN port number, status of bridging and routing, IP protocol controls, and IP address and subnet mask.

eth list

Example: `eth list`

Response:

```
ETHERNET INFORMATION FOR <ETHERNET/0>
  Hardware MAC address................ 00:20:6F:02:98:04
  Bridging enabled.................... no
  IP Routing enabled.................. no
    Firewall filter enabled ........... yes
    Send IP RIP to the LAN............. rip-1 compatible
      Advertise me as default router... yes
    Process IP RIP packets received.... rip-1 compatible
      Receive default route by RIP..... yes
  RIP Multicast address............... default
  IP address/subnet mask.............. 192.168.254.254/255.255.255.0
  IP static default gateway........... none
  IPX Routing enabled................. no
    External network number............ 00000000
    Frame type......................... 802.2
```

Remote Router Access Configuration (REMOTE)

The following commands allow you to add, delete, and modify remote routers to which the target router can connect. Remote router information that can be configured includes:

- PVC numbers
- security authentication protocols and passwords
- WAN IP/ IPX addresses
- IP routes
- IPX routes and SAPS
- remote bridging addresses and bridging control

REMOTE ?

Lists the supported keywords.

remote ?

Response:

```
Sub-commands for remote:
?                   help                add
del                 list                enable
disable             setAuthen           enaAuthen
disAuthen           setPasswd           setOurPasswd
delOurPasswd        setOurSysName       delOurSysName
listPhones          setPVC              setProtocol
addServer           delServer           setIPTranslate
setCompression      stats               statsclear
setSrcIpAddr        setRmtIpAddr        addIproute
delIproute          setIpOptions        listIproutes
setIpxaddr          addIpxroute         delIpxroute
listIpxroutes       addIpxsap           delIpxsap
listIpxsaps         listBridge          enaBridge
disBridge           setBrOptions
```

REMOTE ADD

Adds a remote router entry into the remote router database.

remote add *<remoteName>*

remoteName Name of the remote router (character string). The name is case-sensitive.

Example: `remote add HQ`

REMOTE ADDIPROUTE

Adds an IP address route for a network or station on the LAN network connected beyond the remote router. The target router's routing table must be seeded statically to access networks and stations beyond this remote router. After the connection is established, standard RIP update packets will dynamically add to the routing table. Setting this address is not required if a target router never connects to the remote router and the remote router supports RIP.

NOTE: A **reboot** must be performed on the target router for the addition of a static route to take effect.

remote addIpRoute *<ipNet> <ipNetMask> <hops> <ipGateway> <remoteName>*

ipNet IP address of the remote network or station, in the format of 4 decimals separated by periods.

ipNetMask IP network mask of the remote network or station, in the format of 4 decimals separated by periods.

hops Number between 1 and 15 that represents the perceived cost in reaching the remote network or station.

IpGateway Enter a gateway address only if you are configuring RFC 1483MER. The gateway address that you enter is the address of a router on the remote LAN. Check with your system administrator for details.

remoteName Name of the remote router (character string)

Examples:

```
remote addIpRoute 128.1.210.64  255.255.255.192  1 HQ

remote addIpRoute 128.1.210.032 255.255.255.224 1 HQ
remote addIpRoute 128.1.206.0 255.255.255.0 2 HQ
remote addIpRoute 128.1.210.072 255.255.255.255 1 HQ
remote addIpRoute 0.0.0.0 255.255.255.255 1 HQ
remote addIproute 0.0.0.0 255.255.255.255 1 187.12.10.1 HQ
```

The first two addresses in the list represent subnetworks, the third is a class B network, and the fourth is a host. The fifth address is the default route.

REMOTE ADDIPXROUTE

Adds an IPX route for a network or station on the LAN network connected beyond the remote router. The target router's routing information table must be seeded statically to access networks and stations beyond this remote router. After the connection is established, standard RIP update packets will dynamically add to the routing table. (Setting this address is not required if a target router never connects to the remote router and the remote router supports RIP.)
NOTE: A **reboot** must be performed on the target router for the addition of a static route to take effect.

remote addIpxRoute *<ipxNet#> <hops> <ticks> <remoteName>*

ipxNet# IPX network number represented by 8 hexadecimal characters.

hops Number of routers through which the packet must go to get to the network/station.

ticks Number in 1/8 seconds which is the estimated time delay in reaching the remote network or station.

remoteName Name of the remote router (character string)

Example: `remote addIpxRoute 456 1 4 HQ`

REMOTE ADDIPXSAP

Adds an IPX SAP to the server information table for a service on the LAN network connected beyond the remote router. The target router's SAP table must be seeded statically to access services beyond this remote router. After the connection is established, standard SAP broadcast packets will dynamically add to the table.

NOTE: A **reboot** must be performed on the target router for the addition of a SAP to take effect.

remote addIpxSap *<serviceName> <ipxNet #> <ipxNodeAddr> <sockets> <serverType> <hops> <remoteName>*

serviceName Name of server

ipxNet# IPX network number represented by 8 hexadecimal characters.

ipxNodeAddr IPX node address represented by 12 hexadecimal characters.

remoteName Name of the remote router (character string).

socket Socket address of the destination process within the destination node. The processes include services such as file and print servers.

serverType Number representing the type of server

hops Number of routers through which the packet must go to get to the network/station.

Example: `remote addIpxSap Fileserver 010a020b 0108030a0b0c 451 HQ`

REMOTE ADDSERVER

This Network Address Translation (NAT) command is used to add a server's IP address (on the LAN) associated with this remote router for a particular protocol.

remote addServer *<ipAddr> <protocolid>|tcp|udp <port>|ftp|telnet|smtp|snmp|http <remoteName>*

ipAddr IP address of the host selected as server in the format of 4 decimals separated by periods

protocolid Protocol used by the selected server; can be **tcp,** or **udp,** or a numeric value.

port Port used by the selected server; can be a string such as **ftp, telnet, smtp, snmp,** or **http**, or a numeric value between 0 and 65,535. A numeric value of 0 will match any port.

remoteName Name of the remote router (character string)

Example: `remote addServer 192.168.1.5 tcp smtp`

REMOTE DEL

Deletes a remote router entry from the remote router database.

remote del *<remoteName>*

remoteName Name of the remote router (character string)

Example: **`remote del HQ`**

REMOTE DELIPROUTE

Deletes an IP address for a network or station on the LAN network connected beyond the remote router.

NOTE: A **reboot** must be performed on the target router for a deletion of a static route to take effect.

remote delIpRoute *<ipNet> <remoteName>*

ipNet IP address of the remote network or station, in the format of 4 decimals separated by periods.

remoteName Name of the remote router (character string)

Example: `remote delIpRoute 128.1.210.64 HQ`

REMOTE DELIPXROUTE

Deletes an IPX address for a network on the LAN network connected beyond the remote router.

NOTE: A **reboot** must be performed on the target router for a deletion of a static route to take effect.

remote delIpxRoute *<ipxNet#> <remoteName>*

ipxNet# IPX network number represented by 8 hexadecimal characters.

remoteName Name of the remote router (character string)

Example: `remote delIpxRoute 010a020b HQ`

REMOTE DELIPXSAP

Deletes an IPX service on the LAN network connected beyond the remote router.

NOTE: A **reboot** must be performed on the target router for a deletion of a service to take effect.

remote delIpxSap *<serviceName#> <remoteName>*

serviceName Name of server

remoteName Name of the remote router (character string)

Example: `remote delIpxSap Fileserver HQ`

REMOTE DELOURPASSWD

Removes the unique CHAP or PAP authentication password entries established by the command **remote setOurPasswd.**

remote delOurPasswd *<remoteName>*

remoteName Name of the remote router (character string)

Example: `remote delOurPasswd HQ`

REMOTE DELOURSYSNAME

Removes the unique CHAP or PAP authentication system name entries established by the command **remote setOurSysName.**

remote delOurSysName <remoteName>

remoteName Name of the remote router (character string)

Example: `remote delOurSysName HQ`

REMOTE DELSERVER

This Network Address Translation (NAT) command is used to delete an entry created by the `remote addServer` command.

remote delServer *<ipAddr> <protocolid>|tcp|udp <port>|ftp|telnet|smtp|snmp|http <remoteName>*

ipAddr IP address of the host selected as server in the format of 4 decimals separated by periods

protocolid Protocol used by the selected server; can be **tcp,** or **udp,** or a numeric value

port Port used by the selected server;
Can be a string such as **ftp, telnet, smtp, snmp,** or **http**, or a numeric value between 0 and 65,535.

remoteName Name of the remote router (character string)

Example: `remote delServer 192.168.1.5 tcp ftp router1`

REMOTE DISABLE

Disables communications with the remote router. This allows you to enter routers into the remote router database but sets them inactive.

NOTE: The routing information defined for <routerName> is still in effect when the entry is disabled until you save and reboot. However, no calls will be made to that remote router.

remote disable *<remoteName>*

remoteName Name of the remote router (character string)

Example: `remote disable HQ`

REMOTE DISAUTHEN

This command is intended for situations where third-party routers are not capable of being authenticated: the target router will not attempt to authenticate the remote router.

remote disAuthen *<remoteName>*

remoteName Name of the remote router (character string)

Example: `remote disAuthen HQ`

REMOTE DISBRIDGE

Disables bridging from the target router to the remote router.

NOTE: This command requires rebooting the target system for the change to take effect.

remote disBridge *<remoteName>*

remoteName Name of the remote router (character string)

Example: `remote disBridge HQ`

REMOTE ENAAUTHEN

With this command the target router will try to negotiate authentication as defined in the remote router's database.

remote enaAuthen *<remoteName>*

remoteName Name of the remote router (character string)

Example: `remote enaauthen HQ`

REMOTE ENABLE

Enables communications with the remote router. This command allows you to activate the entry in the remote router database when you are ready.

remote enable *<remoteName>*

remoteName Name of the remote router (character string)

Example: `remote enable HQ`

REMOTE ENABRIDGE

Enables bridging from the target router to the remote router. This command requires rebooting the target system for the change to take effect.

remote enaBridge <*remoteName*>

remoteName Name of the remote router (character string)

Example: `remote enaBridge HQ`

REMOTE LIST

Lists the remote router entry in the remote router database or all the entries in the database. The result is a complete display of the current configuration settings for the remote router(s), except for the authentication password/secret.

remote list [*remoteName*]

remoteName Name of the remote router (character string)

Example: `remote list HQ`

Response:

```
INFORMATION FOR <HQ>
  Status............................... enabled
  Our Password used when dialing out... no
  Protocol in use...................... RFC1483 (SNAP) - Frame Relay IP
  Connection Identifier (VPI*VCI)...... 0*38
  IP address translation............... off
  Compression Negotiation.............. off
  Source IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Remote IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Send IP RIP to this dest............. no
    Send IP default route if known..... no
  Receive IP RIP from this dest........ no
    Receive IP default route by RIP.... no
  Keep this IP destination private..... yes
  Total IP remote routes............... 1
           128.1.0.0/255.255.0.0/1
  IPX network number................... 00000789
  Total IPX remote routes.............. 1 00001001/1/4
  Total IPX SAPs....................... 1
    SERV312_FP 00001001 00:00:00:00:00:01 0451 0004 1
  Bridging enabled..................... yes
    Exchange spanning tree with dest... no
```

The security authentication protocol is CHAP.
A remote IP network can be accessed through a default route. No bridging is defined for any MAC addresses on the Ethernet LAN and bridging is disabled. A remote IPX network (external) is defined.

If an entry is not in the remote router database for HQ, the response is: `Unknown remote name HQ`

REMOTE LISTBRIDGE

Lists the bridging capability from the target router to the remote router.

remote listBridge [*remoteName*]

remoteName Name of the remote router (character string)

Example: `remote listBridge  HQ`

Response:
```
BRIDGING INFORMATION FOR <HQ>
  Bridging enabled................... yes
  Exchange spanning tree with dest... yes
```

REMOTE LISTIPROUTE

Lists all network or station IP addresses defined for the LAN network connected beyond the remote router. If the remote name is not specified, a list of IP Routes is displayed for each remote router in the database.

remote listIpRoute [*remoteName*]

remoteName Name of the remote router (character string)

Example: `remote listIpRoute HQ`

Response:
```
IP INFORMATION FOR <HQ>
Send IP RIP to this dest.............   rip-1 compatible
    Send IP default route if known..... no
  Receive IP RIP from this dest........ rip-2
    Receive IP default route by RIP.... yes
  Keep this IP destination private..... no
  Total IP remote routes............... 0
```

REMOTE LISTIPXROUTE

Lists all network IPX route addresses defined for the LAN network connected beyond the remote router. The network number, hop count, and ticks are displayed. If the remote name is not specified, a list of IPX routes is displayed for each remote router in the database.

remote listIpxRoute [*remoteName*]

remoteName Name of the remote router (character string)

Example: `remote listIpxRoute HQ`

Response:
```
IPX ROUTE INFORMATION FOR <HQ>
Total IPX remote routes............. 1           00001001/1/4
```

REMOTE LISTIPXSAP

Lists all services defined for the LAN network connected beyond the remote router. Each service includes the server name, network number, node number, socket number, server type, and hop count. If the remote name is not specified, a list of IPX SAPs is displayed for each remote router in the database.

remote listIpxSap [*remoteName*]

remoteName Name of the remote router (character string)

Example: `remote listIpxSap HQ`

Response:

```
  IPX SAP INFORMATION FOR <HQ>
Total IPX SAPs....................... 1
SERV312_FP 00001001 00:00:00:00:00:01 0451 0004 1

IPX SAP INFORMATION FOR <ISP>
Total IPX SAPs....................... 0
   SERV312_FP 00001001 00:00:00:00:00:01 0451 0004 1
```

REMOTE LISTPHONE

Lists the PVC numbers available for connecting to the remote router.

remote listPhone [*remoteName*]

remoteName Name of the remote router (character string)

Example: `remote listPhone HQ`

Response:

```
PHONE NUMBER(s) FOR <HQ>
  Connection Identifier (VPI*VCI)...... 0*38
```

NOTE: If the remote name is not specified, a list of phone numbers is displayed for each remote router in the database.

REMOTE SETATMTRAFFIC SCR MBS

This command applies only to ATM routers. Please refer to page 123 for more syntax information.

Remote setAtmTraffic scr mbs <remoteName>

REMOTE SETAUTHEN

Sets the authentication protocol used when communicating with the remote router. The authentication protocol is the minimum security level that the target router must use with the remote router; this level is verified during security negotiation. The router will *always* attempt to negotiate the highest level of security possible (CHAP). The router will not accept a negotiated security level less than this minimum authentication method.
The parameter in the remote router database is used for the local side of the authentication process; the minimum security level used by the target router when challenging or authenticating the remote router.

remote setAuthen <*protocol*> <*remoteName*>

protocol **chap**, **pap,** or **none**. The default is **pap**.

remoteName Name of the remote router (character string)

Example: `remote setAuthen pap HQ`

REMOTE SETBROPTIONS

Sets controls on the bridging process.

Warning: Do not change this setting without approval of your system administrator.

remote setBrOptions <*option*> [**on** | **off**] <*remoteName*>

option stp

Use the spanning tree protocol for bridging. Set this option on only if the bridging peers support the spanning tree protocol and you wish to detect bridging loops. The default is **on**.
NOTE: This adds a 40-second delay each time the ADSL or ATM link comes up; use only if necessary.

remoteName Name of the remote router (character string)

Example: `remote setbroptions stp on HQ`

REMOTE SETCOMPRESSION

Used to enable or disable compression between the local router and the remote router.

remote setCompression [on | off] <*remoteName*>

on Compression will be negotiated between the local and the remote router if both routers are set to perform compression and if they both share a common compression protocol.
off Disables compression. The default is OFF.

remoteName Name of the remote router (character string)

Example*:* `remote setCompression on HQ`

REMOTE SETDLCI

Please refer to page 129 for further information regarding this command.

REMOTE SETIPOPTIONS

RIP is a protocol used for exchanging IP routing information among routers. The following RIP options allow you to set IP routing information protocol controls over a point-to-point WAN.

remote setIpOptions <*option*> [**on** | **off**] <*remoteName*>

option Includes the following choices:

rxrip Receive and process IP RIP-1 compatible packets and RIP-2 broadcast packets from the remote site. Also receive and process RIP-2 multicast packets.
Set this option if the local router is to discover route information from other sites connected to the remote router. This is useful for hierarchical organizations. If connecting to another company or an Internet Service Provider, you may wish to set this option off. The default is **off.**

rxrip1 Receive and process RIP-1 packets only.

rxrip2 Receive and process RIP-2 packets only.

rxdef Receive default IP route address. Set on, the local router will receive the remote site's default IP route. The default is **off.**

txrip Transmit IP RIP-1 compatible broadcast packets and RIP-2 multicast packets to the remote site. Set on, the local router will send routing information packets to the remote site. The default is **off.**

txrip1 Transmit broadcast RIP-1 packets only.

txrip2 Transmit multicast RIP-2 packets only.

txdef Transmit the local router's default IP route. Set on, the local router will send the default route to the remote site. The default is **off.**

private Keep IP routes private. Used to prevent advertisement of this route to other sites by the remote router. Used as a security mechanism when the remote site is outside your company (an Internet Service Provider, for example), or whenever you would prefer to keep the identify of the site private. The default is **yes.**

multicast Allows the remote router to send and receive IP multicast traffic.

remoteName Name of the remote router (character string)

Example: `remote setipoptions private on  HQ`

REMOTE SETIPTRANSLATE

This command is used to control Network Address Translation on a per remote router basis. It allows several PCs to share a single IP address to the Internet. The remote router must assign the source WAN IP address to the routers' local WAN port. This command requires that you define a Source WAN IP Address with the command: `remote setSrcIproute`

remote setIPTranslate on|off <*remoteName*>

remoteName Name of the remote router (character string)

Example: `remote setIPTranslate on HQ`

REMOTE SETIPXADDR

Sets the IPX network number for the remote WAN connection.

remote setIpxAddr <*ipxNet#*> [*port#*]

ixpNet# IPX network number represented by 8 hexadecimal characters.

port# Port number of the Ethernet LAN. This number must be 0 or may be omitted.

Example: `remote setipxaddr 789 HQ`

REMOTE SETOURPASSWD

Sets a unique CHAP or PAP authentication password for the local router used for authentication when the local router connects to the specified remote router. This password overrides the password set in the **system passwd** command. A common use would be to set a password assigned to you by Internet Service Providers.

remote setOurPasswd <*password*> <*remoteName*>

password Authentication password of the local router for use in connecting to the remote router.
NOTE: the password is case-sensitive.

remoteName Name of the remote router (character string)

Example: `remote setOurPasswd s1dpxl7  HQ`

REMOTE SETOURSYSNAME

Sets a unique CHAP or PAP authentication system name for the local router used for authentication when the local router connects to the specified remote router. This system name overrides the system name set in the **system name** command. A common use would be to set a password assigned to you by Internet Service Providers.

remote setOurSysName *<name> <remoteName>*

name System name of the target router.
NOTE: the system name is case-sensitive and must be no more than 50 characters.

remoteName Name of the remote router (character string)

Example: `remote setOurSysName s1dpxl7  HQ`

REMOTE SETPASSWD

Sets the CHAP or PAP authentication password used when the remote router establishes a connection or is challenged by the target router.

remote setPasswd *<password> <remoteName>*

password Authentication password of the remote router. Not that the password is case-sensitive.
remoteName Name of the remote router (character string)

Example: `remote setPasswd s2dpxl7  HQ`

REMOTE SETPROTOCOL

Sets the link protocol for the remote router.

remote setProtocol [PPP | PPPLLC | RFC1483 | RFC1483MER | FRF8] *<remoteName>*

Link protocols options:

PPP	PPP protocol with no encapsulation
PPLLC	PPP protocol with LLC SNAP encapsulation (used with frame relay internetworking units)
RFC1483	RFC 1483 protocol
RFC1483MER	RFC 1483MER (MAC Encapsulated Routing) protocol
FRF8	This protocol implements ATM to frame relay as defined in the Frame Relay Forum RFR.8 Interworking Agreement.

remoteName Name of the remote router (character string)

Example: `remote setprotocol ppp fp1`

REMOTE SETPVC

Specifies the PVC number to be used when connecting to the remote router.

remote setPVC *<vpi number>*<vci number> <remoteName>*

vpi number Virtual Path ID — Number that identifies the link formed by the virtual path.

vci number Virtual Circuit ID — Number that identifies a channel within a virtual path in an ADSL/ATM environment.

remoteName Name of the remote router (character string)

Example: `remote setPVC 0*38 HQ`

REMOTE SETRMTIPADDR

Sets the WAN IP address for the remote router. This address is required only if the remote router does not support IP address negotiation under PPP (i.e., numbered mode is required and the remote router cannot specify a WAN IP address for use during the negotiation process).

remote setRmtIpAddr <*ipAddr*> <*ipNetMask*> <*remoteName*>

ipAddr IP address of the remote router, in the format of 4 decimals separated by periods.

ipNetMask IP network mask of the remote router, in the format of 4 decimals separated by periods.

remoteName Name of the remote router (character string)

Example: `remote setRmtIpAddr 128.1.210.65 255.255.255.192 HQ`

REMOTE SETSRCIPADDR

Sets the IP address for the target WAN connection to the remote router. You may set this address when the remote router requires the target and remote WAN IP addresses to be on the same subnetwork. Another instance is to force numbered mode and to prevent the remote router from changing the target WAN IP Address through IPCP address negotiation. The target WAN IP Address defaults to the Ethernet LAN IP address.

remote setSrcIpAddr <*ipAddr*> <*ipNetMask*> <*remoteName*>

ipAddr Target IP addr of the WAN connection to the remote router, in the format of 4 decimals separated by periods.

ipNetMask IP network mask, in the format of 4 decimals separated by periods.

remoteName Name of the remote router (character string)

Example: `remote setSrcIpAddr 128.1.210.151 255.255.255.192 HQ`

REMOTE STATS

Shows the current status of the connection to the remote router including the bandwidth and data transfer rate.

remote stats [*remoteName*]

remoteName Name of the remote router (character string)

Example: `remote stats HQ`

Response:

```
STATISTICS FOR <HQ>:
   Current state....................... currently connected
  Current output bandwidth............. 0 bps
  Current input bandwidth.............. 0 bps
  Current bandwidth allocated.......... 25600000 bps
  On port ATM_VC/1..................... 0+01:02:36 (0%/0% of 25600000 bps)
  Total connect time................... 0+01:11:48
  Total bytes out...................... 15896
  Total bytes in....................... 0

STATISTICS FOR <internet>:
  Current state....................... not connected
  Current output bandwidth............. 0 bps
  Current input bandwidth.............. 0 bps
  Current bandwidth allocated.......... 0 bps
  Total connect time................... 0+00:00:00
  Total bytes out...................... 0
  Total bytes in....................... 0
```

where:

Current state: connected, not connected, currently connecting, currently attempting to connect, currently closing, out of service, or not known

Bandwidth state: idle, increasing, decreasing, decreasing hold, unknown, and idle

REMOTE STATSCLEAR

Allows to reset the statistics counter for a given remote router.

remote statsclear <*remoteName*>

remoteName Name of the remote router (character string)

Example: `remote statsclear HQ`

Asymmetric Digital Subscriber Line Commands (ADSL)

The following ADSL commands are used to manage the ADSL link for an ADSL router.

ADSL ?

Lists the supported keywords.

adsl ?

Response:
ADSL commands:
?
restart stats speed

ADSL RESTART

This command is used to resynchronize the modem with the Central Office equipment.

adsl restart

Response:
12/02/1997-12:47:46:ADSL: Idle
12/02/1997-12:47:46:ADSL: Startup initiated
12/02/1997-12:47:48:ADSL: Startup training in progress
12/02/1997-12:47:54:ADSL: Modem started successfully
12/02/1997-12:47:54:ADSL: Near Avg SQ #: 44 dB [3]
12/02/1997-12:47:54:ADSL: Far Avg SQ #: 44 dB [3]
12/02/1997-12:47:54:ADSL: Downstream rate: 6272 Kb/s, Upstream rate: 1088 Kb/s
12/02/1997-12:47:54:DOD: connecting to internet @ 0*38 over ATM_VC/1
12/02/1997-12:47:56:ADSL: Data Mode
DUM: BR CHG ATM_VC/1 - to internet now forwarding

ADSL SPEED

This command is used to display the current downstream and upstream rates.

adsl speed

Example: `adsl speed`

Response: downstream rate: 6272 Kb/s, upstream rate: 1088 Kb/s

ADSL STATS

Shows the current error status for the ADSL connection.

adsl stats [clear]

clear Option used to reset the counters

Example: adsl stats

Response:

```
ASDL Statistics:
  Out of frame errors....     0
  HEC errors received...      0
  CRC errors received....     0
  FEBE errors received...     0
  Remote Out-of-frame....     0
  Remote HEC errors......     0
```

Asynchronous Transfer Mode Commands (ATM)

The following ATM commands are used to manage the ATM link for an ATM router.

ATM ?

Lists the supported keywords.

atm ?

Example: `atm?`

Response:
```
ATM commands:

?                   save          speed
```

ATM PCR

This command sets the speed of the ATM link in cells per second. This command is similar to `atm speed` (speed in kilobytes). Please refer to the command `atm speed`.
Note: This command requires privileged access (login password).

atm pcr <cells/second>

cells/second number of cells per second

Example: `atm pcr 471`

ATM RESET

This command is used to perform traffic shaping. It causes the ATM to re-initialize.

atm reset

Example: `atm reset`

ATM SAVE

This command is used to save the ATM configuration settings.

atm save

Example: `atm save`

ATM SPEED

This command sets the speed of the ATM link in kilobits per second. This command is similar to `atm pcr` (speed in cells per second). Please refer to the command `atm pcr.`
The upstream speed default is 326 Kb/s. Use this command if the upstream speed exceeds 326 Kb/s. The speed value is generally obtained from your Network Service Provider.

Note: This command requires privileged access (login password).

atm speed [*speed in Kb/S*]

speed in Kb/S Number provided by the Network Service Provider. 326 Kb/s is the default value for the upstream speed.

Example: `atm speed 326`

Response:
```
ATM Upstream Rate:   326 Kb/S
```

REMOTE SETATMTRAFFIC

This command sets ATM traffic shaping on a remote router. ATM traffic shaping allows the user to set the average rate at which cells are sent (SCR, Sustained Cell Rate) to a value lower than the ATM link speed (PCR, Peak Cell Rate).

Note 1 This command can only apply to one remote router. ATM traffic shaping must be used if more than one remote router is defined.

Note 2: ATM traffic shaping can be disabled with the command**: remote setatmtraffic 0 0** *<remoteName>*

Remote setAtmTraffic scr mbs <*remoteName*>

scr Sustained Cell Rate (cells per second)
mbs Maximum Burst Size (cells)

remoteName Name of the remote router (character string)

Examples: Assume that the ATM link speed (upstream) is 200 Kb/second or 471 cells/second and an average upstream data rate of 20 Kb/second (47 cells/second) is desired, then the following command would be used:
```
remote setatmtraffic 47 31 HQ
```

To disable ATM traffic shaping on HQ, use:
```
remote setatmtraffic 0 0 HQ
```

High-Speed Digital Subscriber Line Commands (HDSL)

The following HDSL commands are used to manage the HDSL link for an HDSL router.

General information about HDSL

Line activation

Line activation is independent of network settings. During activation, the Link light (on the front panel of the router) is yellow and then turns green when the link becomes active.

The router at the CPE end will try auto-speed detection starting at 384 and try to the next higher speed (for about 30 seconds per speed). The WAN light should turn yellow, then green when the link has activated.

Auto-speed detection can can be turned off with the command `hdsl speed noauto`.

If the line was previously set to “no auto-speed” (noauto), the Link light will be amber instead, when the line tries to activate.

The IFS command displays the Link as either Off or Opened when successfully activated. Following is a sample output.

```
ifs
Interface   Speed        In %     Out % Protocol     State        Connection
ETHERNET/0 10.0mb       0%/0%     0%/0% (Ethernet)   OPENED
HDSL/0      384kb       0%/0%     0%/0% ((HDSL)      OPENED
CONSOLE/0  9600 b       0%/0%     0%/0% (TTY)        OPENED
```

Auto-speed sequence

Auto-speed start with the lower speed (384) and tries to activate for 30 seconds. If no activation takes place, the next higher speed is attempted. The time intervals between activation may change if the modems don’t activate as expected. Following is a correct activation output.

```
03/09/1998-17:11:59:HDSL: Deactivated
03/09/1998-17:12:22:HDSL: CPE is Activating at 384 Kb/s
03/09/1998-17:13:00:HDSL: Deactivated
03/09/1998-17:13:01:HDSL: CPE is Activating at 1168 Kb/s
03/09/1998-17:13:32:HDSL: Deactivated
03/09/1998-17:13:32:HDSL: CPE is Activating at 1168 Kb/s
03/09/1998-17:14:11:HDSL: Deactivated
03/09/1998-17:14:12:HDSL: CPE is Activating at 384 Kb/s
03/09/1998-17:14:51:HDSL: Activated
03/09/1998-17:14:53:FRAMER: The framer is synchronized
```

HDSL ?

Lists the supported keywords.

hdsl ?

Example: `hdsl?`

Response:

```
HDSL commands:
?                    help

save                 speed
```

HDSL SPEED

CO end: This command is used to set the speed manually on the CO end only.

CPE end: The router on the CPE end is always in auto-speed mode: it uses an auto-speed algorithm to attempt to match the CO speed. The command `hdsl speed noauto` is used to override auto-speed.

Note 1: The command `hdsl speed` (with no option) displays the current speed if the modem has activated successfully.

Note 2: `hdsl speed noauto` should be followed by the command `hdsl save` to become persistent across reboots.

Note 3: During auto-speed search, use the command `hdsl speed <speed>` to stop the search and restart it at the speed you just entered.

hdsl speed [384 | 1168 | noauto]

384	Default speed for the CO
1168	Authorized non-default speeds for the CO in Mbps
noauto	Used to override auto-speed on the CPE end

Example:

```
hdsl speed 1168
hdsl speed noauto
hdsl speed
```

HDSL SAVE

Used to save the HDSL-related changes across reboots.

hdsl save

Example: `hdsl save`

HDSL TERMINAL

The router is by default configured as the CPE. Use this command if you intend to configure the router as a Central Office equipment (CO).

`hdsl terminal cpe` is used to define the CPE (customer premise) end (default configuration)

`hdsl terminal co` is used to define the CO (central office) end.

`hdsl terminal` displays the current settings.

hdsl terminal [cpe | co]

co This option lets you define the router as the central office (CO).

Example: `hdsl terminal`

Response: `Customer Premises`

Example: `hdsl terminal co`

ISDN Digital Subscriber Line (IDSL)

General information about IDSL

DLCI (Data Link Connection Identifier)

The IDSL router can support several DLCI virtual circuits over a Frame Relay IDSL link. However, a typical connection to the Internet will require only one DLCI.

The DLCI number must match the DLCI of the remote end.

An activated router should have the LINE, CH1, CH2, and NT1 LEDs all lit green.

The following IDSL commands are used to manage the IDSL link for an IDSL router.

ISDN ?

Lists the supported keywords.

Isdn ?

Example: `isdn?`

Response:

```
ISDN commands:
?               help
save            set         list
```

ISDN LIST

Lists the current switch type information.

Isdn list

Example: `isdn list`

Response: `Switch type is Frame Relay IDSL 144k`

ISDN SAVE

Used to save the IDSL-related changes across reboots.

Isdn save

Example: `isdn save`

ISDN SET SWITCH

This command is used to specify link speeds of 64, 128, or 144 Kbps for the IDSL connection.

Isdn set switch [FR64 | FR128 | FR144]

FR64 Link speed of 64 Kbps

FR128 Link speed of 128 Kbps

FR144 Link speed of 144 Kbps

Example: `isdn set switch fr144`

REMOTE SETDLCI

This command allows the user to set the Data Link Connection Identifier – an address identifying a logical connection – in a Frame Relay environment. This number is generally provided by the Network Service Provider.

Remote setDLCI <*number*> <*remoteName*>

number Frame Relay number identifying the data link connection.

remoteName Name of the remote router (character string)

Example: `remote setDLCI 16 HQ`

REMOTE SETPROTOCOL

This IDSL-specific command is used to select the appropriate link protocol for your IDSL connection. Your Network Service Provider will tell you which link protocol to use.

Remote setProtocol [PPP | FR | MER] <*remoteName*>

PPP PPP protocol with no encapsulation

FR RFC 1490 protocol (Multiprotocol encapsulation over Frame Relay)

MER RFC 1490 protocol with MAC Encapsulated Routing

remoteName Name of the remote router (character string)

Example: remote setProtocol FR HQ

Symmetric Digital Subscriber Line Commands (SDSL)

The following SDSL commands are used to manage the SDSL link for an SDSL router.

General information about SDSL

Line activation

Line activation is independent of network settings. During activation, the Link light (on the front panel of the router) is yellow and then turns green when the link becomes active.

The router at the CPE end will try auto-speed detection starting at 384 and try to the next higher speed (for about 30 seconds per speed). The WAN light should turn yellow, then green when the link has activated.

Auto-speed detection can can be turned off with the command `sdsl speed noauto`.

If the line was previously set to “no auto-speed” (noauto), the Link light will be amber instead, when the line tries to activate.

The IFS command displays the Link as either Off or Opened when successfully activated. Following is a sample output.

```
ifs
Interface   Speed        In %     Out % Protocol     State        Connection
ETHERNET/0 10.0mb       0%/0%     0%/0% (Ethernet)   OPENED
SDSL/0      384kb       0%/0%     0%/0% (ATM)        OPENED
CONSOLE/0  9600 b       0%/0%     0%/0% (TTY)        OPENED
```

Auto-speed sequence

Auto-speed start with the lower speed (384) and tries to activate for 30 seconds. If no activation takes place, the next higher speed is attempted. The time intervals between activation may change if the modems don’t activate as expected. Following is a correct activation output.

```
03/09/1998-17:11:59:SDSL: Deactivated
03/09/1998-17:12:22:SDSL: CPE is Activating at 768 Kb/s
03/09/1998-17:13:00:SDSL: Deactivated
03/09/1998-17:13:01:SDSL: CPE is Activating at 1152 Kb/s
03/09/1998-17:13:32:SDSL: Deactivated
03/09/1998-17:13:32:SDSL: CPE is Activating at 1152 Kb/s
03/09/1998-17:14:11:SDSL: Deactivated
03/09/1998-17:14:12:SDSL: CPE is Activating at 384 Kb/s
03/09/1998-17:14:51:SDSL: Activated
03/09/1998-17:14:53:FRAMER: The framer is synchronized
03/09/1998-17:15:19:DOD: connecting to co @ 0*38 over ATM-VC/1
03/09/1998-17:15:35:DOD: link to co over ATM-VC/1 is now up
03/09/1998-17:15:57:SDSL: Line Rate at last activation saved
```

SDSL ?

Lists the supported keywords.

sdsl ?

Example: `sdsl?`

Response:
SDSL commands:

?	help
save	speed

SDSL SPEED

CO end: This command is used to set the speed manually on the CO end only.

CPE end: The router on the CPE end is always in auto-speed mode: it uses an auto-speed algorithm to attempt to match the CO speed. The command `sdsl speed noauto` is used to override auto-speed.

Note 1: The command `sdsl speed` (with no option) displays the current speed if the modem has activated successfully.

Note 2: `sdsl speed noauto` should be followed by the command `sdsl save` to become persistent across reboots.

Note 3: During auto-speed search, use the command `sdsl speed <speed>` to stop the search and restart it at the speed you just entered.

sdsl speed [384 | 768 | 1152 | noauto]

384	Default speed for the CO
768, 1152	Authorized non-default speeds for the CO in Mbps
noauto	Used to override auto-speed on the CPE end

Example:
```
sdsl speed 1152
sdsl speed noauto
sdsl speed
```

SDSL SAVE

Used to save the SDSL-related changes across reboots.

sdsl save

Example: `sdsl save`

SDSL TERMINAL

The router is by default configured as the CPE. Use this command if you intend to configure the router as a Central Office equipment (CO).

`sdsl terminal cpe` is used to define the CPE (customer premise) end (default configuration)

`sdsl terminal co` is used to define the CO (central office) end.

`sdsl terminal` displays the current settings.

sdsl terminal [cpe | co]

co This option lets you define the router as the central office (CO).

Example: `sdsl terminal`

Response: `Customer Premises`

Example: `sdsl terminal co`

Dynamic Host Configuration Protocol Commands (DHCP)

The following DHCP commands allow you to:

- Enable and disable subnetworks and client leases
- Add subnetworks and client leases
- Set the lease time
- Change client leases manually
- Set option values globally, for a subnetwork, or for a client lease
- Enable/disable BootP
- Use BootP to specify the boot server
- Define option types

DHCP ?

Lists the supported keywords.

dhcp ?

Response:

```
Sub-commands for dhcp
?                  help              set
list               bootp             clear
enable             add               del
disable
```

DHCP ADD

This command is used to add a subnetwork, a client lease, or an option type.

dhcp add [<*net*> <*mask*>]	<*ipAddr*>	<*code*> <*min*> <*max*> <*type*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

mask IP network mask, in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

code The code is user-defined can be a number between 128 to 254 or a keyword.

min Minimum number of value(s)

max Maximum number of value(s)

type Byte | word | long | longint | binary | ipAddress | string

Examples: `dhcp add 192.168.254.0.255.255.255.0`
(adds this subnetwork)
`dhcp add 192.168.254.31`
(adds this client lease)

`dhcp add 128 1 4 ipAddress`
(adds this option type.
NOTE: In the above example, 128 allows IP addresses, the server has a minimum of one IP address, the server can have up to four IP addresses, and the type is "ipAddress")

DHCP BOOTP ALLOW

This command allows a BootP request to be processed for a particular client or subnet.

dhcp bootp allow <***net***> | <***ipAddr***>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

Example: `dhcp bootp allow 192.168.254.0`

DHCP BOOTP DISALLOW

This command is used to disallow a BootP request to be processed for a particular client or subnet.

dhcp bootp disallow <*net*> | <*ipAddr*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

Example: `dhcp bootp disallow 192.168.254.0`

DHCP BOOTP FILE

This command lets you specify the boot file name (kernel).

NOTE: The TFTP server IP address must also be set when the file is specified.

dhcp bootp file [<*net*> | <*ipAddr*> **]** <*name*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

name Name of the file to boot from; the default name for this file is KERNEL.100

Example: `dhcp boot file 192.168.254.0 kernel.100`

DHCP BOOTP TFTPSERVER

This command lets you specify the TFTP server (boot server).

dhcp bootp tftpserver [<*net*> | <*ipAddr*>] <*tftpserver ipAddr*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

tftpserver ipAddr IP address of the TFTP server in the format of 4 decimals separated by periods
0.0.0.0 is used to clear the IP address of the server

Examples:

```
dhcp bootp tftpserver 192.168.254.7
dhcp bootp tftpserver 192.168.254.0 192.168.254.8
dhcp bootp tftpserver 192.168.254.21 192.168.254.9
dhcp bootp tftpserver 0.0.0.0
```

DHCP CLEAR ADDRESSES

This command is used to clear the values from a pool of addresses.

dhcp clear addresses <*net*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

Example: `dhcp clear addresses 192.168.254.0`

DHCP CLEAR EXPIRE

This command is used to release the client lease. It then becomes available for other assignments.

dhcp clear expire <*ipAddr*>

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

Example: `dhcp clear expire 192.168.254.12`

NOTE: The client does not get updated. It will still have the old value.

DHCP CLEAR VALUEOPTION

This command is used to clear the value for a global option, for an option associated with a subnetwork, or with a specific client.

dhcp clear valueoption [<*net*>|<*ipAddr*>**]** <*code*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

code Code can be a number between 1 and 61 or a keyword. Use the command **dhcp list definedoptions** to list the codes and keywords.

Examples:
```
dhcp clear valueoption 4
dhcp clear valueoption 192.168.254.0 7
dhcp clear valueoption 192.168.254.2 gateway
```

DHCP DEL

This command is used to delete a subnetwork lease, a specific client lease, or a code.

dhcp del <*net*> |<*ipAddr*> | <*code*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

code The code is user-defined and can be a number between 128 to 254 or a keyword.

Examples:
`dhcp del 192.168.254.0`
(deletes this subnetwork)

`dhcp del 192.168.254.31`
(deletes this client lease)
`dhcp del 128`
(deletes this option with code 128)

DHCP DISABLE

This command is used to disable a subnetwork or a client lease.

dhcp disable <*net*> **|** <*ipAddr*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

Example:
```
dhcp disable 192.168.254.0
dhcp disable 192.168.254.17
```

DHCP ENABLE

This command is used to enable a subnetwork or a client lease.

dhcp enable <*net*>|<*ipAddr*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

Example:
```
dhcp enable 192.168.254.0
dhcp enable 192.168.254.17
```

DHCP LIST

This command lists global, subnetwork, and client lease information.

dhcp list **|** <*net*>|<*ipAddr*>

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

Examples:

To list global information, use: `dhcp list`

Response:
```
    bootp server ................. none
        bootp file ...................
        DOMAINNAMESERVER (6) ......... 192.168.210.20 192.84.210.21
        DOMAINNAME (15) .............. flowpoint.com
        WINSSERVER (44) .............. 192.168.254.73
Subnet 192.168.254.0, Enabled
        Mask ......................... 255.255.255.0
        first ip address ............. 192.168.254.2
        last ip address .............. 192.168.254.253
        lease ........................ Default
        bootp ........................ not allowed
```

```
       bootp server ................. none
       bootp file ..................
    GATEWAY (3) ................. 192.168.254.254
   client 192.168.254.2, Ena, jo-computer , Expired
   client 192.168.254.3, Ena, Jo, 1997/5/16 11:31:33
```

To list information for client 192.168.254.3, use: `dhcp list 192.168.254.3`

Response:

```
Client 192.168.254.3, Enabled
       lease ........................ Default
       expires ...................... 1997/5/16 11:31:33
       bootp ........................ not allowed
       bootp server ................. none
       bootp file ...................
       HOSTNAME (12) ................ JO
       CLIENTIDENTIFIER (61) ........ 1 2 96 140 76 149 180
```

To list information for the subnetwork 192.168.254.0, use: `dhcp list 192.168.254.0`

Response:

```
Subnet 192.168.254.0, Enabled
       Mask .................. 255.255.255.0
       first ip address ...... 192.168.254.2
       last ip address ....... 192.168.254.253
       lease ..................Default
       bootp ..................not allowed
       bootp server ...........none
       bootp file .............
       GATEWAY (3) ............192.168.254.254
   client 192.168.254.2, Ena, Jo-computer, Expired
   client 192.168.254.3, Ena, Jo,  1997/5/16 11:31:33
```

DHCP LIST DEFINEDOPTIONS

This command lists all available predefined and user-defined options.

NOTE: For description of the predefined options listed below, please refer to RFC 1533. A predefined code can be a number between 1 and 61 or a keyword. A user-defined code can be a number between 128 and 254 or a keyword.

dhcp list definedoptions | <*code*> | <*string*>

code Predefined or user-defined number or keyword

string Character string

Examples:

To list all available options (they may be predefined asin the list below, and/or user-defined), use:
`dhcp list definedoptions`

Response:

```
code SUBNETMASK (1), 1 occurrence, type IPADDRESS-RESERVED
code TIMEOFFSET (2), 1 occurrence, type LONG
```

```
code GATEWAY (3), 1 to 63 occurrences, type IPADDRESS
code TIMESERVER (4), 1 to 63 occurrences, type IPADDRESS
code NAMESERVER (5), 1 to 63 occurrences, type IPADDRESS
code DOMAINNAMESERVER (6), 1 to 63 occurrences, type IPADDRESS
code LOGSERVER (7), 1 to 63 occurrences, type IPADDRESS
code COOKIESERVER (8), 1 to 63 occurrences, type IPADDRESS
code LPRSERVER (9), 1 to 63 occurrences, type IPADDRESS
code IMPRESSSERVER (10), 1 to 63 occurrences, type IPADDRESS
code RESOURCELOCATION (11), 1 to 63 occurrences, type IPADDRESS
code HOSTNAME (12), 1 to 255 characters, type STRING
code BOOTFILESIZE (13), 1 occurrence, type WORD
code MERITDUMPFILE (14), 1 to 255 characters, type STRING
code DOMAINNAME (15), 1 to 255 characters, type STRING
code SWAPSERVER (16), 1 occurrence, type IPADDRESS
code ROOTPATH (17), 1 to 255 characters, type STRING
code EXTENSIONSPATH (18), 1 to 255 characters, type STRING
code IPFORWARDING (19), 1 occurrence, type BINARY
code NONLOCALSOURCERTE (20), 1 occurrence, type BINARY
code POLICYFILTER (21), 1 to 31 occurrences, type IPADDRESS
code MAXDGMREASSEMBLY (22), 1 occurrence, type WORD
code DEFAULTIPTTL (23), 1 occurrence, type BYTE
code PATHMTUAGETMOUT (24), 1 occurrence, type LONGINT
code PATHMTUPLATEAUTBL (25), 1 to 127 occurrences, type WORD
code INTERFACEMTU (26), 1 occurrence, type WORD
code ALLSUBNETSLOCAL (27), 1 occurrence, type BINARY
code BROADCASTADDRESS (28), 1 occurrence, type IPADDRESS
code PERFORMMASKDSCVR (29), 1 occurrence, type BINARY
code MASKSUPPLIER (30), 1 occurrence, type BINARY
code PERFORMRTRDSCVR (31), 1 occurrence, type BINARY
code RTRSOLICITADDR (32), 1 occurrence, type IPADDRESS
code STATICROUTE (33), 1 to 31 occurrences, type IPADDRESS
code TRAILERENCAP (34), 1 occurrence, type BINARY
code ARPCACHETIMEOUT (35), 1 occurrence, type LONGINT
code ETHERNETENCAP (36), 1 occurrence, type BINARY
code TCPDEFAULTTTL (37), 1 occurrence, type BYTE
code TCPKEEPALIVEINTVL (38), 1 occurrence, type LONGINT
code TCPKEEPALIVEGARBG (39), 1 occurrence, type BINARY
code NETINFOSVCDOMAIN (40), 1 to 255 characters, type STRING
code NETINFOSERVERS (41), 1 occurrence, type IPADDRESS
code NETTIMEPROTOSRVRS (42), 1 occurrence, type IPADDRESS
code VENDORSPECIFIC (43), 1 to 255 occurrences, type BYTE
code WINSSERVER (44), 1 to 63 occurrences, type IPADDRESS
code NETBIOSTCPDGMDIST (45), 1 to 63 occurrences, type IPADDRESS
code NETBIOSTCPNODETYP (46), 1 occurrence, type BYTE
code NETBIOSTCPSCOPE (47), 1 to 255 characters, type STRING
code XWSFONTSERVER (48), 1 to 63 occurrences, type IPADDRESS
code XWSDISPLAYMANAGER (49), 1 to 63 occurrences, type IPADDRESS
code REQUESTEDIPADDR (50), 1 occurrence, type IPADDRESS-RESERVED
code IPADDRLEASETIME (51), 1 occurrence, type LONGINT-RESERVED
code OPTIONOVERLOAD (52), 1 occurrence, type BYTE-RESERVED
code MESSAGETYPE (53), 1 occurrence, type BYTE-RESERVED
code SERVERIDENTIFIER (54), 1 occurrence, type IPADDRESS-RESERVED
code PARAMREQUESTLIST (55), 1 to 255 occurrences, type BYTE-RESERVED
code MESSAGE (56), 1 to 255 characters, type STRING-RESERVED
code MAXDHCPMSGSIZE (57), 1 occurrence, type WORD-RESERVED
code RENEWALTIME (58), 1 occurrence, type LONGINT
code REBINDTIME (59), 1 occurrence, type LONGINT
code CLASSIDENTIFIER (60), 1 to 255 occurrences, type BYTE
code CLIENTIDENTIFIER (61), 2 to 255 occurrences, type BYTE
code NOTDEFINED62 (62), 1 to 255 occurrences, type BYTE
code NOTDEFINED63 (63), 1 to 255 occurrences, type BYTE
code NISDOMAIN (64), 1 to 255 characters, type STRING
code NISSERVERS (65), 1 to 63 occurrences, type IPADDRESS
code TFTPSERVERNAME (66), 4 to 255 characters, type STRING
code BOOTFILENAME (67), 1 to 255 characters, type STRING
code MOBILEIPHOMEAGNT (68), 0 to 63 occurrences, type IPADDRESS
```

```
code SMTPSERVERS (69), 1 to 63 occurrences, type IPADDRESS
code POP3SERVERS (70), 1 to 63 occurrences, type IPADDRESS
code NNTPSERVERS (71), 1 to 63 occurrences, type IPADDRESS
code WWWSERVERS (72), 1 to 63 occurrences, type IPADDRESS
code FINGERSERVERS (73), 1 to 63 occurrences, type IPADDRESS
code IRCSERVERS (74), 1 to 63 occurrences, type IPADDRESS
code STREETTALKSERVERS (75), 1 to 63 occurrences, type IPADDRESS
code STREETTALKDASRVRS (76), 1 to 63 occurrences, type IPADDRESS
```

To list options starting with the string “ga”, use: `dhcp list definedoptions ga`

Response:

```
code,           number of values,      type of value
code GATEWAY (3), occurrence 1, type IPADDRESS
```

DHCP LIST LEASE

This command lists the lease time.

dhcp list lease

Example:

`dhcp list lease`
Default lease time ..... 168 hours

DHCP SET ADDRESSES

This command is used to create or change a pool of IP addresses that are associated with a subnetwork.

dhcp set addresses <*first ipAddr*> <*last ipAddr*>

first ipAddr First address in a pool of addresses for a particular subnetwork

last ipAddr Last address in a pool of addresses for a particular subnetwork

Example: dhcp set addresses 192.168.254.1 192.168.254.250

DHCP SET EXPIRE

This command is used to manually change a client lease expiration time to a certain value.

NOTE: Changing a client lease time manually is rarely required.

dhcp set expire <*ipAddr*> <*hours*>| **default | infinite**

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

hours Lease time; minimum is 1 hour; 168 hours is the global default

default Lease time that has been specified at the subnetwork or global level

infinite No lease time limit; the lease becomes permanent

Example: `dhcp set expire 192.168.254.18 8`

NOTE: The client information does not get updated. It will still have the old value.

DHCP SET LEASE

This command is used to control lease time.

dhcp set lease [*<net>* | *<ipAddr>* **]** *<hours>* **| default | infinite**

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

hours Lease time; minimum is 1 hour; 168 hours is the global default

default Lease time that has been specified at the subnetwork or global level

infinite No lease time limit; the lease becomes permanent

Examples: `dhcp set lease 192.168.254.17 default`
(sets client lease time to default)

`dhcp set lease 192.168.254.0 infinite`
(sets lease time to infinite for this subnet)

`dhcp set lease 2`
(sets global lease time to 2 hours)

DHCP SET VALUEOPTION

This command is used to set values for global options, options specific to a subnetwork, or options specific to a client lease.

dhcp set valueoption [*<ipAddr>*|*<net>*] *<code> <value>....*

net IP address of the subnetwork lease in the format of 4 decimals separated by periods

ipAddr IP address of the client lease in the format of 4 decimals separated by periods

code Code can be a number between 1 and 61 or a keyword. Use the command **dhcp list definedoptions** to list the codes and keywords.

value Can be a byte, word, signed long, unsigned long, binary, IP address, or string depending on the type of option

Examples: `dhcp set value option 192.168.254.0 gateway 192.168.254.254`

(sets the value for an option associated with a subnetwork)

```
dhcp set valueoption domainnameserver 192.168.254.2
 192.168.254.3
```

(sets a global value for the domain name server option)

```
dhcp set valueoption 192.168.254.251 winserver 192.168.254.7
```

(sets a value for an option associated with a specific client)

Bridging Filtering Commands (FILTER BR)

Bridging filtering allows you to control the packets transferred across the router. This feature can be used to enhance security or improve performance. Filtering occurs based on matched patterns within the packet at a specified offset. Two filtering modes are available:

- Deny mode will discard any packet matched to the deny filter database and let all other packets pass.
- Allow mode will only pass the packets that match the allow filter database and discard all others.

Up to 40 deny and 40 allow filters can be activated from the filter database.

FILTER BR ?

Lists the supported keywords.

filter br ?

Response: `Bridge filter commands:`

```
?                   add                 del
use                 list
```

FILTER BR ADD

Adds a bridging filter to the filtering database.

filter br add <*pos*> <*dataPattern*> **deny**|**allow**

pos Byte offset within a packet; number from 0-127

dataPattern Hex number up to 6 bytes

Example: `filter br add 12 8035 deny`
(This filter prevents forwarding of RARP packets across the bridge.)

FILTER BR DEL

Deletes a bridging filter from the filtering database.

filter br del <*pos*> <*dataPattern*> **deny**|**allow**

pos Byte offset within a packet; number from 0-127

dataPattern Hex number up to 6 bytes

Example: `filter br del 12 8035 deny`

FILTER BR LIST

Lists the bridging filters in the filtering database.

filter br list

Example: `filter br list`

Response:

```
Allow Filter:

Deny Filter:
pos:12, len=2, <80><35>
```

FILTER BR USE

Sets the mode of filtering to either deny, allow, or none.

filter br use none|deny|allow

Example: `filter br use allow`

Save Configuration Commands (SAVE)

These commands can be used to save the entire configuration of parts of the router's configuration to FLASH memory. The parts of the configuration you can save include:

- System
- Ethernet LAN
- DHCP settings
- Remote Router Database settings
- Filters

SAVE ALL

Saves the configuration settings for the system, Ethernet LAN, ATM or ADSL line, and remote router database into FLASH memory. Note that there is a time lag between the response issued by a save command and the time the data is actually stored in FLASH memory. Issue a **sync** command after a **save** command prior to powering off the router. This commits the changes to FLASH memory.

save all

Example: `save all`

SAVE ATM25

Saves the ATM configuration settings. All new entries and changed entries are erased from FLASH memory.

save atm25

Example: save atm25

SAVE DOD

Saves the current state of the remote router database. All new entries and changed entries are saved into FLASH memory.

save dod

Example: `save dod`

SAVE DHCP

Saves the DHCP configuration settings into FLASH memory.

save dhcp

Example: `save dhcp`

SAVE ETH

Saves the configuration settings for the Ethernet LAN into FLASH memory.

save eth

Example: `save eth`

SAVE FILTER

Saves the bridging filtering database to FLASH memory. A reboot must be executed to load the database for active use.

save filter

Example: `save filter`

SAVE SYS

Saves the name, message, and authentication password system settings into FLASH memory.

save sys

Example: `save sys`

Erase Configuration Commands (ERASE)

These commands can be used to erase the entire configuration or parts of the router's configuration from FLASH memory. The parts of the configuration you can erase include:

- System
- Ethernet LAN
- ATM or ADSL and Remote Router Database settings
- DHCP settings
- Filters

Once you erase part of the configuration, you will need to reconfigure that part of the configuration entirely.

Important: All of the following **erase** commands require a reboot without a save command to take effect.

ERASE ALL

Erases the configuration settings for the system, Ethernet LAN, ATM or ADSL line, DHCP, and remote router database from FLASH memory.

NOTE: There is a time lag between the response issued by the **erase** command and the time the data is actually deleted from FLASH memory. Issue a **sync** command after an **erase** command prior to powering off the router. This commits the changes to FLASH memory.

erase all

Example: `erase all`

ERASE ATM25

Erases the ATM configuration settings. All new entries and changed entries are erased from FLASH memory.

erase atm25

Example: `erase atm25`

ERASE DHCP

Erases the dhcp configuration settings. All new entries and changed entries are erased from FLASH memory.

erase dhcp

Example: `erase dhcp`

ERASE DOD

Erases the current state of the remote router database. All new entries and changed entries are erased from FLASH memory.

erase dod

Example: `erase dod`

ERASE ETH

Erases the configuration settings for the Ethernet LAN from FLASH memory.

erase eth

Example: `erase eth`

ERASE FILTER

Erases the current bridging filtering database from FLASH memory. This command requires a **reboot** (without a **save**).

erase filter

Example: `erase filter`

ERASE SYS

Erases the name, message, and authentication password system settings from FLASH memory.

erase sys

Example: `erase sys`

File System Commands

The file system commands allow you to perform maintenance and recovery on the router. These commands allow you to:

- Format the file system
- List the contents of the file system
- Copy, rename, and delete files

The router file system is DOS-compatible and the file system commands are similar to the DOS commands of the same name.

COPY

Copies a file from the source to the destination. This command allows you to update the router software level or to write configuration files to a TFTP server.

copy *<srcFile> <destFile>*

srcFile Filename of the source file to be copied.

destFile Destination filename from where the file is to be copied.

Example: `copy tftp@128.1.210.66:kernelnw kernel.f2k`

Response:
```
Copying ...
421888 bytes copied
```

A filename is either the name of a local file or a file accessed remotely via a TFTP server:

A local filename is in the format:
`yyyyyyyy.yyy`.

A remotely accessed filename is specified as:
`TFTP@xxx.xxx.xxx.xxx:yyyyyyyy.yyy`

where `xxx.xxx.xxx.xxx` is the (optional) TFTP server address and `yyyyyyyy.yyy` is the name of the file to be copied. If the TFTP server address is not specified, the address used is the one from which the router booted or the one permanently configured in the boot system. Issue a **sync** command after a **copy** to commit the changes to FLASH memory.

Caution: No warning message is issued if you copy over an existing file.

DIR

Displays the directory of the file system. The size of each file is listed (bytes).

dir

Example: `dir`

Response:

```
SYSTEM   CNF  2304
ATM25    DAT  20
DHCP     DAT  1536
KERNEL   F2K  257014
IDL_7    AIC  14828
ASIC     AIC  14828
FILTER   DAT  1284
```

FORMAT DISK

Erases and reformats the router file system. This command should **only** be used when the file system is unusable. If the router does not execute the POST test and software boot successfully, and the result of the **dir** command indicates the file system is corrupted, you may wish to reformat the disk, reboot the router, and recopy the router software.

format disk

Example: `format disk`

Response:

```
NEWFS: erasing disk...
NEWFS: fs is 381k and will have 762 sectors
NEWFS: 128 directory slots in 8 sectors
NEWFS: 747 fat entries in 3 sectors
NEWFS: writing boot block...done.
NEWFS: writing fat tables...done.
NEWFS: writing directory...done.
Filesystem formatted!
```

MSFS

Checks the file structure of the file system. This command performs a function similar to the DOS **`chkdsk`** command. The router analyzes the File Allocation Table (FAT) and produces a file system status report.

If **fix** is specified, errors are corrected in the FAT. This option should *only* be used when an **msfs** command results in a recommendation to apply the **fix** option.

WARNING: When specifying **fix**, make sure that no other operation is being performed on the configuration files at the same time (by the Configuration Manager).

msfs [fix]

Example: `msfs`

Response:

```
Filesystem 0, size=825k :
Checking filesystem...
Checking file entries...
  SYSTEM   CNF ...   2304 bytes .. ok.
  ATM25    DAT ...     20 bytes .. ok.
  DHCP     DAT ...   1536 bytes .. ok.
  KERNEL   F2K ... 257014 bytes .. ok.
  IDL_7    AIC ...  14828 bytes .. ok.
  ASIC     AIC ...  14828 bytes .. ok.
  FILTER   DAT ...   1284 bytes .. ok.
  1097 fat(s) used, 0 fat(s) unused, 0 fat(s) unref, 534 fat(s) free
  561664 bytes used by files, 9728 bytes by tables, 273408 bytes free
```

DELETE

Removes a file from the file system.

delete <*fileName*>

fileName Name of the file to be deleted. The filename is in the format xxxxxxxx.xxx.

Example: `delete kernel.f2k`

Response: `kernel.f2k deleted.`

RENAME

Renames a file in the file system to a new name.

rename <*oldName*> <*newName*>

oldName Existing name of the file to be renamed

newName New name of the file.

The filename is in the format xxxxxxxx.xxx.

Example: `rename ether.dat oldeth.dat`

Response: `'ether.dat' renamed to 'oldeth.dat'`

SYNC

Commits the changes to the file system to FLASH memory.

sync

Example: `sync`
Response: `Syncing filesystems...done.`

Warning: Syncing is not complete until you see '`done`'.

Chapter 6. Managing The Router

This chapter describes the options available for booting software, how to upgrade the router with new releases of software, and explains the process for maintaining copies of configuration files.

Simple Network Management Protocol (SNMP)

SNMP, a member of the TCP/IP protocol suite, was designed to provide network management interoperability among different vendors' management applications and equipment. SNMP provides for the exchange of messages between a management client and a management agent. The messages contain requests to get or set variables that exist in network nodes, thus allowing a management client to obtain statistics, set configuration parameters and monitor events. These variables (or objects) are defined in Management Information Bases (MIBs), some of which are general or standard SNMP-defined bases. Other bases, Enterprise Specific MIBs are defined by the different vendors for specific hardware.

The 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.

The supported MIB and a description of their contents are listed in the following table:

MIB II	Internet-standard MIB contains only essential elements such as system, interface, addressing, protocol (IP, etc.) and SNMP objects
Bridge MIB	States/statistics (including spanning tree states) within bridging system
Ethernet MIB	State/statistics of Ethernet port (collisions, etc.)
IP Forwarding MIB	State of routing tables (updates MIB II)
PPP MIB For LCP	State/Statistics for each PPP link
Enterprise MIB for configuration	Router-specific objects for configuration purposes

Any management application using SNMP over UDP/IP has access to the local SNMP agent. SNMP network management tools vary but often have features to display network maps of SNMP nodes, poll nodes at intervals, trigger alarms on thresholds, graph or list node statistic counters, view and edit individual MIB variables and print reports.

An example of useful information that can be obtained from a remote SNMP client would be the current status of the router's WAN link and Ethernet interfaces including: protocol (PPP, CSMA-CD), line speed, maximum frame (transmission unit) size, physical address, operating status, or packet traffic rates.

TELNET Remote Access

TELNET access to the router is supported. TELNET allows you to log in to the router as if you are directly connected through the Console port. In this manner you can issue commands, using the command line interface, to configure the router and perform status monitoring from any remote location. You can use one of the

available TCP/IP packages containing the TELNET application. To access the router using TELNET, issue the appropriate command syntax and assign the IP address of the router. You are then directly connected to the router and can issue commands. When you wish to end the TELNET session, exit the application by entering 'logoff' or another appropriate command.
Use the command `system telnetport` to enable or disable TELNET access.

Client TFTP Facility

A client Trivial File Transfer Protocol (TFTP) facility is built into the router and is capable of reading from and writing to the network. A TFTP server must be properly configured to communicate with the router for file transfers to be successful. The client TFTP facility is employed to boot software from a TFTP server, perform software upgrades and copy configuration files to a TFTP server. A TFTP server is integrated into the Windows' Configuration Manager and can also be used as a standalone application.

Software Boot Options

The router provides a number of options for booting router software. You can boot from the router's FLASH memory, the most common option. Or, you can boot across the LAN network from a TFTP server, perhaps to test a new level of router software before downloading to FLASH memory. You can also boot through a gateway to a WAN. The router allows you to set permanent network boot parameters used during network booting and enables you to temporarily override those parameters. Finally, the router lets you define the order in which the router boot procedures are performed. You can make changes to the boot procedures and specify network boot parameters by entering manual boot mode.

Manual Boot Mode

The router, as received when shipped, will be set for automatic boot from FLASH. If you wish to change the boot options to allow for network booting, change the order of boot procedures or perform a manual boot, you must enter manual boot mode. Automatic and manual boot is controlled by Configuration Switches. (Refer to *Appendix E. Changing Configurations Switches* in the User Guide, for the location and function of the Configuration Switches.) Set Switch 6 **DOWN** for Manual Boot mode and reboot the router by issuing the **reboot** command. The router then displays a menu of options:

```
1. Retry start-up
2. Boot from Flash memory
3. Boot from network
4. Boot from specific file
5. Configure boot system
6. Set date and time
7. Set console baud rate
8. Start extended diagnostics
```

When you are ready to return to automatic boot mode, set switch 6 **UP** and reboot by selecting **1**, **2**, **3,** or **4**. Rebooting with switch 6 in the **UP** position will cause the router to boot router software automatically in the order and manner you have specified.

1. Retry Reboot in Boot Procedure Order

When in Manual Boot mode, you can reboot the router in the boot procedure order by selecting option **1**, '`Retry start-up`'. The boot procedure order is either one you have specified or the default order. The default order is to boot from FLASH memory and then the network (if defined). If you wish to boot from the network and/or alter the boot procedure order, refer to *Booting from the Network*.

2. Manual Boot from FLASH

If you wish to perform a manual boot from FLASH, select **2** from the main boot procedure menu. The router will attempt to boot from FLASH. If unsuccessful, the router will return to manual boot mode. (When you first receive the router, the router defaults to booting from FLASH during power-up or automatic reboot.)

Booting from the Network

Once you have installed router software on a network TFTP server, you can have the router boot across the LAN. Network booting requires three parameters:

- the boot IP address
- the TFTP boot server address
- the router software filename on the server

The boot IP address is the router LAN IP address used *during* the boot procedure. This address may differ from the LAN IP address that the router is ultimately assigned. This address is different so that a system can be booted from one subnetwork and then moved to its operational network, if necessary.

The boot IP address is of the form:
`zzz.zzz.zzz.zzz`.

The TFTP boot server address is specified as:
`tftp@xxx.xxx.xxx.xxx`

where `xxx.xxx.xxx.xxx` is the LAN IP address of the boot server. The filename must be in the format `yyyyyyyy.yyy`, similar to the DOS filename format.

Note that once you have set a TFTP server address, it will be assigned to the router software TFTP facility. This server address will then be used whenever a server address is not explicitly specified, including when the **copy** command is in the form:

```
copy tftp:filename kernel.f2k
```

Manual Boot from Network

First, you have to define permanent network boot parameters using selection **5**. Then, select **3** from the main boot procedure menu to perform a manual boot from the network. The router will attempt to boot from the network using the permanent network boot parameters you have specified.

If you have not defined network boot parameters, the router attempts to locate a BOOTP or RARP server on the network.

BOOTP can be used to supply an IP address, a TFTP Server IP address, and a filename.

RARP is used to obtain an IP address, given the MAC address. The router assumes that the RARP server is also capable of performing the duties of a TFTP Server and will request the filename kernel.f2k or the filename assigned when setting permanent network boot parameters.)

If a BOOTP or RARP server exists and is properly configured with the router's MAC address, the router will boot from the network. If unsuccessful, the router will return to manual boot mode.

Overriding Permanent Network Boot Parameters

You can temporarily override permanent network boot parameters when performing a network boot. When the router is in Manual Boot mode, select option **4**, `'boot from specific file'`, from the main boot procedure menu. Set the network boot parameters; the current default (permanent) parameters are as shown. After setting the parameters, hit return and the router will boot from the network using the temporary boot parameters. If unsuccessful, the router will return to manual boot mode.

Configure Boot System

1. If you wish to specify permanent network boot parameters, boot the router in Manual Boot mode.

2. Then select **5**, `'Configure boot system'`, from the main boot procedure menu to set permanent values.

3. Select **2**[2], **3**, and **4** to set the three boot parameters described above. After setting permanent network boot parameters, you can change the boot procedure order and/or perform a manual boot from the network.

4. Select **4** to "Boot through the IP gateway"; In this procedure, the router on the local LAN can boot from a boot server not connected directly. Instead, the path to the boot server can include other networks (including WAN, if adequate routers exist). The gateway must be located on the local LAN and reachable by the local router.

Boot Procedure Order

You can specify whether the router boots from FLASH first, a network TFTP server first, or never automatically reboots.

1. To set the order, select **1** under `'Configure boot system'` option **5**.

2. To boot from FLASH first, enter **1**; to boot from the network first, enter **2**. If you enter **3**, the router will always go into manual boot mode; i.e., you must select the boot procedure to be performed.

2 To reset any parameter, press enter when prompted.

Other Manual Boot Options

Set Time and Date

To set the current time and date, boot the router in Manual Boot mode, and select **6** from the main boot procedure menu. Set the new date in the format MM[/DD[/YY (or YYYY)]]. Set the new time in military format HH[:MM[:SS]]). You are shown the current date and time. If you set the date to `0/0/0`, the real-time clock will be disabled.

Set Console Baud Rate

Select **7** to alter the baud rate that is used by the router to communicate over the Console port with the terminal emulation program. You can override the default rate of 9600. Remember to set the identical baud rate in your terminal emulation program.

Start Extended Diagnostics

Manual boot mode allows you to run extended diagnostics. You may want to run extended diagnostics if you suspect a hardware problem. If you select **8** from the main boot procedure menu, you will see the following display:

```
[1] DRAM test
[2] Parity test
[3] POST firmware CRC test
[4] Real-Time Clock chip test
[5] Timers and Interrupts test
[6] Multi-port UART (internal loopback) test
[7] Multi-port HDLC (internal loopback) test
[8] SCC2 External Loopback test
[9] SCC3 External Loopback test
[a] SCC4 External Loopback test
[b] Ethernet Transceiver (internal loopback) test
[-] Deselect all tests
[+] Select all tests
[.] Run selected tests
[#] Enter debugger
[/] Exit extended diagnostics (reboot)
```

Enter the number of each test that you would like run or select all tests. Then enter '**.**' to begin diagnostic testing. (All of the tests are automatically run when you power up or reboot the router.) A debugging mode is available for use primarily when you have encountered a serious problem, in consultation with customer support services.

Software Kernel Upgrades

Booting and Upgrading from the LAN

You can download a new version of the router software kernel using a TFTP server existing on the LAN. Note that only one copy of the kernel software can be saved in the router. The following steps show you how to boot the router software from the network and copy the image from the network into the router's FLASH memory.

NOTE: We strongly suggest that you use the Configuration Manager's Upgrade/Backup tool to upgrade or backup the kernel: this Configuration Manager's tool is more convenient to handle than the Command Line Interface.

Upgrade Instructions

*Read the following steps very **carefully***!

1. **WARNING: Before performing this procedure, make sure that you can successfully boot from the network using the manual boot procedure option 3 or 4. Refer to the section *Booting from the Network*.**

2. Copy the router software, 'kernel.f2k' to a directory where it can be accessed by a TFTP server. The TFTP server must be on the same LAN as the target router; i.e., there must not be a router or gateway between the target system and the TFTP server. If the TFTP sever is not on the same network as the target router, enter the gateway in the boot menu as described in the previous section.

3. Log in to the Command Line Interface.

4. Enter `reboot` using the Command Line Interface to synchronize the file system and reboot the router. Since the kernel is no longer stored in FLASH, the router will try to boot from the network. If you have never set permanent boot parameters, the router attempts to locate a BOOTP or RARP server. If the router successfully reboots from the server, go to step 7.

5. Select **4** to boot router software from the TFTP server using temporary network boot parameters. You are prompted for: the router's boot LAN IP address, the TFTP server's IP address, the load address and the filename of the router's kernel saved on the server. Note that the LAN IP address is the address to be used during the network boot and this may differ from the IP address ultimately assigned to the router. Enter the temporary network boot parameters (hit return for the load address). If all entered information is valid, the router will boot from the network. An example follows:

```
Enter selection: 4
   Enter my IP address: 128.1.210.65
   Enter server IP address: 128.1.210.70
   Enter load address [80100]:
   Enter file name: kernel.f2k
```

   Alternatively, select **5** to set permanent network boot parameters and then boot from the network with selection **3**. You would use this option if you wish to boot from the network for a period of time before copying the software to FLASH memory.

6. After the boot is complete, verify that the boot code is running successfully.

7. When you are satisfied that the new kernel is performing as expected, copy the kernel into FLASH memory

in the router using the following command:

```
copy tftp@xxx.xxx.xxx.xxx:sfilename kernel.f2k
sync
```

where `xxx.xxx.xxx.xxx` is the TFTP server IP address, `sfilename` is the server filename of the kernel and `kernel.f2k` is the name of the file loaded from FLASH memory by the boot procedure. If you do not specify the server address, a permanent or more recent override TFTP server address will be used, if defined. Enter the **sync** command to commit the changes to FLASH memory.

WARNING: After the kernel is copied, DO NOT power down the router until you have either issued a `SYNC` command or rebooted the router. Otherwise the file is not written to FLASH memory.

8. After successfully copying the kernel to the router, set Configuration switch 2 or 6 **UP** (if you have set it down)**,** and reboot the router from FLASH memory via the `reboot` command. If you have altered the boot procedure order in any way, reset to boot from FLASH memory first. Verify the software revision number by issuing the **vers** command.

   The system is now ready to be re-configured if necessary. The configuration files are unchanged by the upgrade process.

Upgrading from the WAN Line

You can download a new version of the router software kernel using a TFTP server over the WAN line. Note that only one copy of the kernel software can be saved in the router. The following steps show you how to copy the software across the WAN line into the router's FLASH memory.

WARNING: Before performing this procedure, make sure that you can successfully access the software across the WAN line via a TFTP server.

1. Copy router software, 'kernel.f2k' to a directory where it can be accessed by a TFTP server.
2. Log in to the Command Line Interface.
3. Copy the kernel into FLASH memory in the router using the following command:

   ```
   copy tftp@xxx.xxx.xxx.xxx:sfilename kernel.f2k
   sync
   ```

   where `xxx.xxx.xxx.xxx` is the TFTP server IP address, `sfilename` is the server filename of the kernel and `kernel.f2k` is the name of the file. If you do not specify the server address, a permanent or more recent override TFTP server address will be used, if defined.

WARNING: After the kernel is copied, DO NOT power down the router until you have either issued a `SYNC` command or rebooted the router. Otherwise the file is not written to FLASH memory.

4. After successfully copying the kernel to the router, reboot the router from FLASH memory via the `reboot` command. If a problem occurs during the upgrading, try the command again (do not reboot until you have successfully copied the kernel.) If you have altered the boot procedure order in any way, be sure to reset to boot from FLASH memory first. Verify the software revision number by issuing the **vers** command.
   The system is now ready to be re-configured if necessary. The configuration files are unchanged by the upgrade process.

Backup And Restore Configuration Files

The `copy` command is used to upload configuration files to the TFTP server where the destination is in the form:

tftp@xxx.xxx.xxx.xxx:filename.ext

To successfully save configuration files to the server, the files to be saved to the server must already exist, be writeable by everyone. This restriction is part of the TFTP protocol. Also, all the files accessed by the TFTP server must be under a single "root" directory. Multiple sub-directories can exist below this root, but they must be created manually at the server. Neither the sub-directories nor the files can be created remotely.

The recommended backup procedure is to:

1. Create a directory under the TFTP root directory corresponding to the system name you want to back up.

2. Create files called SYSTEM.CNF and FILTER.DAT in this subdirectory. The files can be empty or not, but should be writeable by everyone.

3. To backup a copy of configuration files, enter:

   ```
   copy system.cnf tftp@xxx.xxx.xxx.xxx:myname/system.cnf
   copy filter.dat tftp@xxx.xxx.xxx.xxx:myname/filter.dat
   ```

   where `xxx.xxx.xxx.xxx` is the IP address of the TFTP server and `myname` the router name.

   To restore the configuration files, enter:

   ```
   copy tftp@xxx.xxx.xxx.xxx:myname/system.cnf system.cnf
   copy tftp@xxx.xxx.xxx.xxx:myname/filter.dat filter.dat
   sync
   ```

FLASH Memory Recovery Procedures

In the unlikely event that the FLASH file system becomes corrupted, you can take a number of steps to attempt to recover. Perform the following procedures in the order listed:

1. Try to repair the file system by issuing the `msfs` command. While logged in, issue a `sync` command followed by an `msfs` command. If the display shows that the file system is corrupted, verify that no other console (via TELNET) is currently modifying the file system with the `ps` command. Then attempt to repair the file system with the following commands:

   ```
   msfs fix
   sync
   ```

2. If the file system is still corrupted; i.e., you cannot write a file, you will have to reformat the file system. First, attempt to save your configuration files as explained in the section *Backup and Restore Configuration Files*. Then, while logged in, enter the following commands:

   ```
   format disk
   save
   copy tftp@xxx.xxx.xxx.xxx:kernel.f2k kernel.f2k
   sync
   ```

   The above assumes that the software presently running from RAM is correctly configured and still functional. The `save` step re-creates all the configuration files (except the FILTER.DAT file, which you

may re-create manually by typing `save filter`). The `copy` command reinstalls the operational software on the FLASH file system and `sync` commits all this information to disk.

3. In the event that the software running from RAM is not functional enough to perform those steps, you will have to boot from the network using a TFTP server, as explained in the section *Software Upgrades*.

   If you cannot issue the `format` command as explained in the previous tip, you will have to erase the FLASH file system from the boot code.

   a. Flip configuration switch 6 to the **DOWN** position and reboot the router (by powering down and up again, for example).

   b. At the manual boot menu, enter **5** to select `5. Configure boot system`, and enter the "magical" number 98. Then, move switch 2 or 6 back to its **UP** position and fasten the face plate.

   c. Reboot from the network following the steps described in the software upgrade procedure. You will notice error messages indicating that the file system is not formatted. Then log in and enter:

      ```
      format disk
      ```

   d. Recreate the configuration files either by re-entering the information or by restoring them from a TFTP server. Re-install the operational software with the command:

      ```
      copy tftp@xxx.xxx.xxx.xxx:kernel.f2k kernel.f2k
      ```

      This assumes that TCP/IP routing is enabled and that an IP address has been assigned to the Ethernet interface.

Batch File Command Execution

This feature is used to load batch files of configuration commands into the router. This allows for customization and simpler installation of the router. A script file can contain commands, comments (lines introduced by the # or ; characters) and blank lines.

There are two kinds of script files:

- A one-time script that is executed on startup (only once).
- A group of commands that can be executed at any time from the Command Line Interface with the `execute <file>` command.

One-time scripts are useful to execute the complete configuration process from a default (unconfigured) state.

The following steps describe how to proceed in order to create and execute a one-time script from Quick Start.

- Create the script on your PC using Notepad or other text editor. The command syntax can be found in the Command Line Reference manual or enter **?** on the router command line (assuming you have access to the Command Line with the console or with Telnet)..

- Select the Tools | Execute Script menu item and choose the script file you just prepared. When you click OK, the script file is loaded to the router (under the name AUTOEXEC.BAT) and the router is restarted, thus executing the script.

Alternatively, you can manually transfer the script file from your PC to the router using the following method:

- Start the TFTP server on your PC and set the root directory where the script file is located

- Use the following command to copy the script file to the router file system:
  ```
  copy tftp@<PC_IP_address>:<PC_file> <router_file>
  ```

- To process the commands in the script file, you can either reboot your router (if the script file was copied under the name AUTOEXEC.BAT onto the router) or use the command execute <file>.

Notes: If present, the file AUTOEXEC.BAT is renamed AUTOEXEC.OLD before it is executed, so that it is only run once. If you clear the router configuration with the Reset Defaults button of the Upgrade/Backup tool or the reboot default command, the AUTOEXEC.OLD is renamed back to AUTOEXEC.BAT and re-run after the boot up, thus restoring your configuration.

You can include the commands rename autoexec.old autoexec.bat or reboot in a script file: there is no limitation on the commands that you might define in your scripts. The rename command is useful if you need the script to execute on every startup, whereas the reboot command is useful to apply changes and have them take effect (almost) immediately. However, be aware of the following caution note.

Caution: If you create a one-time script file (copied to the router under the name AUTOEXEC.BAT), do not include both the following commands: rename autoexec.old autoexec.bat and reboot. This would result in an endless loop of starting the router, executing the script, restarting the router, re-executing the script.

Chapter 7. Troubleshooting

Software problems usually occur when the router's software configuration contains incomplete or incorrect information.
This chapter discusses:

- Diagnostic tools that are available to help identify and solve problems that may occur with your router
- Symptoms of software configuration problems
- Actions for you to take, and also lists system messages

Diagnostic Tools

Using LEDs

Most hardware problems can be diagnosed and solved by checking the LEDs on 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 (modem link)

If the Power (PWR) light is off:

- Check that the power cord is firmly plugged into the back panel of the 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	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	5 to 10 sec	1. Check your ATM or ADSL cable. 2. Check the physical connection from your router to the DSLAM (Central Office).

LINK - amber		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 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.

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 the Configuration Manager) or from TELNET.

Accessing History Log through TELNET

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

2. Click **Connect.**

Accessing History Log through the 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.

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 at the console, 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 and green.

Instructions

1. Start a DOS Window:

a. Select **Start** from the Windows 95 taskbar.

b. Select **Programs**.

c. Select **MS-DOS Prompt**.

2. Issue the PING Command:

In the DOS window, type the command:

`ping <IP address>`

Example: `ping 192.168.254.254`

Interpretation and Troubleshooting

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 are in 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 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 router configuration with your 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 the 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 the User Guide, Appendix E, *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

- Make 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).
- Check that a bridging default destination has been configured and is enabled.
- Be sure to reboot if the bridging destination or status has been changed.
- Check that bridging is enabled locally (use the **remote listbridge** command).

- Verify that bridging is enabled by the remote router (use the **remote list** command).
- Verify that the authentication passwords are correct.
- Reboot your PC if you have Windows for Work Groups.
- In Windows 95, do not forget to declare shared disk directories. Check the sharing properties on your C: drive.
- In the Terminal Window, check that calls are answered from the remote router.
- Check also for any PAP/CHAP errors for the remote router.

If TCP/IP Routing

- Check that Ethernet LAN TCP/IP Routing has been enabled (**eth list** command).
- 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 same subnetwork
- Reboot if you have made any IP address, control or protocol option changes.
- Check that the IP address of the station/network connected to the LAN beyond the remote router is correct, as well as the associated subnet mask.
- If the remote router WAN IP address and subnet mask are required, check that they have been specified correctly.
- Check that a default route has been specified, if needed.
- Be sure to reboot if IP addresses, control or protocol option changes have been made.
- Check that you are using an Ethernet cable.
- Check that IP routing is enabled at both ends.
- The IP address must be within the valid range for the subnet.
- Verify that the IP and gateway addresses are correct on the PC.
- Windows 95 may remember MAC addresses: if you have changed MAC addresses, reboot the router and the PC.
- In Windows 3.1., check that the TCP driver is installed correctly. Ping (**ping** command) your PC's IP address from the PC.
- Successful "pinging" results let you know that the TCP driver is working properly.
- If you have changed an IP address to map to a different MAC device, and Ping or IP fails, reboot your PC.
- Use the **Iproutes** command, to verify which router's name is the default gateway (this cannot be 0.0.0.0).

If IPX Routing

- Check that IPX Routing has been enabled and the remote end is enabled for IPX routing

- 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.
- Validate that the IPX WAN network number matches the remote router's WAN network number.
- 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.
- Check that IPX SAPs correctly identify the servers and applications on the remote network and have valid network numbers, node numbers, etc.
- Be sure to reboot if IPX addresses, routes, SAPs or control has been changed.

If the router fails to negotiate IPX:

- Make sure that at least one WAN number is not equal to zero at one end of the link.
- The server must have an IPX route to the remote LAN.
- The Novell server needs to have burst mode turned on.
- Large Internet packets have to be turned on:

  Novell 3.12and later.
  Client needs VLM.EXE, net.cfg: large Internet packets=ON, Pburst=5

If you can't see the server SAPs:

- Check the frame types using the **eth list** command and that they are the same on both routers.
- Check that the Ethernet cable is correctly plugged in.
- Make sure that the Novell server is up.

Problems Accessing the Router via TELNET

- Ensure that the router has a valid IP address.
- Check that the Ethernet cable is plugged in.

Problems Downloading Software

- Ensure that a TFTP server is properly set up to locate the router software
- Verify that the router is loading from the network and not from FLASH.

System Messages

System messages are displayed on the terminal and sent to a log file (if you have opened one). The messages listed in this section are time-stamped informational and error messages. The messages are in the following format:

dd+hh:mm:ss:nn sysfunc: message

where:

dd	date in xx/xx/xx format as specified during router initialization
hh	number of hours (military format)
mm	number of minutes
ss	number of seconds
nn	hundredths of seconds
sysfunc	software function
message	message

The following are some examples of the messages:

12/05/1997-16:31:17:ADSL: Startup initiated
12/05/1997-16:36:26:ADSL: Startup handshake in progress

Time-Stamped Messages

<router/user> didn't negotiate our IP address correctly
Explanation: The remote router did not negotiate the IP address options as was expected by the local router.

<router/user> terminated IPCP prematurely
Explanation: IP failed to negotiate. Try to change the remote or the source WAN IP address.

Far Avg SQ #: <2-digit number> dB [4-digit number]
Explanation: Message about the average signal quality for the remote router. This information appears during modem startup and should be ignored unless requested by Technical Support.

Authorization failed
Explanation: PAP cannot be negotiated.

Can't agree with <router/user> on what their IP address should be
Explanation: The IP address entry for the remote router in the remote router database does not match with what the local router expects.

Can't obtain an IP address from <router/user>: one is needed in single user mode
Informative message.

Can't supply an IP address to <router/user>
Explanation: The remote end requests an IP address from the local end, which cannot supply it.

Cannot remove SYSTEM.CNF
Informative message.

Connecting to <router/user> @ <number> over <link/number>
Explanation: The local router is trying to connect to the specified remote destination.

Data Mode
Explanation: The connection is established and operational.

Duplicate IPX route to <router/user>
Explanation: There exists two routes to the same IPX destination. One route needs to be removed.

Duplicate IPX SAP <SAP number> to <router/user>
Explanation: There exists two IPX SAPs for the same IPX destination. One SAP needs to be removed.

Duplicate route <IP route> found on remote <router/user>
Explanation: There exists two IP routes to the same IP destination. One route needs to be removed.

Idle
Explanation: data is not being transmitted.

IP is configured for numbered mode with <router/user>, but no address for it
Explanation: On one end of the connection, remote entries have been configured for numbered mode. On the other end, remote entries have been configured for unnumbered mode. Both ends cannot communicate with each other.

No Signal Detected -- Check WAN Cable!
Explanation: (SDSL-specific error message) Your SDSL router cannot establish connectivity. Check your physical line.

No system name known - using defaults
Explanation: The router does not have a system name. For PAP/CHAP negotiation, the router will use a default name and password.

Note: IPX is misconfigured for <router/user> - no IPX WAN network
Explanation: IPX WAN address is wrong or missing.

Note: There is no IPX route statically defined for <router/user>
Informational message.

PPP: Peer not negotiating <IP | BNCP | IPX | CCP> right now
Explanation: One end of the network is not negotiating the same protocol as the other end.

Remote <router/user> didn't accept our CHAP password
Informational message.

Remote <router/user> does not respond to LPC echo. Link closed
The connection was terminated.

Remote <router/user> on <channel> didn't authenticate in time
Explanation: PPP authentication protocol did not succeed.

Remote <router/user> refuses to authenticate
Informational message.

Remote <router/user> tried to use PAP when CHAP was expected
Explanation: The remote end negotiated PAP while its minimum security level in the remote database was set to CHAP.

Remote <router/user> used wrong password <CHAP | PAP>
Explanation: The remote end has used an invalid password during CHAP or PAP security authentication.

Remote didn't accept our CHAP password
Explanation: The router attempted CHAP security authentication but the remote end rejected the password.

Remote on <interface> didn't authenticate in time
Informational message.

Remote on <interface> rejected our password with PAP
Informational message.

Remote on <interface> refuses to authenticate with us
Explanation: The remote destination refused to participate in the PAP/CHAP authentication process.

Startup failed
Explanation: The ATM modem could not synchronize with the remote end. The user should call Technical Support.

Startup failed: failure code = <number>, Status [code]
Explanation: The ATM modem could not synchronize with the remote end. The user should call Technical Support

TelnetD
Explanation: Connection accepted. A remote configuration session has been established.

User <router/user> is disabled in remote database
Informative message.

User <router/user> not found in remote database <PAP | CHAP>
Explanation: The authentication is coming from an unknown remote router.

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 the Configuration Manager) or from Telnet. Follow the steps described below:

1. If accessing the logging utility through Telnet, enter the router's IP address and connect.
   If accessing the logging utility through the Configuration Manager, select **Tools** and **Terminal Window** (the
   console cable is required).

2. Login with your administration password into the router (e.g. "`admin`").

3. Enter the command **system history** to view the buffer contents.

Other logging commands:

- If you wish to monitor your router activity at all time, enter the command **`system log start`** to view a continuous log**.** This command will not work in a Terminal Window session, but only from Telnet.

- **`System log status`** is used to find out if other users, including yourself, are using this utility.

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

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

NOTE: The History Log is preserved across reboots but not across power outages or power down.

How To Obtain Technical Support

If you are having difficulty configuring the router, take the following steps:

- Review the sections in the *User Guide* on installing router hardware.
- Check that all cables and connectors have been attached properly.
- Verify that power has been attached.
- Verify that the Power-On -Self -Test displays the correct existence of all ordered hardware.
- Review Chapter 3, *Configuring Router Software* and Chapter 6, *Troubleshooting.*

Before you contact Technical Support, please have the following information ready:

- Router model number
- Router software version
- Date of purchase
- Type of Operating System (Windows 95, Windows for Workgroups, or Windows NT)
- Description of the problem
- List of other equipment such as personal computers, modems, etc. and third party software you are using, including revision levels.

How to contact Technical Support in the U.S.	Addresses / Numbers
Telephone	1-408-364-8300
E-Mail	support@flowpoint.com
Fax	(408) 364-8301
Address	FlowPoint Corp. 180 Knowles Drive, Suite 100 Los Gatos, California 95030
Web Site	http://www.flowpoint.com

Appendix A. 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/RFC 1490 with IP Routing configuration
- RFC 1483/RFC 1490 with IPX Routing configuration
- RFC 1483/RFC 1490 with Bridging configuration
- RFC 1483MER? RFC 1490MER with IP Routing configuration
- FRF8 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 WAN link.

Note: You may want to review one of the sample configurations, refer to the *Sample Configurations* section in chapter 3.

Configuring PPP with IP Routing

PPP with IP Routing		
STEPS	**COMMANDS**	**YOUR SETTINGS**
System Settings		
System Name	system name < name>	…….
System Message	system msg <message>	…….
Authentication Password	system passwd < password>	…….
Ethernet IP Address	eth ip addr <ipAddr> <ipNetMask>	…….
DHCP Settings	dhcp set valueoption domainname <domainname> dhcp set valueoption domainnameserver <ipAddr>	……. ……..
Change Login	system admin < password>	…….
Remote Routers		
New Entry	remote add <remoteName>	…….
Link Protocol	remote setProtocol PPP <remoteName>	…….
PVC or DLCI	remote setPVC <vpi number>*<vci number> <remoteName> remote setDLCI <number><remoteName>	……. …….
Security	remote setAuthen <protocol> <remoteName>	…….
Remote's Password	remote setPasswd <passwd> <remoteName>	…….
Bridging On/Off	remote disBridge <remoteName>	…….
TCP/IP Route Address	remote addIproute <ipNet> <ipNetMask> <hops> <remoteName>	…….
If NAT is enabled: To enable NAT -and- You may need to enter a Source WAN Port Addr	remote setIpTranslate on <remoteName> remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>	…….
If NAT is OFF: You may need to enter a Source WAN Port Addr	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>	…….
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	eth ip enable eth ip firewall <on | off>	……. …….
IPX Routing	eth ipx disable	…….
Store **Reboot**	Save Reboot	

Configuring PPP with IPX Routing

PPP with IPX Routing		
STEPS	**COMMANDS**	**YOUR SETTINGS**
System Settings		
System Name	system name < name>	…….
System Message	system msg <message>	…….
Authentication Password	system passwd < password>	…….
Ethernet IP Address	eth ip addr <ipAddr> <ipNetMask>	…….
DHCP Settings	dhcp set valueoption domainname <domainname>	…….
	dhcp set valueoption domainnameserver < ipAddr>	……..
Change Login	system admin < password>	…….
Ethernet IPX Network #	eth ipx addr <ipxNet#> eth ipx frame <type>	……. …….
Remote Routers		
New Entry	remote add <remoteName>	…….
Link Protocol	remote setProtocol PPP <remoteName>	…….
PVC or DLCI	remote setPVC <vpi number>*<vci number> <remoteName> remote setDLCI <number> <remoteName>	……. …….
Security	remote setAuthen <protocol> <remoteName>	…….
Remote's Password	remote setPasswd <passwd> <remoteName>	…….
Bridging On/Off	remote disBridge <remoteName>	…….
IPX Routes Add	remote addIpxroute <ipxNet> <metrics> <ticks> <remoteName>	……..
IPX SAPs Add	remote addIpxsap <service_name> <ipxNet> < ipxNode> <socket> <type> <hops> <remoteName>	…….
	remote setIpxaddr <ipxNet> <remoteName>	
IP and IPX Routing		
TCP/IP Routing	eth ip disable	…….
IPX Routing	eth ipx enable	…….
Store **Reboot**	Save Reboot	

Configuring PPP with Bridging

PPP with Bridging		
STEPS	**COMMANDS**	**YOUR SETTINGS**
System Settings		
System Name	system name < name>	……
System Message	system msg <message>	……
Authorization Password	system passwd < password>	……
DHCP Settings	dhcp set valueoption domainname <domainname>	……
	dhcp set valueoption domainnameserver < ipAddr >	……..
Change Login	system admin < password>	……
Remote Routers		
New Entry	remote add <remoteName>	……
Link Protocol	remote setProtocol PPP <remoteName>	……
PVC or DLCI	remote setPVC <vpi number>*<vci number> <remoteName> remote setDLCI <number><remoteName>	……..
		……
Security	remote setAuthen <protocol> <remoteName>	……
Remote's Password	remote setPasswd <passwd> <remoteName>	……
Bridging On/Off	remote enaBridge <remoteName>	
IP and IPX Routing		
IP Routing	eth ip disable	……
IPX Routing	eth ipx disable	……
Store **Reboot**	save reboot	

Configuring RFC 1483 / RFC 1490 with IP Routing

RFC 1483 / RFC 1490 with IP Routing		
STEPS	**COMMANDS**	**YOUR SETTINGS**
System Settings		
System Message	system msg <message>	……
Ethernet IP Address	eth ip add <ipNet> <ipNetMasK>	……
DHCP Settings	dhcp set valueoption domainname <domainname>	……
	dhcp set valueoption domainnameserver < ipAddr>	……..
Change Login	system admin < password>	……
Remote Routers		
New Entry	remote add <remoteName>	……
Link Protocol/PVC* (for ATM routers)	remote setProtocol RFC1483 <remoteName>	……
	remote setPVC <vpi number>*<vci number><remoteName>	……..
Link Protocol /DLCI** (for Frame Relay Routers)	remote setProtocol FR <remoteName>	……
	remote setDLCI <number><remoteName>	……
Bridging On/Off	remote disBridge <remoteName>	……
TCP/IP Route Address	remote addiproute <ipNet> <ipNetMask> <hops> <remoteName>	……
If NAT is enabled: To enable NAT -and- You must enter a Source WAN Port Address	remote setIpTranslate on <remoteName>	……
	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>	……
If NAT is OFF: You may need to enter a Source WAN Port Address	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName>	……
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	eth ip enable eth ip firewall <on | off>	…… ……
IPX Routing	eth ipx disable	……
Store **Reboot**	Save Reboot	

*Enter this information if you are using RFC 1483 in an ATM environment.
**Enter this information if you are using RFC 1490 in a Frame Relay environment.

Configuring RFC 1483 / RFC 1490 with IPX Routing

RFC 1483 / RFC 1490 with IPX Routing		
STEPS	**COMMANDS**	**YOUR SETTINGS**
System Settings		
System Message	system msg < message>	……
Ethernet IP Address	eth ip addr <ipAddr> <ipNetMask>	……
DHCP Settings	dhcp set valueoption domainname <domainname>	……
	dhcp set valueoption domainnameserver < ipAddr>	……..
Ethernet IPX Network #	eth ipx addr <ipxNet>	……
	eth ipx frame <type>	……
Change Login	system admin < password>	……
Remote Routers		
New Entry	remote add <remoteName>	……
Link Protocol/PVC* (for ATM routers)	remote setProtocol RFC1483 <remoteName>	……
	remote setPVC <vpi number>*<vci number> <remoteName>	……
Link Protocol /DLCI** (for Frame Relay Routers)	remote setProtocol FR <remoteName>	……
	remote setDLCI <number><remoteName>	……
Bridging On/Off	remote disBridge <remoteName>	……
IPX Routes Add	remote addIpxroute <ipxNet> <metrics> <ticks> <remoteName>	……
IPX SAPs Add	remote addIpxsap <service_name> <ipxNet> < ipxNode> <socket> <type> <hops> <remoteName>	……
	remote setIpxaddr <ipxNet> <remoteName>	……
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	eth ip disable eth ip firewall < on | off >	…… ……
IPX Routing	eth ipx enable	……
Store **Reboot**	Save Reboot	

*Enter this information if you are using RFC 1483 in an ATM environment.
**Enter this information if you are using RFC 1490 in a Frame Relay environment.

Configuring RFC 1483 / RFC 1490 with Bridging

RFC 1483 / RFC 1490 with Bridging		
STEPS	**COMMANDS**	**YOUR SETTINGS**
System Settings		
System Message	system msg <message>	…….
DHCP Settings	dhcp set valueoption domainname <domainname>	…….
	dhcp set valueoption domainnameserver < ipAddr>	……..
Change Login	system admin < password>	…….
Remote Routers		
New Entry	remote add <remoteName>	…….
Link Protocol/PVC* (for ATM routers)	remote setProtocol RFC1483 <remoteName>	…….
	remote setPVC <vpi number>*<vci number> <remoteName>	……..
Link Protocol /DLCI** (for Frame Relay Routers)	remote setProtocol FR <remoteName>	…….
	remote setDLCI <number><remoteName>	…….
Bridging On/Off	remote enaBridge <remoteName>	…….
IP and IPX Routing		
IP Routing	eth ip disable	…….
IPX Routing	eth ipx disable	…….
Store **Reboot**	save reboot	

*Enter this information if you are using RFC 1483 in an ATM environment.
**Enter this information if you are using RFC 1490 in a Frame Relay environment.

Configuring RFC 1483MER / RFC 1490MER with IP Routing

RFC 1483MER/RFC 1490MER with IP Routing		
STEPS	**COMMANDS**	**YOUR SETTINGS**
System Settings		
System Message	system msg <message>	……
Ethernet IP Address	eth ip add <ipNet> <ipNetMasK>	……
DHCP Settings	dhcp set valueoption domainname < ipAddr>	……
	dhcp set valueoption domainnameserver <domainnameserver>	……..
Change Login	system admin < password>	……
Remote Routers		
New Entry	remote add <remoteName>	……
Link Protocol/PVC* (for ATM routers)	remote setProtocol RFC1483MER <remoteName>	……
	remote setPVC <vpi number>*<vci number><remoteName>	……..
Link Protocol /DLCI** (for Frame Relay Routers)	remote setProtocol MER <remoteName>	……
	remote setDLCI <number><remoteName>	……
Bridging On/Off	remote disBridge <remoteName>	……
TCP/IP Route Address	remote addiproute <ipNet> <ipNetMask><IpGateway> <hops> <remoteName>	……
If NAT is enabled: To enable NAT,enter:	remote setIpTranslate on <remoteName>	……
-and- Enter a Source WAN Port Addr	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName> ***	……
If NAT is not enabled: You may need to enter a Source WAN Port Addr	remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName> ***	……
IP and IPX Routing		
TCP/IP Routing	eth ip enable	……
(Internet Firewall)	eth ip firewall <on | off>	……
IPX Routing	eth ipx disable	……
Store	save	
Reboot	reboot	

*Enter this information if you are using RFC 1483 in an ATM environment.
**Enter this information if you are using RFC 1490 in a Frame Relay environment.
* **The mask is the mask of the remote network

Configuring FRF8 with IP Routing

RFC 1483FR with IP Routing		
STEPS	**COMMANDS**	**YOUR SETTINGS**
System Settings		
System Message	System msg <message>	……
Ethernet IP Address	eth ip add <ipNet> <ipNetMasK>	……
DHCP Settings	dhcp set valueoption domainname < ipAddr>	……
	dhcp set valueoption domainnameserver <domainnameserver>	……..
Change Login	system admin < password>	……
Remote Routers		
New Entry	Remote add <remoteName>	……
Link Protocol/PVC	Remote setProtocol FRF8 <remoteName>	……
	Remote setPVC <vpi number>*<vci number> <remoteName>	……..
Bridging On/Off	Remote disBridge <remoteName>	……
TCP/IP Route Address	Remote addiproute <ipNet><ipNetMask><hops><remoteName>	……
If NAT is enabled: To enable NAT -and- You must enter a Source WAN Port Addr	Remote setIpTranslate on <remoteName> Remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName> *	…… ……
If NAT is not enabled: You may need to enter a Source WAN Port Addr	Remote setSrcIproute <ipAddr> <ipNetMask> <hops> <remoteName> *	……
IP and IPX Routing		
TCP/IP Routing (Internet Firewall)	eth ip enable eth ip firewall <on | off>	…… ……
IPX Routing	eth ipx disable	……
Store **Reboot**	Save Reboot	

***** The mask is the mask of the remote network

Appendix B. Configuring IPX Routing

IPX Routing Concepts

IPX Routing is established by entering all remote routers in the remote router database to which this router will connect. For each remote router, you enter network addresses and services that may be accessed beyond the remote router. You also enter a network number for the WAN link. After specifying the route addressing and services, you then enable IPX routing across the Ethernet LAN.

When IPX traffic is for network segments and servers beyond the remote router, the target router's routing information table must be statically seeded. Static seeding ensures that the target router connects to the appropriate remote router. After the link is established, RIP broadcast packets will dynamically add to the target router's routing table. Seeding the routing table is not necessary when a target router never connects; it will discover remote networks beyond the calling router as soon as RIP updates arrive (provided the remote router supports RIP). However, for watchdog spoofing to work, the remote IPX routes for network segments and servers should be defined.

Configure IPX Routing

Configuring your router for IPX routing can be rather tricky. The following section will guide you through the configuration process for IPX routing. Remember that the elements of PPP Authentication must be completed *before* attempting the IPX routing configuration. The full router configuration for simple IPX routing includes the following elements:

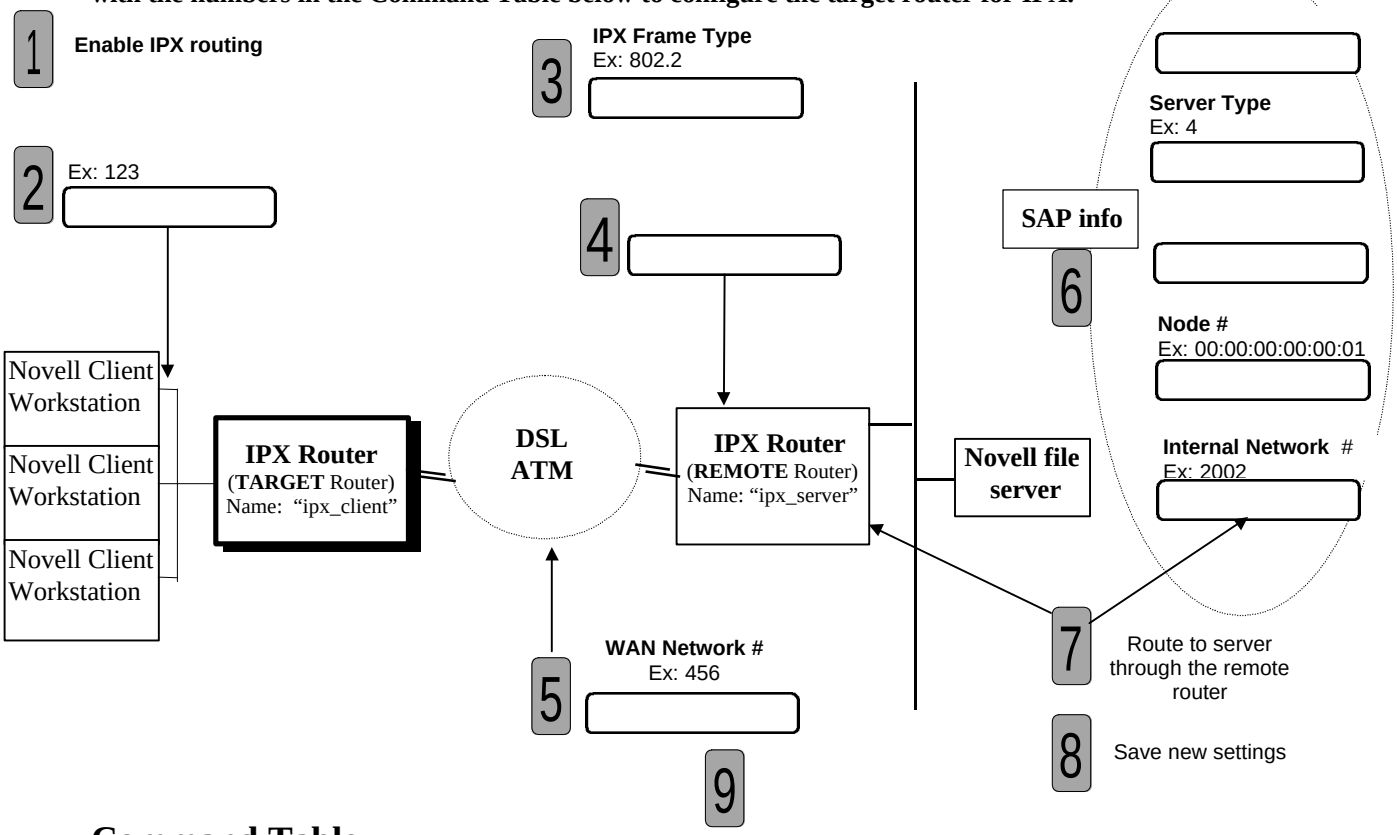
- PPP Authentication
- IPX routing (this section)

The following section, *Step 1: CollectYour Network Information for the Target Router*, provides a configuration diagram and a command table to assist you with the configuration of the target router.

Step2: Review Your Settings lists the commands used to review the IPX configuration and provides a configuration example.

Step 1: Collect Your Network Information for the Target (Local) Router

remote side of the WAN link has all of the file and print services.
Enter the needed network information in the blank boxes of the diagram. Then match the boxes numbers with the numbers in the Command Table below to configure the target router for IPX.



Command Table

These commands are used to configure the Target (client-side) router (**ipx_client** in our example).
Login with the password **admin.**

IPX Commands with examples	Ref #	Comments
eth ipx ena	1	Enable IPX Routing
eth ipx addr 123	2	Set the local 'wire' address
eth ipx frame 802.2	3	Set the Frame Type
remote add ipx_server	4	Add a connection name
remote setipxaddr 456 ipx_server	5	Set the WAN network # (common to both sides)
remote addipxsap SERVER2 2002 00:00:00:00:00:01 0451 4 1 ipx_server	6	Add a file server (SAP)
remote addipxroute 2002 1 4 ipx_server	7	Add a route to the server
Save	8	Save your settings
Reboot	9	Reboot for changes to take effect

NOTE: The Remote (server side) router (called "ipx_server" in our example) must be configured with an IPX route to the Target (client side) router's external network # (see 2).

Step 2: Review Your Settings

Commands used to review your IPX configuration:

- **eth list**
- **remote list**
- **ipxsaps**

```
> eth list
ETHERNET INFORMATION FOR <ETHERNET/0>
  Hardware MAC address................ 00:20:6F:02:4C:35
  Bridging enabled..................... no
  IP Routing enabled................... no
    Firewall filter enabled ........... yes
    Process IP RIP packets received.... yes
    Send IP RIP to the LAN............. yes
    Advertise me as the default router. Yes
    Receive default route using RIP.... yes
  IP address/subnet mask............... 192.84.210.123/255.255.255.0
  IP static default gateway............ none
  IPX Routing enabled................... yes
  External network number............ 00000123
  Frame type......................... 802.2
```

```
> remote list
INFORMATION FOR <ipx_server >
  Status............................... enabled
  Protocol in use.................….. PPP
  Authentication....................... enabled
  Authentication level required........ PAP
  IP address translation............... on
  Compression Negotiation.............. off
Source IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Remote IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Send IP RIP to this dest............ no
  Receive IP RIP from this dest........ no
  Send IP default route if known....... no
  Receive IP default route using RIP... no
  Keep this IP destination private..... yes
  Total IP remote routes............... 0
IPX network number................... 00000456
Total IPX remote routes............... 1
        00002002/1/4
Total IPX SAPs....................... 1
   SERVER2 00002002 00:00:00:00:00:01 0451 0004 1
Bridging enabled..................... no
   Exchange spanning tree with dest... no
   Mac addresses bridged............... none
```

```
> ipxsaps
Service Name    Type  Node number  Network Skt Hops

SERVER2          4  000000000001:00002002:0451 1
```

Commands used to set and modify your IPX Settings:

1 **eth ipx ena**

2 **eth ipx addr <Ethernet network number>**

Ex: eth ip addr 123

3 **eth ipx frame [802.2 | 802.3 | DIX]**

Ex: eth ip frame 802.2

4

5 **remote setipxaddr <WAN network #> <remote name>**

Ex: remote setipxaddr 456 ipx_server

7 **remote addipxroute <IPX net #> <hops> <ticks> <remote name>**

Ex: remote addipxroute 2002 1 4 ipx_server

6 **remote addipxsap <server name> <Internal IPX net #> <IPX node address> <socket> <server type> <hops> <remote name>**

Ex: remote addipxsap SERVER2 2002 0:00:00:00:00:01 451 4 2 ipx_server

Index

A

advanced features
  bridge filtering, 21
  unique system passwords, 21

B

boot options
  baud rate for console, 157
  booting from the network, 155
  extended diagnostics, 157
  manual boot mode, 154
  time and date, 157
bridging
  configuration information (with PPP), 30
  configuration information (with RFC 1483), 34
  configuration information (with RFC 1490), 34
  configuration table (with PPP), 43
  configuration table (with RFC 1483/RFC 1490), 46
  general information, 12
  test, 50
bridging filtering, 65
bridging filtering commands, 142

C

CHAP, 54, 55
Command Line Interface
  access, 9
commands
  ?, 83
  addIpRoute, 107
  addIpxSap, 108
  addServer, 108
  adsl ?, 121
  adsl restart, 121
  adsl speed, 121
  adsl stats, 122
  atm ?, 123
  atm pcr, 123, 124
  atm reset, 123
  atm save, 123
  atm speed, 124
  bi, 84
  bi list, 84
  copy, 149
  delete, 151
  dhcp ?, 133
  dhcp add, 133
  dhcp bootp allow, 134
  dhcp bootp disallow, 134
  dhcp bootp file, 135
  dhcp bootp tftpserver, 135
  dhcp clear addresses, 135
  dhcp clear expire, 135
  dhcp clear valueoption, 136
  dhcp del, 136
  dhcp disable, 137
  dhcp list, 137
  dhcp list definedoptions, 138
  dhcp list lease, 140
  dhcp set addresses, 140
  dhcp set expire, 140
  dhcp set lease, 141
  dhcp set valueoption, 141
  dir, 150
  erase all, 146
  erase atm25, 146
  erase dod, 147
  erase eth, 147
  erase filter, 147
  erase sys, 147
  eth ?, 100
  eth ip addr, 100
  eth ip addroute, 101
  eth ip defgateway, 101
  eth ip disable, 101
  eth ip enable, 102
  eth ip firewall, 102
  eth ip options, 102
  eth ip ripmulticast, 103
  eth ipx addr, 103
  eth ipx disable, 104
  eth ipx enable, 104
  eth ipx frame, 104
  eth list, 105
  exit, 84
  filter br ?, 142
  filter br add, 142
  filter br del, 142
  filter br list, 143
  filter br use, 143
  format disk, 150
  hdsl ?, 126
  hdsl save, 126
  hdsl speed, 126
  hdsl terminal, 127
  help, 83
  ifs, 85
  ipifs, 85
  iproutes, 85
  ipxroutes, 86
  ipxsaps, 86
  isdn ?, 128
  isdn list, 128
  isdn save, 128
  isdn set switch, 129
  login, 86
  logout, 86
  mem, 87
  mlp summary, 87
  msfs, 150
  ping, 87
  ps, 88
  reboot, 89
  remote ?, 106
  remote add, 106
  remote addIpxRoute, 107
  remote del, 108
  remote delIpRoute, 109
  remote delIpxRoute, 109

remote delIpxSap, 109
remote delOurPasswd, 109
remote delOurSysName, 110
remote delServer, 110
remote disable, 110
remote disAuthen, 111
remote disBridge, 111
remote enaAuthen, ***111***
remote enable, ***111***
remote enaBridge, ***112***
remote list, ***112***
remote listBridge, ***113***
remote listIpRoute, 113
remote listIpxRoute, 113
remote listIpxSap, 114
remote listPhone, 114
remote setatmtraffic scr mbs, 124
remote setAuthen, 115
remote setBrOptions, 115
remote setCompression, 115
remote setdlci, 129
remote setIpOptions, 116
remote setIpxAddr, 117
remote setOurPasswd, 117
remote setOurSysName, 117
remote setPasswd, 118
remote setprotocol, 129
remote setProtocol, 118
remote setPVC, 118
remote setRmtIpAddr, 119
remote setSrcIpAddr, 119
remote stats, 119
remote statsclear, 120
rename, 151
save all, 144
save atm25, 144
save dhcp, 145
save dod, 144
save eth, 145
save filter, 145
save sys, 145
sdsl ?, 131
sdsl save, 131
sdsl speed, 131
sdsl terminal, 132
setIpTranslate, 117
sync, 151
system ?, 92
system addserver, 92
system addsnmpfilter, 93
system addtelnetfilter, 93
system addudprelay, 93
system admin, 92
system authen, 94
system bootpserver, 94
system community, 94
system delserver, 94
system delsnmpfilter, 95
system deltelnetfilter, 95
system deludprelay, 95
system history, 96
system list, 96
system log, 96
system msg, 97
system name, 97
system passwd, 97
system snmpport, 98
system supporttrace, 98
system telnetport, 98
system wan2wanforwarding, 99
vers, 90
configuration
example, 51, 59
configuration files
backup/restore, 160
configuration information
FRF8 + IP, 37
PPP + bridging, 30
PPP + IP, 26
PPP + IPX, 28
RFC 1483 + bridging, 34
RFC 1483 + IP, 31
RFC 1483 + IPX, 33
RFC 1483MER + IP, 35
RFC 1490 + bridging, 34
RFC 1490 + IP, 26, 28, 30, 31
RFC 1490 + IPX, 33
RFC 1490MER + IP, 35
configuration tables
FRF8 + IP routing, 48
mixed network protocols, 49
PPP + bridging, 43
PPP + IP routing, 41
PPP + IPX routing, 42
RFC 1483/RFC 1490 + bridging, 46
RFC 1483/RFC 1490 + IP routing, 44
RFC 1483/RFC1 490 + IPX routing, 45
RFC 1483MER/RFC 1490MER + IP routing, 47

D

DHCP commands, 133
DHCP configuration, 66

E

encapsulation options, 18
erase commands, 146
error messages, 171
Ethernet commands, 100

F

file system commands, 149
filter br commands, 142
FLASH memory
recovery procedures, 160
FRF8, 37

H

history log, 165, 174

I

IP Firewall configuration, 65
IP routing
configuration information (with FRF8), 37
configuration information (with PPP), 26

configuration information (with RFC 1483), 31
configuration information (with RFC 1483MER), 35
configuration information (with RFC 1490), 26, 28, 30, 31
configuration information (with RFC 1490MER), 35
configuration table (with FRF8), 48
configuration table (with MAC Encapsulated Routing), 47
configuration table (with RFC 1483/RFC 1490), 44
configuration table (with RFC 1483MER/RFC 1490MER), 47
configuration tables (with PPP), 41
test, 49
IPX routing
concepts, 185
configuration information (with RFC 1483), 33
configuration information (with RFC 1490), 33
configuration sample, 185
configuration table (with PPP), 42
configuration table (with RFC 1483/RFC 1490), 45
test, 50

K

kernel
upgrade from the LAN, 158
upgrade from the WAN line, 159

L

LED sequence, 164
login password
reset, 168

M

MAC Encapsulated Routing, 35
management security, 80

N

Network Address Translation
classic NAT, 78
masquerading, 75
Network Address Translation configuration, 75
network information
example, 61
sample worksheets, 61

P

PAP/CHAP
general information, 14
password
example, 58
ping command, 166
PPP
general, 14
PPP Link Protocol, 26
protocol standards, 17

R

remote commands, 106
remote router
definition, 23
remote router database
definition, 23
RFC 1483, 26, 31
RFC 1483MER, 35
RFC 1490, 26, 31
RFC 1490MER, 35
RFCs, 17
routing
general information, 11

S

sample configuration, 59
PPP with IP and IPX, 51
RFC 1483 with IP and bridging, 59
save commands, 144
security
general information, 15
SNMP
features, 153
SNMP client validation, 80
system commands, 92
system files, 20
system level commands, 84
system messages, 171

T

TCP/IP routing
control, 55, 62
TCP/IP Routing
source and remote addresses, 32
Technical Support information, 175
Telnet, 153
Telnet client validation, 80
TFTP, 154
time-stamped messages, 171
troubleshooting
bridging, 168
console, 167
diagnosis tools, 165
factory configuration, 167
hardware problems, 167
history log, 165
IP routing, 169
IPX routing, 169
login password, 168
normal LED sequence, 164
PC connection, 167
power light off, 164
remote network access, 168
software configuration, 167
terminal window display, 167
using history log, 174
using LEDs, 164
using ping, 166