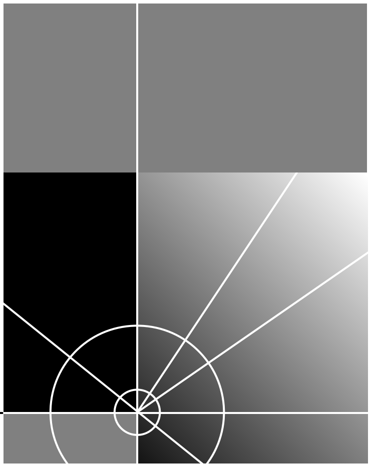
OfficeConnect™ Remote 840 SDSL Router User’s Guide

Release 1.2.0



http://www.3com.com/

Part No. 10031396 Rev. AA
May 2000

3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Portions of this documentation are reproduced in whole or in part with permission from (as appropriate).

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, Boundary Routing, EtherDisk, EtherLink, EtherLink II, LANsentry, LinkBuilder, Net Age, NETBuilder, NETBuilder II, OfficeConnect, Parallel Tasking, SmartAgent, SuperStack, TokenDisk, TokenLink, Transcend, and ViewBuilder are registered trademarks of 3Com Corporation. ATMLink, AutoLink, CoreBuilder, Dynamic*Access*, FDDILink, NetProbe, PACE and Total Control are trademarks of 3Com Corporation. 3ComFacts is a service mark of 3Com Corporation.

Artisoft and LANtastic are registered trademarks of Artisoft, Inc. Banyan and VINES are registered trademarks of Banyan Systems Incorporated. CompuServe is a registered trademark of CompuServe Interactive Services, Inc. DEC and PATHWORKS are registered trademarks of Digital Equipment Corporation. Intel and Pentium are registered trademarks of Intel Corporation. AIX, AT, IBM, NetView, and OS/2 are registered trademarks and Warp is a trademark of International Business Machines Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. PictureTel is a registered trademark of PictureTel Corporation. UNIX is a registered trademark of X/Open Company, Ltd. in the United States and other countries.

All other company and product names may be trademarks of the respective companies with which they are associated.

About This Guide

1

Overview

2

SYSTEM ADMINISTRATION

3

REMOTE SITE MANAGEMENT

5

CONFIGURING BRIDGING

6

NETWORK ADDRESS TRANSLATION USING THE OFFICECONNECT REMOTE 840

7

CONFIGURING DHCP

8

CONFIGURING DNS

9

CONFIGURING IPX ROUTING

12

CONFIGURING FILTERS

13

TROUBLESHOOTING

A

Bridging and Routing

B

IP Addressing

C

ADDRESS TRANSLATION TUTORIAL

D

USING THE CLI GUIDE

E

CONFIGURATION (NON-SETUP WIZARD) OF THE OFFICECONNECT REMOTE 840

F

TECHNICAL SUPPORT

3COM CORPORATION LIMITED WARRANTY

FCC CLASS B STATEMENT

FCC DECLARATION OF CONFORMITY

ABOUT THIS GUIDE

Introduction

This guide describes the features and advanced configuration of the OfficeConnectRemote 840 SDSL Router. The guide is intended for both first-time and experienced computer network users who are using the OfficeConnectRemote 840.

For information on the initial configuration of the unit, see the OfficeConnect Remote 840 SDSL Router Installation Guide (included in the box when your purchased your Router). That guide contains steps to get the user started accessing the Internet or telecommuting to a remote office.

This OfficeConnectRemote 840 SDSL Router User's Guide is intended to be used for advanced configuration, presenting more detailed information on the unit.

First-time users may want to read the tutorials in this Guide to help you learn more about the networking technologies used by the OfficeConnectRemote 840 SDSL Router.

The appendixes describe how to set up your router without using the Setup Wizard.

How to Use This Guide

This table shows where to find specific information in this guide.

If you are looking for:	Turn to:
OfficeConnect Remote 840 Product Overview and Configuration	Chapters 1, 2
Configuration of your Router (Remote Sites, IP Routing, Bridging, NAT, DHCP, DNS, IPX Routing)	Chapter 3 – 9
Upgrading Software	Chapter 10
Monitoring Capabilities	Chapter 11
Configuring Filters	Chapter 12
Troubleshooting	Chapter 13
Information on the difference between Bridging and Routing	Appendix A
Information about IP Addressing	Appendix B
Information on Address Translation	Appendix C
Information on using the CLI Guide	Appendix D
Information on Configuration	Appendix E
Information on Technical Support	Appendix F

These and other user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

`http://www.3com.com/ocr840`

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
i	Information note	Information that describes important features or instructions
!	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
⚡	Warning	Information that alerts you to potential personal injury

Table 2 Text Convention

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
`Syntax`	The word “syntax” means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example: To add a login user, use the following syntax: `Add user <name> password <password>` In this example, you must supply a user name for <name> and a password for <password>.
`Commands`	The word “command” means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example: To view the current login users, use the command: **`list users`**
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Document Notation

References to specific OfficeConnect Remote 840 Manager pages in this document will use a specific notation to describe the location of a page relative to the OfficeConnect Remote 840 Manager home page. The notation uses the' **>**' character to indicate that a sub-menu on a page must be accessed.

For example, to monitor the IP ARP Table you would (starting from the home page) access the **Monitor** menu. From the Monitor menu you would access the Networks sub-menu. From the Networks sub-menu you would access the IP sub-menu. Finally, from the IP sub-menu, you would access the ARP Table page. This is specified as **Monitor > Networks > IP > ARP Table**.

When accessing a page that requires data entry, press the **Help** icon displayed in the Main area to obtain information about the each data field on the page.

Safety Information

When using the unit, observe the following safety information:

- Retain this user guide for later use and pass it on to subsequent owners/managers of the unit.
- The power adapter supplied with the unit is fitted with a molded plug for connection to a standard electrical mains system supply socket. If this plug is not suitable for connection to your mains supply, contact your reseller for advice. Do not attempt to connect to the mains supply using an inappropriate mains adapter.
- Protect the unit from sudden, transient increases and decreases in electrical power by fitting an in-line surge suppressor or uninterruptible power supply.
- Products manufactured by 3Com are safe and without risk provided they are installed, used, and maintained in good working order and in accordance with their instructions and recommendations.
- Should any of the following conditions occur, isolate the electricity supply and refer to your 3Com reseller.
  - If the case or cover is not correctly fitted.
  - If the case is damaged.
  - If the unit begins to make an odd noise, smell or smoke.
  - If the unit shows signs of a distinct change in performance.
- Never install telephone wires during a thunder storm, or install telephone connection sockets in wet locations (unless the socket is specifically designed for wet locations).
- Do not touch uninstalled telephone wires or terminals unless the telephone line has been disconnected at the network interface. Always exercise caution when installing or modifying telephone lines.
- Do not use a telephone that is connected to the unit to report a gas leak in the vicinity of the leak.

- Do not use a telephone that is connected to the unit (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not spill food or liquids on the unit. If the unit gets wet, isolate the electrical supply and contact your 3Com reseller.
- Do not push any objects into the openings of the unit. Doing so can cause fire or electric shock by shorting out internal components.
- Ensure nothing rests on the unit's system cables and that the cables are not located where they can be stepped on and cause damage to the unit.
- Keep the unit away from radiators and heat sources. Allow 25mm (1 inch) around the unit or stack to provide adequate air circulation.
- Install the unit in a clean area that is free from dust or extreme temperatures.
- The unit has been designed to be a free standing unit. Do not place anything else on top of the unit's case.
- Allow a clearance gap of at least a 150 mm from the rear panel of the unit, to allow for cable access.
- This unit contains a lithium battery which is attached to a microchip on the printed circuit board. The defective battery must be disposed of safely in accordance with the manufacturers instructions.

  Cette unité contient une pile au lithium attachée à une puce sur la carte à circuit imprimé. Se débarrasser de la pile défectueuse en toute sécurité conformément aux instructions du fabricant.

Additional Safety Information

See the printed installation guide for additional important safety information.

Year 2000 Compliance

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 web page:

`http://www.3Com.com/products/yr2000.html`

1 OVERVIEW

Introduction

This chapter provides an overview of the OfficeConnect Remote 840. It contains the following sections:

- “What Is the OfficeConnect Remote 840?”
- “What is an SDSL Modem?”
- “What is ATM?”
- “What is Frame Relay?”
- “What is a BRouter?”
- “What is a Remote Site?”
- “What is RFC 1483”
- “What is RFC 1490?”
- “What is PPP?”
- “What is DHCP?”
- “What is DNS?”
- “What is Address Translation?”
- “What is DHCP Smart Mode?”
- “What Is Default Bridge Mode?”
- “Getting Started Quickly”
- “OfficeConnect Remote 840 Panel Features”
- “Configuration Overview”
- “How to Manage the OfficeConnect Remote 840”
- “Starting the OfficeConnect Remote 840 Manager”
- “Using the OfficeConnect Remote 840 Manager”
- “Online Help”

- "Where to Find More Configuration Information"

What Is the OfficeConnect Remote 840?

The OfficeConnect Remote 840 is a stand-alone BRouter with data interfaces to a Local Area Network (LAN) and a Wide Area Network (WAN). The Symmetric Digital Subscriber Line (SDSL) port composes the WAN interface, which can support Point-to-Point protocol (PPP), RFC 1483, or RFC 1490 connections. The LAN port is a twisted-pair Ethernet 10Base-T interface. Additionally, the OfficeConnect Remote 840 has a standard serial interface console port.

The OfficeConnect Remote 840 allows one or more networked workstations to connect to other computers on a remote LAN. Once connected, local users (a local branch office) can communicate with remote computers (the main office) as if they were connected locally (see the figure below). The OfficeConnect Remote 840 moves data back and forth quickly, and accesses any program or file you would ordinarily use on the network.

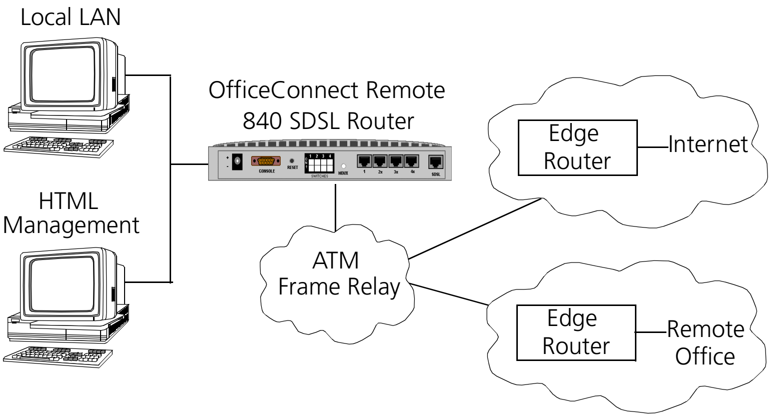


Figure 1–1 Connection to Remote Networks

The OfficeConnect Remote 840 can provide high-speed access to the Internet.

The OfficeConnect Remote 840 provides static and dynamic routing of the **Internet Protocol (IP)** and **Internetwork Packet Exchange (IPX)** protocols as well as bridging, with support for learning bridge and 802.1d spanning tree functionality to eliminate loops. Other important features include: Routing Information Protocol (RIP), Simple Network Management Protocol (SNMP), address translation, telnet, and packet filtering. The web browser-based OfficeConnect Remote 840 Manager and the IP Wizard provide a user-friendly configuration interface.

To simplify the installation process, the OfficeConnect Remote 840 can be initialized with pre-configured parameters using DIP switches located on the back of the unit. There are three operational modes: DHCP Smart Mode, Default Bridge Mode, and Unconfigured Mode.

What is an SDSL Modem?

An SDSL modem is a device that transmits and receives data through regular telephone lines at speeds that far exceed traditional analog modem technology.

It allows your workstation to connect to a remote site using a network protocol such as IP or IPX. The OfficeConnect Remote 840 contains one SDSL modem port which is the WAN interface.

What is ATM?

Asynchronous Transfer Mode (ATM) is a modern networking technology that provides support for a wide variety of services and applications. The OfficeConnect Remote 840 provides support for ATM over SDSL.

ATM is based on the transfer of fixed-length cells containing a header and an information field. The header is used to route the cells through the ATM network backbone.

ATM defines connections by two main parameters, which are explained later in this Guide:

- Virtual Path Identifier (VPI)
- Virtual Channel Identifier (VCI).

What is Frame Relay?

Frame Relay is a framed-based technology that runs over *HDLC* (High Level Data Link Control). Virtual Circuits are defined which connect the OfficeConnect Remote 840 to up to 16 remote sites within a Frame Relay Network. Each Virtual Circuit is identified by a *Data Link Connection Identifier* (DLCI), which is included in the frame header.

What is a BRouter?

A BRouter is an interface between two networks, functioning as a router and/or a bridge. A router finds the best route between networks and provides network management capabilities. The OfficeConnect Remote 840 is a protocol independent router that does not rely on the workstations on a LAN for routing information, such as the destination location and best route.

Routing vs. Bridging

Routers forward packets based on network-level addresses. Bridges forward packets based on hardware-level, or media access control (MAC) addresses. In other words, when a router receives a packet from one port, it looks at the destination network level address (for example, the IP address) to determine which port to forward the packet to. When a bridge receives a packet from one port, it looks at the destination MAC address to determine which port to forward the packet to.

In each case, the unit maintains either a forwarding table (bridges) or a routing table (routers) that contains information about which port to use to reach the destination address. These tables are for the most part maintained automatically by the unit so the administrator does not have to add or delete entries as the network topology changes.

An example illustrating the difference between bridges and routers would be the case where both a bridge and a router have tables with 256 entries. Because the bridge forwards based on MAC address, it can know about the location of 256 MAC addresses (physical machines such as workstations, servers, etc.). The router can know about the location of 256 networks, where each network can contain many physical machines.

Bridges make forwarding decisions based on destination addresses, while routers makes forwarding decisions based on networks to which destination addresses belong. Therefore, routers are more efficient and capable of handling more traffic.

The OfficeConnect Remote 840 provides a Bridge Firewall function which allows flexible configuration of simultaneous bridging and routing. For more information on the Bridge Firewall, see Appendix A, "Bridging and Routing".

MAC-Encapsulated Routing

MAC-Encapsulated Routing enables the OfficeConnect Remote 840 to function as a router but to work in a bridged environment. When enabled, the network level addresses are used for forwarding, but the

MAC layer addresses are pre-pended in the ethernet header over the Wide Area Connections. Address Resolution procedures (ARP), are used to dynamically learn the MAC address of the remote router.

What is a Remote Site?

The OfficeConnect Remote 840 can be configured to route IP or IPX, and/or bridge other protocols between workstations on the Local Area Network (LAN) and up to 16 remote locations over an ATM or Frame Relay Wide Area Network (WAN). This is illustrated in the diagram below, showing the local LAN simultaneously connected to a remote office and the Internet.

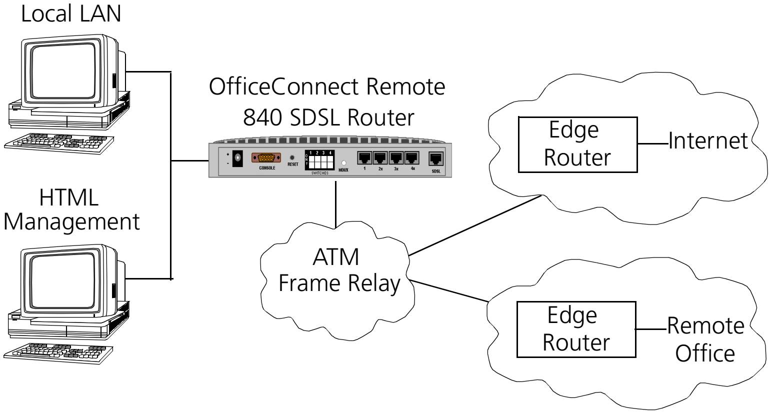


Figure 1–2 Connection to a Remote Internet Network

Data is transmitted to and from remote sites through ATM or Frame Relay. With ATM, each VC has a configured Quality of Service (QOS) and is identified by a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI). With Frame Relay, each Virtual Circuit is identified by a DLCI. Obtain these parameters from your Service Provider.

The data is framed in either PPP, RFC 1483 or RFC 1490 encapsulation, which also is specified by your Service Provider.

The IP, IPX, and bridge protocols transmit over the ATM VCs. When a remote site is configured to route IP, there will be a corresponding remote network IP subnet address and (optionally) a local WAN interface address within the same subnet. When the local side of the WAN interface has an assigned address, it is referred to as being "numbered." Otherwise, it is referred to as "unnumbered."

For a more in-depth description of "numbered" versus "unnumbered" interfaces, see Appendix B, "IP Addressing".

When PPP is used, both the local and remote WAN addresses can by dynamically learned. Otherwise, they must be specified. The diagram below shows a OfficeConnect Remote 840 with 3 VCs and the corresponding IP addresses.

When PPP is used, both the local and remote WAN addresses can by dynamically learned. Otherwise, they must be specified. The diagram below shows an OfficeConnect Remote 840 with 3 VCs and the corresponding IP addresses.

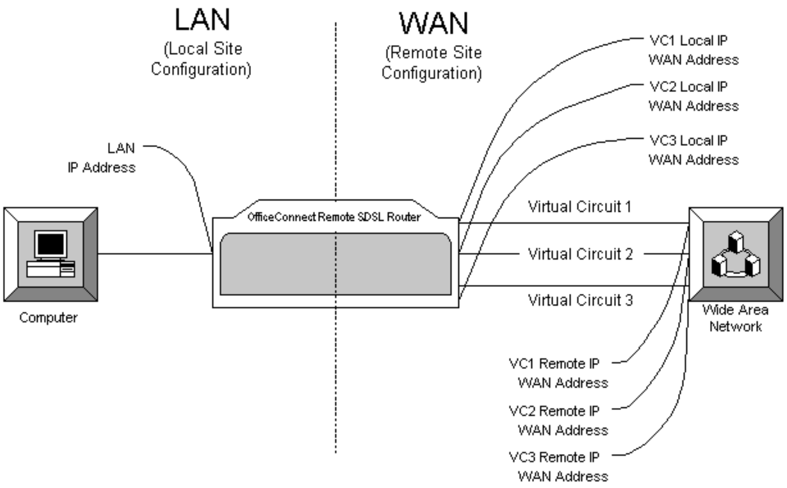


Figure 1–3 Connection with Three Virtual Circuits (VCs)

What is RFC 1483

RFC 1483 is a protocol standard that describes two encapsulations methods for carrying network interconnect (Bridging and Routing) traffic over ATM AAL5.

RFC 1483 is a single-link interface between two packet-switching devices, such as a bridge or router. An RFC 1483 link may be created between the OfficeConnect Remote 840 and a remote router after they establish a connection. RFC 1483 is a conduit for multiple protocols such as IP and IPX, which are encapsulated and passed across the communications datalink.

The OfficeConnect Remote 840 supports RFC 1483 and can establish a RFC 1483 connection to other devices supporting RFC 1483.

Benefits of Using RFC 1483

RFC 1483 offers interoperability of multi-vendor equipment and identification and aggregation of multiple protocol packets into one data stream.

What is RFC 1490?

It is a protocol standard that describes an encapsulation method for carrying network interconnect traffic over a Frame Relay backbone. It covers aspects of both Bridging and Routing.

The OfficeConnect Remote 840 supports RFC 1490 and can establish a RFC 1490 connection to other devices supporting RFC 1490.

What is PPP?

The Point-to-Point Protocol (PPP) is a WAN protocol. It is a single or multi-link interface between two packet switching devices, such as a bridge or router. A PPP link may be created between the OfficeConnect Remote 840 and a remote router after they connect. PPP is an efficient conduit for multiple protocols such as IP and IPX, which are encapsulated across the communications datalink.

PPP provides built-in negotiation for addresses and connection parameters, and it can route multiple protocols over a single link.

The OfficeConnect Remote 840 supports PPP and can establish a PPP connection to other devices supporting PPP.

Benefits of Using PPP

PPP offers interoperability of multi-vendor equipment, and support for dynamic configuration between the connecting devices.

What is DHCP?

Dynamic Host Configuration Protocol (DHCP) is designed to provide a centralized approach to configuring IP addresses and parameters.

When a workstation is configured for automatic assignment of IP addresses, it broadcasts a request on the LAN. The DHCP Server responds with an IP address for the workstation and the IP addresses of the default router and Domain Name Server.

The OfficeConnect Remote 840 can be configured to be a DHCP Server, with a pool of up to 40 IP addresses.

What is DNS?

A Domain Name Server (DNS) provides an IP address to a host computer for a given domain name. A DNS Proxy receives requests and attempts to find an entry in its local tables, and if one is not found, forwards the request to a remote DNS Server. The remote DNS Server can be learned dynamically through PPP or can be statically assigned.

The OfficeConnect Remote 840 can be configured as a DNS proxy. A static local host entry of **ocrdsl-3com.com** is configured for the OfficeConnect Remote 840 by default. Therefore, the OfficeConnect Remote 840 can be easily accessed with a web browser, by typing in **ocrdsl-3com.com** in the location or address field in the browser.

*In unconfigured mode, **ocrdsl-3com.com** is not configured by default. In this mode, you will have to configure a static host entry.*

What is Address Translation?

Address Translation allows private network addresses to be mapped into public addresses. The OfficeConnect Remote 840 provides two methods for mapping private, non-registered LAN IP addresses to the public Internet address(es) used for a wide-area connection. The two methods are:

- Network Address Translation (NAT). NAT simply substitutes public IP addresses for private IP addresses.
- Port Address Translation (PAT). PAT allows sessions from multiple private IP addresses to use a single public IP address.

NAT and PAT can be configured for each remote site.

What is DHCP Smart Mode?

To simplify the installation process, the OfficeConnect Remote 840 can be initialized with a set of pre-configured parameters. This operational mode is referred to as DHCP Smart Mode. In DHCP Smart Mode, the unit will automatically be assigned an IP address and will provide a pool of IP addresses to be assigned to each workstation attached to the LAN. When you choose this boot option, you will set up your workstation(s) for automatic IP address assignment.

What Is Default Bridge Mode?

The second operational mode is Default Bridge Mode. This mode preconfigures the unit to bridge all packets. The unit can be automatically set up so that you will not be required to fill out any forms, use Setup Wizard, or install any software from the CD unless you want to change the configuration.

What is Unconfigured Mode?

Unconfigured Mode allows you to set all configuration parameters yourself. You can configure it using Command Line Interface (CLI) (see the *OfficeConnect Remote 840 CLI User's Guide*), or the Web-based OfficeConnect Remote 840 Manager.

Getting Started Quickly

The features described above can be utilized to make configuring the OfficeConnect Remote 840 very easy.

- Use DHCP Smart Mode to preconfigure a LAN IP address, the DHCP pool of addresses, and the DNS information for the LAN workstations.
- Use Default Bridge Mode to have the unit automatically bridge all packets. No software installation is required.
- Use PPP to allow the OfficeConnect Remote 840 to automatically learn the WAN IP addresses and DNS information.
- Use PAT to allow the workstations on the LAN to share a single IP address when accessing the Internet or a remote office.

Use these features together and all you will need to do is enter authentication and ATM information for your remote site IP connection. Or:

- Use Default Bridge Mode to have the unit automatically bridge all packets. No software installation or configuration is required.

OfficeConnect Remote 840 Panel Features

All LED and status information can be found on the front panel of the unit, while the power jack and ports are located on the back of the unit.

Front Panel

Below is a representation of the front panel of your unit:

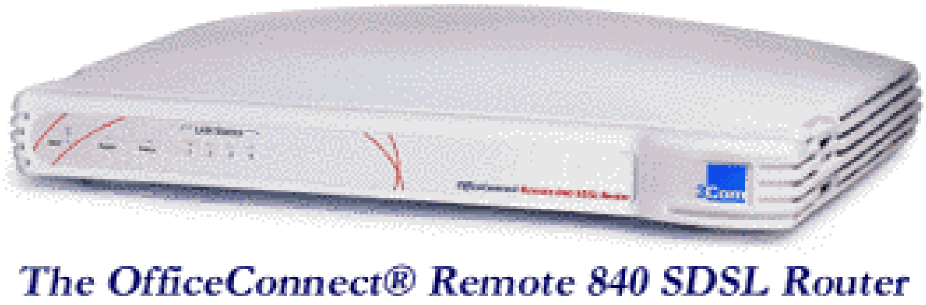


Figure 1–4 OfficeConnect Remote 840 Front Panel

Table 1–1 LED definitions

LED	Status	Meaning
Alert	FLASHING RED	When software is initializing
Power	STEADY GREEN	When power is applied to the unit
SDSL Link Status	OFF	No signal detected
	FLASHING ORANGE	The unit is attempting to acquire synchronization with the CO equipment.
	STEADY GREEN	Link is up.
	FLASHING GREEN	When data is being sent over the link.
LAN Status (4)	STEADY GREEN	When a client is connected to the corresponding port on the hub.

A table of LED operation is provided in **Chapter 3** of the *OfficeConnect Remote 840 SDSL Router Installation Guide* in the section **“Installing The OfficeConnect Remote 840.”**

Back Panel

Below is a representation of the back panel of your SDSL router:

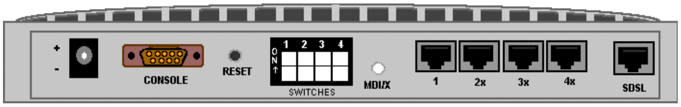


Figure 1–5 OfficeConnect Remote 840 Back Panel

- **Power Inlet** — The power port attaches to an external, 15-volt DC power supply included with the OfficeConnect Remote 840 package. The other end of the power supply cable connects to a standard electrical socket.
- **Console Port —** The DB-9 terminal port connects the OfficeConnect Remote 840 with your console. A straight-through serial cable is supplied to make the connection.
- **Reset Button** — To reset the OfficeConnect Remote 840 to factory defaults, press this button while rebooting (unplugging and replugging into an electrical outlet) the unit. You can reset the unit in Unconfigured Mode, DHCP Smart Mode, or Default Bridge Mode. (See the *Installation Guide* for more information on the different modes.)
- **MDI/X Switch** — Swaps the transmit (Tx) and receive (Rx) signal pairs on Ethernet port 1. When MDI/X is "out" (not depressed), Port 1 is pinned the same as the remaining 3 ports. In this mode, a PC's Ethernet port or the cascade port on another hub can be connected to any of the four ports on the unit. When MDI/X is pressed "in", then Port 1 on the unit becomes a cascade hub port, for connection to a non-cascade port on another hub. The MDI/X button must be "out" to use Port 1 for connection to a PC.
- **Ethernet (LAN) Ports (4)** — The shielded, 8-pin, RJ-45 Ethernet (10Base-T) ports connect the OfficeConnect Remote 840 with the LAN. A straight-through cable is supplied in the package to make this connection. Switches on the back of the unit provide crossover to allow a direct connection to a single workstation.
- **SDSL Modem Port** — The 4-pin, RJ-11 line port connects your OfficeConnect Remote 840 to the telephone company wall jack. An RJ-11 modem cable is provided.
- **DIP (Dual Inline Package) Switches (4) —** Switches 1 through 4 can be turned on and off in certain combinations for different

configurations. See the table below for information about which switches to set for which configurations.

Table 1–2 DIP Switch Modes

DIP Switch				
1	2	3	4	Mode
off	off	off	**on**	Default Bridge Mode, Frame Relay, DLCI = 528, data encapsulated over RFC 1483.
off	off	**on**	off	Default Bridge Mode, Frame Relay, DLCI = 16, data encapsulated over RFC 1490.
off	**on**	off	off	DHCP Smart Mode
on	off	off	**on**	Default Bridge Mode, ATM, One VC define as a bridge, VPI/VCI = 0/38
off	off	off	off	Unconfigured Mode
All other configurations: Unconfigured Mode				

- **DHCP Smart Mode** — (switch 2 on; all other switches off) This setting simplifies the configuration process by setting up the OfficeConnect Remote 840 as a DHCP and DNS server with a fixed IP address. For more information, see Chapter 2 of the *Installation Guide.*
- **Default Bridge Mode** — There are several different settings for Default Bridge Mode. The different settings control the WAN operational mode; ATM or Frame Relay, and the VPI/VCI or DLCI settings (see the table above). If you set the OfficeConnect Remote 840 to this mode and no configuration exists, the OfficeConnect Remote 840 will automatically set up a bridge network on the Ethernet and will create a VC profile that bridges using RFC 1483 or RFC 1490 encapsulation with various VPI/VCI or DLCI values (see the table above for details).

Configuration Overview

The OfficeConnect Remote 840 configuration is divided into three areas: Local Site (LAN), Remote Site (WAN), and Global configuration. The following shows the areas of configuration for each.

Local Site	**Remote Site**	**Global**
IP	Network Service	DHCP
IPX	ATM	DNS
Bridging	IP	Administrative
	IPX	
	Static WAN Routes	
	Bridging	

To successfully configure the OfficeConnect Remote 840 to route or bridge a network, you should perform the following steps.

General Configuration Steps

The following steps provide an outline to follow when configuring the OfficeConnect Remote 840 to route or bridge. For detailed instructions on first time installation and basic configuration, see the *OfficeConnect Remote 840 SDSL Router Install Guide.*

Perform the following steps to configure the OfficeConnect Remote 840 to route or bridge a network:

1. Complete the appropriate **Configuration Planning Form**. A form is provided in the box when you purchase your OfficeConnect Remote 840. Copies of the forms are provided in the *OfficeConnect Remote 840 SDSL Router Install Guide* for your convenience.
2. Install the OfficeConnect Remote 840 utilities from your OfficeConnect Remote 840 CD. If necessary, install a web browser on your workstation (Microsoft Internet Explorer 4 is included on the CD).
3. Connect to the OfficeConnect Remote 840 through either the web browser or the CLI.
4. Configure the OfficeConnect Remote 840.
   - Ethernet Interface Protocols
   - IP, IPX, Bridging
   - Remote Sites
   - Global Parameters
   - Run the configuration audit.
   - Save the configuration.

- Test the network accessibility.
- Ping a remote site
- Check the routing tables on configured protocols

How to Manage the OfficeConnect Remote 840

You can manage the OfficeConnect Remote 840 either through the Command Line Interface (CLI) or through a web browser. If you choose to manage the unit through CLI, see the *OfficeConnect Remote 840 SDSL Router CLI User's Guide*, included on the CD shipped with your unit.

If you choose to use a web browser, you will use the web browser-based OfficeConnect Remote 840 Manager. This user-friendly system is the preferred method of management. The OfficeConnect Remote 840 Manager uses the HTTP protocol via a web browser (such as Netscape Navigator or Microsoft Internet Explorer) to allow you to easily setup and manage the OfficeConnect Remote 840. In order for the OfficeConnect Remote 840 Manager to function correctly, you will need to use at least Netscape Navigator 4.0 or Internet Explorer 3.02. Internet Explorer 4 is provided on the OfficeConnect Remote 840 Installation CD.

You do not need to be connected to the Internet to use this method.

The main features of the OfficeConnect Remote 840 Manager are:

- Complete configuration control.
- Configuration Audit for detecting errors.
- Troubleshooting and monitoring capabilities.
- Capability to download software updates.

The OfficeConnect Remote 840 must have an IP address and an administrative login profile (username and password) in order to connect to it with a browser. The IP address and administrative login profile are automatically created when the unit is initially configured using the IP Wizard or in DHCP Smart Mode or Default Bridge Mode, or the IP address and administrative login profile can be created using the CLI.

See the *OfficeConnect Remote 840 SDSL Router Installation Guide* for information about assigning an IP address and creating an administrative login profile.

Starting the OfficeConnect Remote 840 Manager

To access the OfficeConnect Remote 840 Manager, either enter the unit's LAN IP address or DNS host name into the Location or Address field of your web browser. When entering the IP address or DNS host name you do not have to enter http:// (i.e., you can enter http://192.168.200.254 or simply 192.168.200.254).

If you initially configured your unit with DHCP Smart Mode, your unit will have an IP address of 192.168.200.254 and a DNS host name of ***ocrdsl-3com.com****.*

When prompted to login to the unit, enter the administrative login name and password. After successful authentication, you will access the OfficeConnect Remote 840 Manager "home page."

OfficeConnect Remote 840 Manager Menus

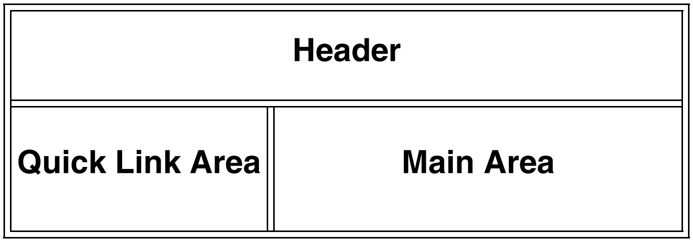
The OfficeConnect Remote 840 Manager is a hierarchical menu-based interface. The highest level page in the hierarchy is the OfficeConnect Remote 840 Manager home page. The home page displays a list of five menu choices:

- Setup Wizard
- Online Guide
- Tools
- Configuration
- Monitor

Each of the 5 main menus contain sub-menus with more choices.

Using the OfficeConnect Remote 840 Manager

All OfficeConnect Remote 840 Manager screens have three basic areas:



- **Header** — Shows the title of the current page being accessed.
- **Quick Link Area** — Indicates the position of the current page in the OfficeConnect Remote 840 Manager menu hierarchy and provides links which allow quick access to the home page and the five menu options. This allows you to quickly go from one menu area to another, such as from Configuration to Monitor.
- **Main Area** — Displays the current page containing configuration or status information.

To access a particular OfficeConnect Remote 840 Manager page follow the links through the menu hierarchy in the Main area. You can use the Quick Link area to quickly get back to the top of the menu hierarchy or to one of the five menu options selections.

You can configure your web browser's link display options to customize the colors of the Quick Links.

Document Notation

References to specific OfficeConnect Remote 840 Manager pages in this document will use a specific notation to describe the location of a page relative to the OfficeConnect Remote 840 Manager home page. The notation uses the ">" character to indicate that a sub-menu on a page must be accessed.

For example, to monitor the IP ARP Table you would (starting from the home page) access the **Monitor** menu. From the **Monitor** menu you would access the **Networks** sub-menu. From the **Networks** sub-menu you would access the **IP** sub-menu. Finally, from the **IP** sub-menu, you would access the **ARP Table** page. This is specified as **Monitor > Networks > IP > ARP Table**.

Online Help

The OfficeConnect Remote 840 Manager provides two methods of obtaining help.

- The *Online User's Guide*. This guide contains detailed information about configuring and using your OfficeConnect Remote 840. You can access the *Online User's Guide* from the OfficeConnect Remote 840 Manager home page.
- A detailed HTML help screen is available for each configuration page. There is a Help button at the bottom of each page requiring manual data entry or selection. The help text describes the valid values for each data entry field that may be entered on the current screen.

The Online User's Guide and HTML help screens are not part of the OfficeConnect Remote 840 operational software. They must be installed on each workstation where you will run your OfficeConnect Remote 840 Manager browser. That is, if you have two workstations from which you will run the OfficeConnect Remote 840 Manager, and if you want access to the Online Guide and screen HTML help screens, you must run the CD installation at both workstations.

Where to Find More Configuration Information

See the referenced chapters of this Guide to help you perform the following tasks:

- Administrative Tasks such as updating software or controlling login access — “System Administration”
- IP Routing Parameters — “Configuring IP Routing”
- IPX Routing Parameters — “Configuring IPX Routing”
- Bridging Parameters — “Configuring Bridging”
- How to Monitor the OfficeConnect Remote 840 SDSL Router — “Monitoring the OfficeConnect Remote 840”
- Configuring the OfficeConnect Remote 840 either for accessing the Internet or for Telecommuting / Remote Access – *OfficeConnect Remote 840 SDSL Router Install Guide*, **Chapter 3**.

2 SYSTEM ADMINISTRATION

Performing System Administration Tasks

This section describes the details for performing the following System Administration OfficeConnect Remote 840 Manager tasks:

- "Controlling Login and Telnet Access"
- "Modifying the Date and Time"
- "Restoring Factory Defaults"
- "Updating OfficeConnect Remote 840 Software"
- "Controlling SNMP Access"
- "Controlling TFTP Access"
- "Assigning SNMP Trap Managers"
- "Assigning Syslog Managers"

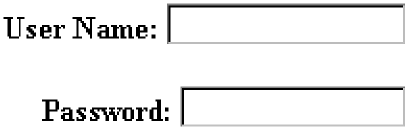
Controlling Login and Telnet Access

This allows you to set up management access security. The configured username and password combination allows web browser and Telnet access. Connecting to the OfficeConnect Remote 840 with a web browser allows you to configure and monitor your unit using the OfficeConnect Remote 840 Manager. Connecting using Telnet on a workstation allows you to remotely manage the unit using CLI.

A default user name of **root** and password **!root** are provided by DHCP Smart Mode and the IP Wizard during the initial installation. For secure access, you should add a private login name and password and delete the default name.

Adding a Login

1 From the home page, select **Configuration > Global > Administrator > Login**. Click **Add**. The following screen fields appear:



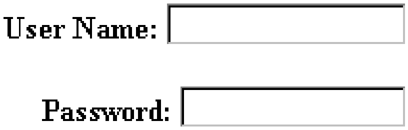
2 Enter the following fields:

- **User Name** — Enter the login or Telnet username in this field.
- **Password** — Enter the login or Telnet password in the field.

3 After the fields have been entered, click **Submit**. To clear the fields, click **Reset**.

Deleting a Login

1 From the home page, select **Configuration > Global > Administrator > Login**. Click **Add**. The following screen fields appear:



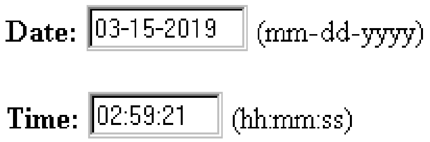
2 Select the login name to be deleted.

3 Click **Delete**.

Modifying the Date and Time

This allows you to modify the system date and time.

1 From the home page, select **Configuration > Global > Administrator > Date and Time**. The screen with the following fields appear:



Date: 03-15-2019 (mm-dd-yyyy)

Time: 02:59:21 (hh:mm:ss)

2 Enter the date and time information, utilizing the correct formats as shown next to the fields.

3 After the fields have been entered, click **Submit**. To clear the fields, click **Reset**.

Restoring Factory Defaults

Restoring the OfficeConnect Remote 840 to factory defaults causes all configuration information to be deleted and the unit to be rebooted.

To check the boot mode, go to the **Configuration > Global > Administrator > System** screen.

If you boot to the unconfigured state, you will need to run IP Wizard or use CLI to reassign an IP address to your OfficeConnect Remote 840. If you boot in DHCP Smart Mode, the IP address will be set to 192.168.200.254.

If you boot in Default Bridge Mode, you may not need an IP address assigned to the unit. However, if you do want one, you must use Command Line Interface. For detailed instructions on using CLI, please see the *OfficeConnect Remote 840 CLI User's Guide*, printable or viewable from the OCR840 CD.

You can set the switches before you restore the defaults to have the OfficeConnect Remote 840 boot in the mode you wish. See Table 1–2, **DIP Switch Modes** in Chapter 1 to select the mode you wish.

There are two ways to restore factory defaults:

- OfficeConnect Remote 840 Manager.

- Reset button on the back of the unit.

Using the OfficeConnect Remote 840 Manager to Restore Defaults

1. Select **Tools > Reboot**.
2. Select the **Delete all configuration and reboot device information** option.
3. Click **Submit**.
4. Wait one minute. Then, configure an IP address if DHCP Smart Mode is not in use.
5. Open up the web browser and start the OfficeConnect Remote 840 Manager by entering the new IP address in the browser location/address box.

Using the Reset Button

1. Turn the OfficeConnect Remote 840 off by unplugging the unit.
2. At this time, set the DIP switches to their appropriate settings (DHCP Smart Mode, Default Bridge Mode, or Unconfigured Mode). If you select Unconfigured Mode, you can set one of the other modes later using CLI or the OfficeConnect Remote 840 Manager.
3. While holding down the **Reset** button on the back panel, plug the unit back in. You should hold down the reset button for at least five seconds after plugging the unit back in. The unit takes about one minute to come up and the Alert LED will flash until bootup is finished.
4. If DHCP Smart Mode is not in use, configure an IP address after the unit comes up.
5. Open up the web browser and start the OfficeConnect Remote 840 Manager by entering the new IP address in the browser location/address box.

Updating OfficeConnect Remote 840 Software

See “Upgrading Operational Software for the OfficeConnect Remote 840” in Chapter 10 for information on updating the operational and system software.

Controlling SNMP Access

The **Simple Network Management Protocol (SNMP)** is used for managing routers and other network devices from a central station or stations. These stations, the SNMP Managers, query the managed units for configuration and monitoring information.

The OfficeConnect Remote 840 can be managed by SNMP Managers in read-only or read-write mode.

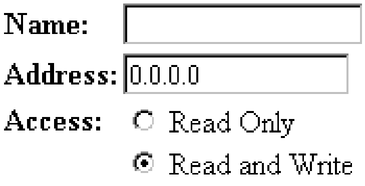
Using SNMP to manage the OfficeConnect Remote 840 is more complicated than the preferred method of management, the OfficeConnect Remote 840 Manager.

SNMP access is provided by an SNMP community name and access mode.

*To Download the Management Information Base (MIB) files, go to the website, **http://www.3com.com/support/ocr840/index.html,** and click the drop-down menu under **software/MIB downloads**.*

To set up an SNMP community on the OfficeConnect Remote 840, follow these instructions:

1 From the home page, select **Configuration > Global > Administrator > SNMP**. Click **Add** and the following screen fields appear:



Name:

Address: 0.0.0.0

Access: ○ Read Only ● Read and Write

2 Enter the following fields:

- **Name** — Enter the community name to be used as the access name.
- **Address** — Enter the address of the SNMP server (e.g., 192.168.200.52).

Specifying 0.0.0.0 allows any SNMP server access if they supply the correct name.

- **Access** — Check the box for **Read Only** or **Read & Write**. Read Only allows only the user to view the screens.

3 After the fields have been entered, click **Submit**. To clear the fields, click **Reset**.

4 Repeat steps 1-3 for each management station which is a part of this community.

Be careful to have the Access box checked the same for each new member of the community.

The entire community will be given the access rights of the last member.

5 To alter previously set Access Rights, follow step 1 and select the community from the community list and click **Modify**.

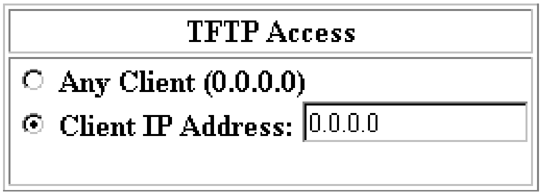
6 To delete a management station from a community, go to the home page and, select **Configuration > Global > Administrator > SNMP**. Select the community and management station from the lists and click **Delete**.

Controlling TFTP Access

The **Trivial File Transfer Protocol (TFTP)** provides a simple way to transfer files from one machine to another. The OfficeConnect Remote 840 has a TFTP server that allows you to copy files to or from the unit. All you have to do is set up TFTP access on the OfficeConnect Remote 840 and run a TFTP client program on a workstation. TFTP transfers files over either the LAN or WAN interfaces.

To configure the OfficeConnect Remote 840 to provide TFTP access, follow the instructions below:

1 From the home page, select **Configuration > Global > Administrator > TFTP**. Click **Add** and the following fields appear:



TFTP Access

○ Any Client (0.0.0.0)

● Client IP Address: 0.0.0.0

2 Enter the address of the client workstation or select **Any Client** for unrestricted client access.

3 After the fields have been entered, click **Submit**. To clear the fields, click **Reset**.

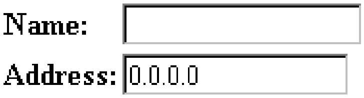
Assigning SNMP Trap Managers

An **SNMP trap** is an event that causes the OfficeConnect Remote 840 to send an unsolicited message to a SNMP manager.

These events are generally critical events that indicate an operational problem. (Critical events can also be viewed on the OfficeConnect Remote 840 Manager's **Monitor > Events > Critical Event Log** screen.)

To configure the OfficeConnect Remote 840 to send traps, follow these instructions:

1 From the home page, select **Configuration > Global > Administrator > TRAP**. Click **Add** and the following screen fields appear:



Name:

Address: 0.0.0.0

2 Enter the following fields:

- **Name** — Enter the name of the SNMP Trap Manager.
- **Address** — Enter the address of the SNMP Trap Manager (e.g., 192.168.200.50).

Specifying 0.0.0.0 causes SNMP Traps to be broadcast.

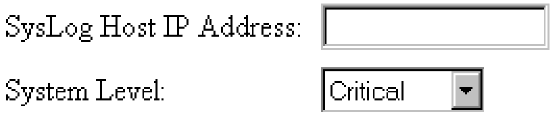
3 After the fields have been entered, click **Submit**. To clear the fields, click **Reset**.

To alter previously set fields, follow step 1 and select an SNMP Trap Manager, then click **Modify**. To delete a server from your configuration, select an SNMP Trap Manager from the TRAP screen and click **Delete**.

Assigning Syslog Managers

A **Syslog manager** is a workstation that accepts and saves informational messages from a network device. The OfficeConnect Remote 840 Manager can be configured to send log messages to a syslog manager as follows:

1 From the home page, select **Configuration > Global > Administrator > Syslog**. Click **Add** and the following screen fields appear:



SysLog Host IP Address:

System Level: Critical

2 Enter the following fields:

- **Syslog Host IP Address —** Enter the address of the Syslog host.
- **System Level** — Select one of the following levels: Critical, Unusual, Common, Verbose, and Debug.

3 After you enter the fields, click **Submit**. To clear the fields, click **Reset**.

3 REMOTE SITE MANAGEMENT

Introduction

This chapter provides an overview on managing remote site profiles using the web browser based OfficeConnect Remote 840 Manager. If you need information on setting up or initially configuring the unit, see the OfficeConnect Remote 840 SDSL Router Installation Guide. This section is divided into the following parts:

- "Remote Site Overview"
- "Managing a Remote Site Profile"
- "Configuring Network Service Information (PPP / RFC 1483 / RFC 1490)"
- "Configuring ATM Information"
- "Configuring Protocol Parameters"
- "Monitoring Remote Site Connections"

Remote Site Overview

To set up connections over the WAN, a remote site profile must be created and edited for each remote location you want to connect to. With this profile, you specify ATM virtual circuit or Frame Relay DLCI information, protocols, and addresses that determine the method of connection and communication to the remote site.

You first need to add a remote site profile, and then you modify the profile to include WAN connection and network information.

The following list summarizes the necessary information.

- **WAN** — Network Service (PPP / RFC 1483/RFC 1490) information, and ATM Virtual Channel (VC) or Frame Relay (DLCI) information
- **IP** — IP addresses, address translation tables, static routes, and RIP usage.

- **IPX** — IPX network address information, static routes and services, and RIP usage.
- **Bridging** — Bridging (enable / disable) to the remote site.

If you need to connect to multiple remote sites such as the Internet and a remote office, you should set up a remote site profile for each location.

Managing a Remote Site Profile

Once created, remote site profiles can be *enabled* or *disabled*. When a profile is enabled, the OfficeConnect Remote 840 reads the connection parameters for the remote site from the profile and continuously attempts to establish a connection to the remote site.

When a profile is disabled, the connection will be terminated and no other data will be directed to the remote site.

Configuration changes to a remote site profile do not take effect until the next time the profile is enabled. The OfficeConnect Remote 840 Manager automatically disables and re-enables the remote site profile when the **Modify** button is pressed on the Remote Site menu page.

To disable or enable a profile manually, clear or check the **Enable Remote Site** checkbox as appropriate.

*Once you start modifying a Remote Site, you must click **Modify** before you exit the Remote Site screens, or else the data you entered will be lost. Also, remember to save your configuration before rebooting your OfficeConnect Remote 840 so that your changes will be written to permanent FLASH memory.*

Adding a Remote Site Profile

1. From the OfficeConnect Remote 840 Manager home page, select **Configuration > Remote Sites (WAN)**. Then click the **Add** button to bring up the **Remote Site General Add** screen.
2. Enter the **Remote Site Name**. Enter a name to use to identify the remote site profile. (Ex: ISP or CorpOffice)
3. Ensure that the **Enable Remote Site** box is checked if you want to the connection to come up as soon as you finish the configuration.

4 Click **Add**. Then click **Save Configuration** on the sidebar to permanently save the changes.

The Network Service (PPP and RFC 1483/ RFC 1490), ATM, and network protocol (Bridging, IP, and IPX) information has not been configured yet. To make a connection with the remote site you must configure the Network Service, ATM, and at least one network protocol. (See "Configuring Network Service Information (PPP / RFC 1483 / RFC 1490)", "Configuring ATM Information", and "Configuring Protocol Parameters" for details.)

Modifying a Remote Site Profile

1 From the OfficeConnect Remote 840 home page, select **Configuration > Remote Site (WAN)**.

2 Select the name of a remote site profile and click **Modify**. This brings up the **Remote Site General Modify** screen.

3 Change configuration parameters as needed and use the **Next** button to continue to the **ATM**, **IP**, **IP Advanced**, and **IPX** configuration screens.

For quick help on specific parameters, click the **Help** button located at the bottom of each screen.

For more detailed help, go to the appropriate place in this guide (see "Configuring ATM Information" and Configuring Other WAN Parameters).

- Click **Modify** on any screen to set all the Remote Site parameters.
- Click **Save Configuration** on the sidebar to permanently save the changes.

Deleting a Remote Site Profile

1 From the OfficeConnect Remote 840 home page, select **Configuration > Remote Site (WAN)**.

2 Select the name of a remote site profile and click **Delete**. This brings up the **Remote Site General Delete** screen.

3 To delete the profile, click **Delete**. To return to the remote site profile selection list, click **Prev**.

Configuring Network Service Information (PPP / RFC 1483 / RFC 1490)

A Network Service defines the data encapsulation and protocol characteristics for the connection between two packet switching devices.

The OfficeConnect Remote 840 supports **PPP, RFC 1483** and **RFC 1490** Network Services. The OfficeConnect Remote 840 and the remote site must both use the same Network Service in order for a connection to be established.

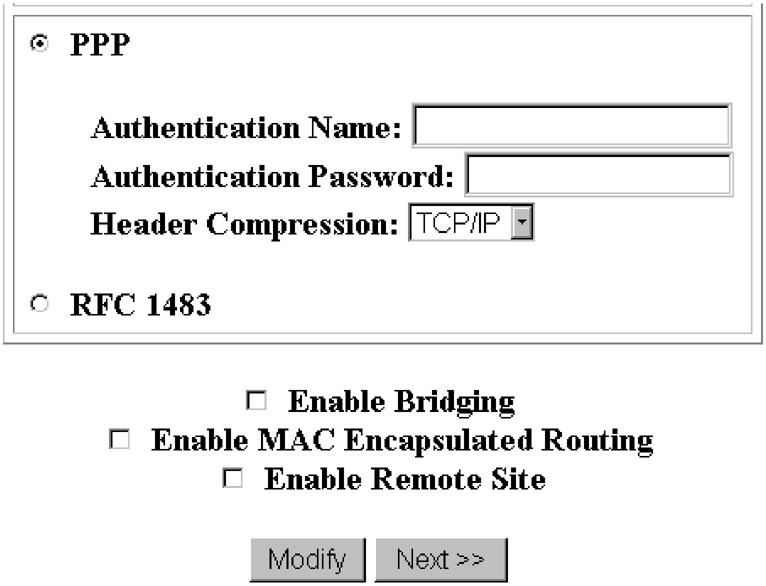
For PPP, the authentication name and password must be provided to allow the connection to be established. The OfficeConnect Remote 840 supports both PAP and CHAP authentication.

The Network Service parameters can be configured on the **Remote Sites General** screen.

1 Access this screen by going to the OfficeConnect Remote 840 home page. Select **Configuration > Remote Sites (WAN)**, select a defined remote site and click **Modify**.

2 This will access the **Remote Sites General Modify Screen**.

3 If your unit is using ATM, the **Remote Sites General Modify Screen** will contain the following fields:



● PPP

Authentication Name:

Authentication Password:

Header Compression: TCP/IP

○ RFC 1483

□ Enable Bridging

□ Enable MAC Encapsulated Routing

□ Enable Remote Site

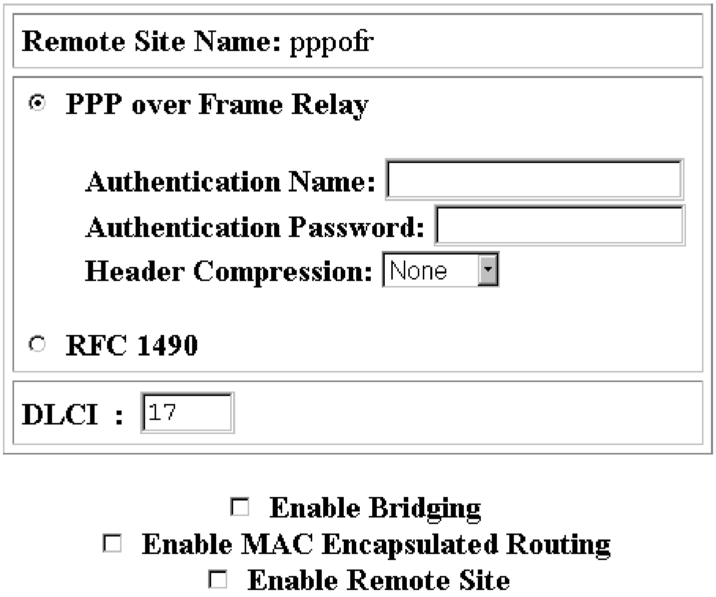
4 Select the network service to be either RFC 1483, or PPP.

If PPP, enter the Authentication Name and Authentication Password provided to you. You can change the header compression from the default of none to TCP/IP if you wish.

5 Click **Next** to proceed to the ATM Configuration screen.

Frame Relay

1 If your unit is using Frame Relay, the **Remote Sites General Modify** screen will contain the following fields:



Remote Site Name: pppofr

● **PPP over Frame Relay**

Authentication Name:

Authentication Password:

Header Compression: None

○ **RFC 1490**

DLCI : 17

□ **Enable Bridging**

□ **Enable MAC Encapsulated Routing**

□ **Enable Remote Site**

2 Enter a name to identify the remote site.

3 Select **Network Service** to either **PPP over Frame Relay** or **RFC 1490**.

If you select PPP over Frame Relay, enter the Authentication Name and Authentication Password provided to you. You can change the header compression from the default of None to TCP/IP if you wish.

4 Enter the **DLCI**.

5 Check the **Enable Bridging** and **Enable MAC Encapsulated Routing** boxes according to your service provider’s directions.

6 Check the **Enable Remote Site** box.

Configuring ATM Information

The ATM parameters are supplied by your service provider. These parameters consist of:

- ATM VC information
- ATM Category of Service parameters

ATM allows for permanent connections (PVCs) and switched connections (SVCs). For a PVC, the required VC information parameters consist of the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI).

The VPI / VCI uniquely specify the path to the remote site and are placed in the ATM cell header that is used to route each cell to the remote site.

Two remote site profiles with the same VPI and VCI cannot be active simultaneously. You may encounter this situation if you want to log in to the same remote site with different PPP authentication parameters. You should disable all profiles using the same VPI / VCI and then enable the one that should be active.

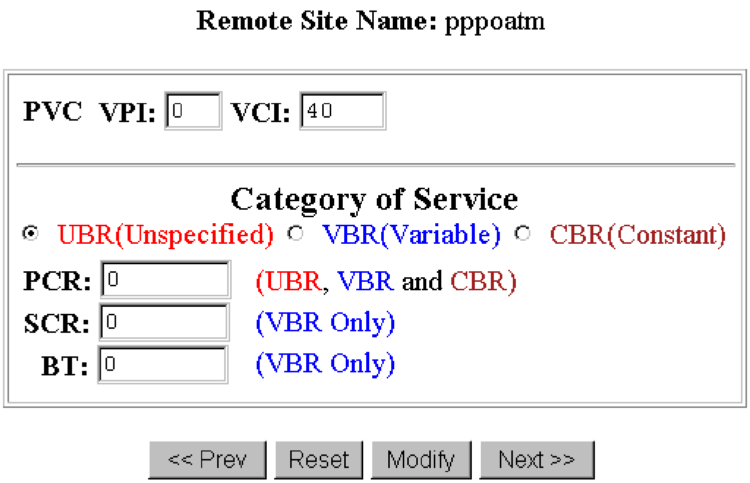
For SVCs, there is not a fixed VPI / VCI. Instead, a destination address is used to set up a path through the ATM backbone network when the connection is to be established. Currently, the SVC capability is disabled in the OfficeConnect Remote 840.

ATM Category of Service parameters specify characteristics (also referred to as traffic shaping) of data transmitted from the OfficeConnect Remote 840 to the remote site. They have no effect on data transmitted from the remote site to the OfficeConnect Remote 840.

ATM Modify Screen

Go to **Configuration > Remote Sites (WAN)**. Select a site from the list and click **Modify**.

Click **Next** to proceed to the **ATM Modify** screen. The screen contains the following fields:



Remote Site Name: pppoatm

PVC VPI: 0 **VCI:** 40

Category of Service

● UBR(Unspecified) ○ VBR(Variable) ○ CBR(Constant)

PCR: 0 (UBR, VBR and CBR)

SCR: 0 (VBR Only)

BT: 0 (VBR Only)

- If PVC is selected, enter the VPI and VCI.
  - **VPI —** The Virtual Path Identifier (VPI) is part of the cell header for the cells that are transferred over this connection.
  - **VCI** — The Virtual Channel Identifier (VCI) is part of the cell header for the cells that are transferred over this connection. If you are configuring multiple VCs, enter the number of the respective VC in this field.
- If necessary, enter any Category of Service parameters that have been provided to you.
  - **UBR** — Unspecified Bit Rate; no limit has been specified for the rate for information flow.
  - **VBR** — Variable Bit Rate; a certain rate has been specified for the flow of information.
  - **CBR** — Constant Bit Rate; a constant rate has been specified for the flow of information.
- Enter the cell rate transmission parameters, if applicable.
  - **PCR** — The Peak Cell Rate is the maximum amount of cells per second transmitted over this connection. This is determined by the minimum intercell spacing in seconds, which is the time interval from the first bit of one cell to the first bit of the next cell.
  - **SCR** — The Sustainable Cell Rate, in cells/second. This is the rate at which cells are transmitted over this connection. This is the

maximum average rate or cells that are sent in bursts at a peak rate.

- **BT** — The Burst Tolerance (also referred to as Maximum Burst Size), in cells/second. This is the maximum number of cells that can be sent at the peak rate.

If no traffic shaping parameters have been provided you should choose the default parameter of UBR with a PCR value of 0. The OfficeConnect Remote 840 will attempt to use all of the upstream bandwidth when transmitting data to the remote site.

Configuring Protocol Parameters

There are more WAN connection parameters that can be configured, such as IP routing, IPX routing, Bridging, and Address Translation. Instructions for configuring these parameters are located in:

- "Configuring IP Routing"
- "Configuring IPX Routing"
- "Configuring Bridging"
- "Network Address Translation Using the OfficeConnect Remote 840"

Monitoring Remote Site Connections

- To determine which remote sites have been configured and to see a summary of the remote site WAN parameters, access the **Monitor > Remote Sites > Remote Site Status** screen.
- To monitor packet counters for a specific remote site, access the **Monitor > Remote Sites > Remote Site Counters** screen. (Remote Site Counters are only applicable for active connections.)
- To determine whether a remote site connection has been established or to determine why a connection is not working properly, check the connection event log. This log is accessed at **Monitor > Events > Connection Event Log**.
- To monitor throughput for all active remote sites, access the **Monitor > ATM Throughput** screen.

For more information on these and other monitoring capabilities, see Chapter 11, "Monitoring the OfficeConnect Remote 840".

4 CONFIGURING IP ROUTING

Introduction

This chapter contains information on configuring routing for IP protocol using the OfficeConnect Remote 840. It is divided into the following sections:

- "Overview"
- "Enabling IP Routing"
- "Configuring IP for the LAN"
- "Configuring IP RIP on the LAN"
- "Configuring IP for the Remote Site Connection"
- "Configuring IP RIP on a Remote Site"
- "Configuring IP Static and Framed Routes"
- "Using IP Address Validation"
- "Monitoring"
- "IP Testing (PING)"

Overview

The OfficeConnect Remote 840 can be configured as a router to forward packets between the local LAN interface and one or more Remote Sites.

The router maintains a forwarding table. This table specifies which interface to route an IP packet based on the destination IP address. Entries in the forwarding table are either static or dynamic. Static entries are based on the LAN's and Remote Site's subnet addresses and user configured static routes. Dynamic entries are added when Routing Information Protocol (RIP) is enabled and routes are learned from neighboring routers.

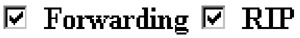
The OfficeConnect Remote 840 does not support OSPF (Open Shortest Path First) protocol.

To configure IP routing, IP must be defined on both the LAN interface and one or more remote sites. On the LAN, an IP network must exist and it must have a specified IP address and subnet mask. On the remote sites, IP routing needs to be enabled, and the remote router address, a remote subnet mask and local WAN interface address need to be configured. The remote site address configuration can be learned dynamically when the remote site connection is established if the network service is PPP, otherwise it has to be specified.

Enabling IP Routing

When the OfficeConnect Remote 840 is to be used for IP Routing, forwarding must be enabled in the global IP setting.

Access the IP Screen through **Configuration > Global > IP > IP Settings**. This screen contains the following fields:



☑ Forwarding ☑ RIP

Check the Forwarding box to enable the routing of IP packets.

In addition to Forwarding, the RIP check box is used to enable or disable RIP for all Remote Sites and the local LAN. If RIP is globally disabled, it is disabled for the local LAN and Remote Sites on the OfficeConnect Remote 840. If RIP is globally enabled, it can be enabled or disabled on the local LAN and for each Remote Site.

Configuring IP for the LAN

To configure IP over the LAN, assign an IP network to the LAN port by providing a name and a network address. After adding a network, you can modify advanced parameters.

If you ran the IP Wizard or booted the unit in DHCP Smart Mode, an IP network has already been added over the LAN port. Its name is IP and its address is either entered from the IP Wizard or it is **192.168.200.254**. You can view or modify configuration parameters for this network (e.g., Enable RIP).

If you use this IP address for accessing the OfficeConnect Remote 840 Manager, be careful not to delete the network.

For routing to take place across the OfficeConnect Remote 840, you also have to set up a corresponding network over the WAN port (see "Configuring IP for the Remote Site Connection").

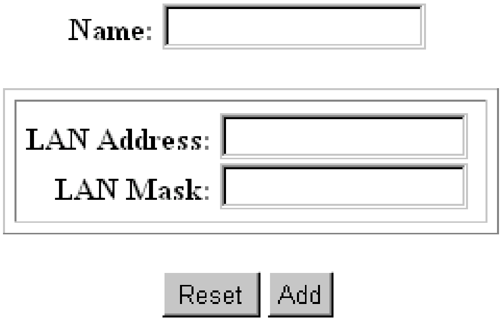
Use the **Configuration > Local Site (LAN) > IP screen** to define or modify all IP networks over the LAN. Note that all IP networks defined over the LAN only support Ethernet II framing.

Adding a Local IP Network

You may add multiple IP networks over the Ethernet interface by following these steps:

Select **Configuration > Local Site (LAN) > IP**.

Click **Add**. This brings up a screen containing the following fields:



Enter the following information:

- **Name** — The name is limited to 32 characters. If you use any blank spaces, surround the whole phrase with double quotes (e.g., "test site x").
- **LAN Address** — Enter the address of the IP network in this format: ddd.ddd.ddd.ddd where ddd is a value between 1--255.
- **LAN Mask** — Enter the mask of the IP network in this format: ddd.ddd.ddd.ddd where ddd is a value between 0--255.

By default, RIP is not enabled for this new IP network. If you wish to enable RIP, proceed to the Modify portion of the following section.

Click **Add** when you have entered these fields. This returns to the IP menu screen.

Resetting Parameters

If you need to return to the original parameters for this screen, click **Reset** before you click **Add**.

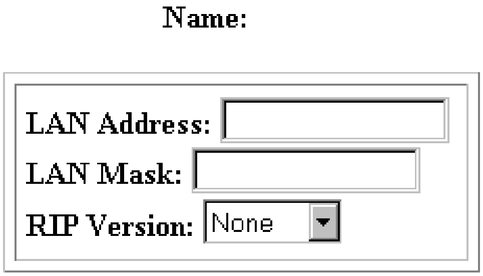
Modifying or Deleting an IP Network

To modify information pertaining to an existing IP network, or to delete that information from your configuration, follow these steps:

1 Proceed to the IP screen, following steps from the previous section.

2 Select an IP network you wish to modify or delete.

3 Click **Modify/Delete**.This brings up the **IP Modify/Delete** screen containing the following fields:



Name:

LAN Address:

LAN Mask:

RIP Version: None

4 Modify or delete the information about the selected IP network by altering the fields and clicking the **Modify/Delete** button.

*If you **alter** the address that your browser is using, the connection will be lost. To reconnect, enter the new IP address in your browser's address/location field. If you **delete** the address, you will also lose the connection. You will not be able to reconnect until a new address is assigned using either the IP Wizard, CLI, or by rebooting in DHCP Smart Mode.*

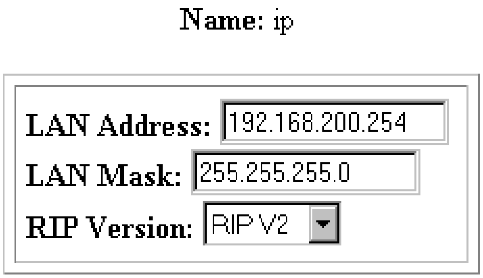
5 If you need to return to the original parameters for this screen, click **Reset** before you click **Modify**.

Configuring IP RIP on the LAN

RIP is utilized as a means of communicating routing information between routers. This is done to keep the routers updated on information.

Local Site (LAN) RIP

The RIP options for the LAN can be accessed through **Configuration > Local Site > IP**. Select a defined local site connection from the list and click **Modify/Delete**, which accesses the **IP Modify/Delete** screen, containing the following fields:



Name: ip

LAN Address: 192.168.200.254

LAN Mask: 255.255.255.0

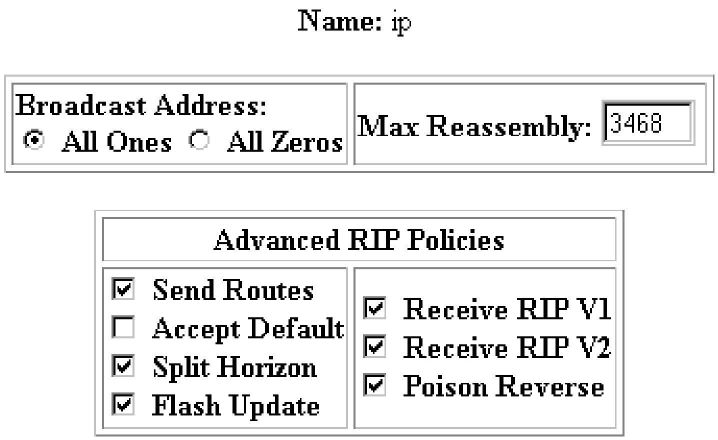
RIP Version: RIP V2

You can then select the RIP version to be either None, RIPV1, or RIPV2. You can also modify the Advanced RIP parameters. You should not need to change any of these parameters from the defaults, but you can if necessary.

Advanced RIP Modification Options

Select a local site connection from the list on the main IP screen, and click **Advanced.**

This brings up a screen containing the following fields:



Name: ip

Broadcast Address: ● **All Ones** ○ **All Zeros**

Max Reassembly: 3468

Advanced RIP Policies

☑ **Send Routes**
□ **Accept Default**
☑ **Split Horizon**
☑ **Flash Update**

☑ **Receive RIP V1**
☑ **Receive RIP V2**
☑ **Poison Reverse**

1. You may enter the following fields:
   - Broadcast Address - Check one of two options: All Ones or All Zeroes.
   - Max Reassembly - Enter the maximum value that your network cannot exceed for this function.
2. Under the following two categories, you may customize your RIP:
   - Advanced RIP Policies - You may enable these options as necessary. They control what is sent out or received concerning RIP.
3. Click **Submit** when the fields have been entered to save your customizations.

Resetting Parameters

*If you need to return to the original parameters for this screen, click **Reset** before you click **Add**.*

Configuring IP for the Remote Site Connection

To set up connections over the WAN, a remote site profile must be created and edited for each remote location you want to connect to. With this profile, you specify ATM virtual circuit information, protocols, and addresses that determine the method of connection and communication to that remote site.

You first need to add a remote site profile, then modify the profile to include WAN connection and network information. The following list summarizes the necessary information:

- **Frame Relay/ATM WAN** — Network Service (PPP/RFC 1483/ RFC 1490) information, ATM VC information
- **IP** — IP addresses, address translation tables, static routes, RIP usage
- **IPX** — IPX network address information, static routes and services, RIP usage
- **Bridging** — Enable or disable bridging to the remote site

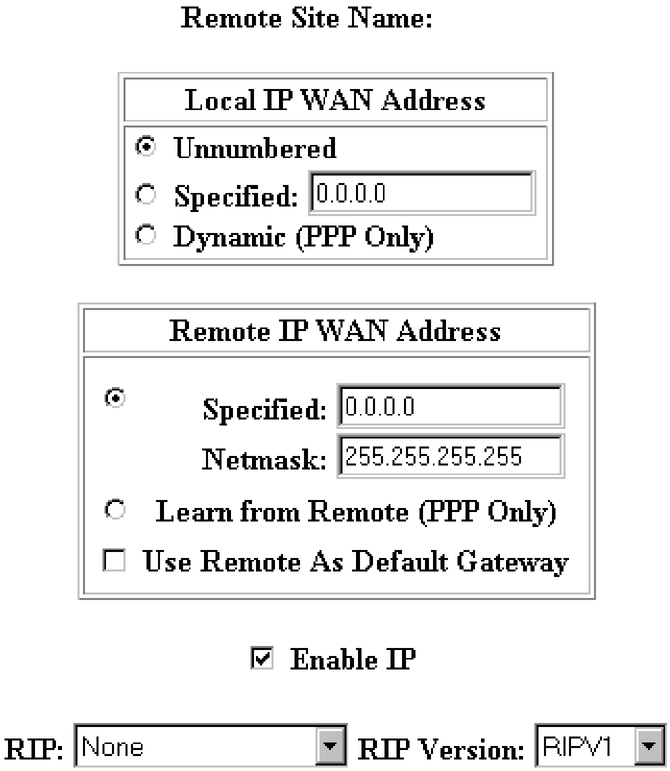
If you need to connect to multiple remote sites (i.e., the Internet and a remote office) you should set up a remote site profile for each location.

Configuring IP Parameters for the Remote Site

The following steps illustrate how you configure the IP parameters of the remote site profile.

These instructions assume you have already added a remote site profile. If you need to add a remote site profile, select **Add** instead of **Modify** in step 1.

1. Access this screen by going to the OfficeConnect Remote 840 home page. Select **Configuration > Remote Sites (WAN)**, and click **Modify**. This will access the **Remote Sites General** screen.
2. Continue clicking **Next** to advance through the **ATM Modify** screen to the **IP Modify** screen.



Remote Site Name:

Local IP WAN Address

● Unnumbered

○ Specified: 0.0.0.0

○ Dynamic (PPP Only)

Remote IP WAN Address

● Specified: 0.0.0.0

Netmask: 255.255.255.255

○ Learn from Remote (PPP Only)

□ Use Remote As Default Gateway

☑ Enable IP

RIP: None RIP Version: RIPV1

Configure the Remote Site IP Network Information

The following steps illustrate how you configure the remote site IP network information.

1 Complete the following entries:

Local WAN IP Address:

- If you were provided a single IP address, select **Specified** and enter that address.
- If you are using PPP to dynamically assign an address, select **Dynamic**, and the remote site on the WAN will assign a local WAN IP address to the WAN port of your OfficeConnect Remote 840.
- Otherwise, select **Unnumbered**, and there will be no IP address assigned to the local WAN interface for this VC.

Remote WAN IP Address:

- If you were provided a remote IP address and netmask, select **Specified** and type in that address and netmask.
- If the OfficeConnect Remote 840 is learning the remote IP address from the remote site (PPP only), select **Learn from Remote**.

2 In order to have the remote site you are configuring as the default gateway, check the **Use Remote as Default Gateway** checkbox.

3 If you are routing IP traffic to multiple remote sites, select one to be your default gateway. Then check this box only in the profile for that remote site.

4 Select from the pull-down menu to have the RIP set to Broadcast, Listen, or Broadcast & Listen, and if one of these is chosen, set the RIP option to RIPV1 or RIPV2.

If you are using address translation (PAT / NAT), you must set routing to either ***Listen*** *or* ***None****. This is because you have set up a private network and therefore do not want to be broadcasting information to other routers.*

5 Ensure that Enable IP is checked (enabled) and click **Modify**.

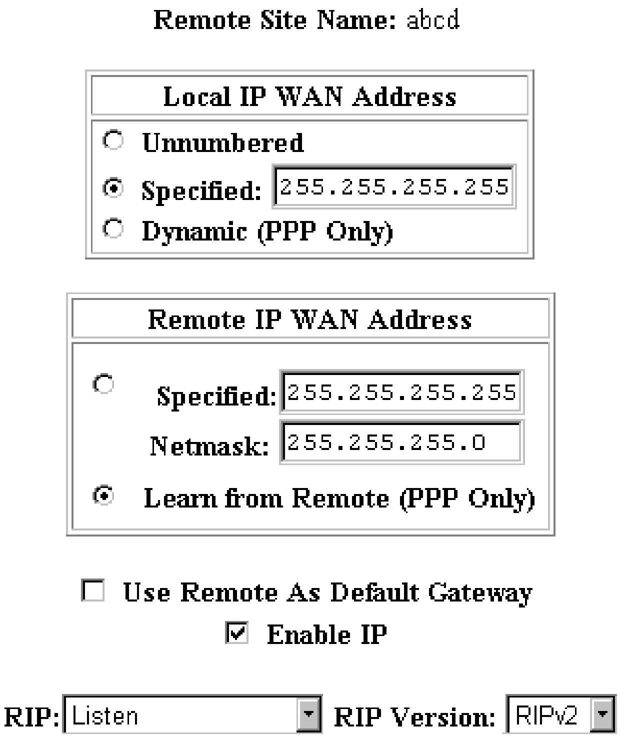
You are now done configuring the basic IP information for the Remote Site Connection.

Further Remote Site IP Configuration information is available in the following sections:

- Address Translation information is available in "Network Address Translation Using the OfficeConnect Remote 840".
- Address Validation Information is available under "Using IP Address Validation".

Configuring IP RIP on a Remote Site

Access the RIP options for the WAN through **Configuration > Remote Sites > IP**.



Remote Site Name: abcd

Local IP WAN Address

○ Unnumbered

● Specified: 255.255.255.255

○ Dynamic (PPP Only)

Remote IP WAN Address

○ Specified: 255.255.255.255

Netmask: 255.255.255.0

● Learn from Remote (PPP Only)

□ Use Remote As Default Gateway

☑ Enable IP

RIP: Listen RIP Version: RIPv2

1 Select a defined remote site connection from the list and click **Modify**. Keep clicking **Next** until you advance to the **IP Modify** screen.

2 You can select the RIP version to be either **Broadcast**, **Broadcast & Listen**, **Listen** or **None**. Broadcast refers to when routing information packets are sent out to the network, and Listen refers to the OfficeConnect Remote 840 receiving routing information packets from remote sources.

*If you are using address translation (PAT/NAT), you must set routing to either **Listen** or **None**. This is because you have set up a private network and therefore do not want to be broadcasting information to other routers.*

3 You can then choose between RIPV1 (version 1) or RIPV2 (version 2) for your routing information protocol.

Configuring IP Static and Framed Routes

A Static route is a configured route that will remain in the routing table until deleted. Static routes differ from Dynamic routes in that Dynamic routes are learned real-time via RIP.

A Framed route is much like a static route in that you manually configure the route. The difference is that a static route is defined for the LAN while a framed route is associated with a remote site. Also, while a static route is active when the LAN is connected, a framed route is active only when the connection to the associated remote site is active.

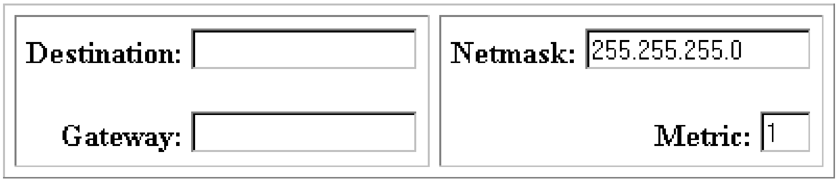
Only use static and framed routes for networks not learned using RIP.

Adding a Static IP Route to the LAN

To add, modify, or delete an IP Static route to the LAN, follow these steps:

1 Select **Configuration > Global > IP > Static Routes**.

2 Click the **Add** button. This accesses a screen containing the following fields:



Destination:

Gateway:

Netmask: 255.255.255.0

Metric: 1

3 Define the Route by entering the following fields: **Destination** (network), **Gateway** (IP address), **Netmask**, and **Metric**. Click **Submit**. To clear the fields, click Reset.

4 To delete a route from your configuration, select the route and click **Delete**.

Adding a Framed IP Route to a Remote Site

To add, modify, or delete a Framed Route to a Remote Site, follow these steps:

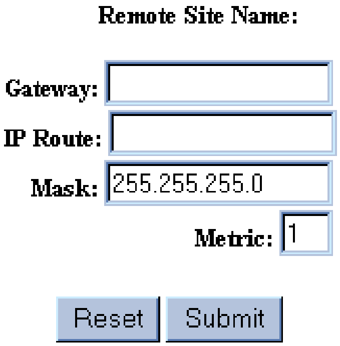
1 Select **Configuration > Remote Sites (WAN)**.

2 Select the remote site to modify, and click **Modify**.

3 Continue clicking **Next** to advance through the **ATM Modify** and **IP Modify** screens to the **IP Advanced Modify** screen.

4 Click **Manage** in the Framed Routes box.

5 Click **Add** to define the following parameters:



Remote Site Name:

Gateway:

IP Route:

Mask: 255.255.255.0

Metric: 1

- **Gateway** (address) — The address of the neighbor router.
- **IP Route**
- **Mask** — The IP address for the mask.
- **Metric** — The maximum number of routers (1-15) through which the data packets must travel before reaching their destination.

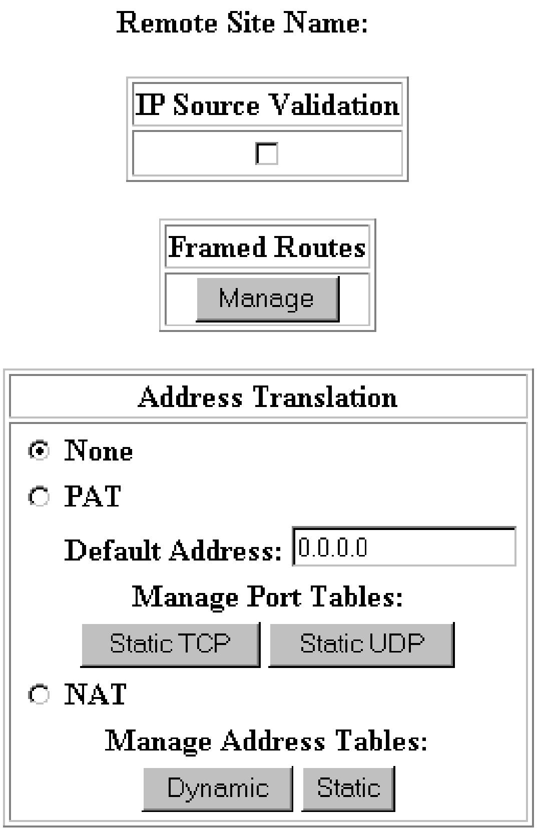
6 After you have entered the fields, click **Submit**.

7 Click **Modify** to change the fields, the **Details** button to view the fields, and the **Delete** button to erase the parameters you have set.

Using IP Address Validation

When IP Source Validation is enabled, the source address of all IP frames received from a remote site will be validated. A source address is valid if the OfficeConnect Remote 840 will route an IP frame destined to the source address on the same interface it came in on.

You need to access the IP Advanced Modify screen, by selecting **Configuration > Remote Sites**, selecting a remote site definition, and click **Modify**. Then keep clicking **Next** to advance through the screens until reaching the **IP Advanced Modify** screen, which contains the following fields:



Remote Site Name:

IP Source Validation

□

Framed Routes

Address Translation

● None

○ PAT

Default Address: 0.0.0.0

Manage Port Tables:

○ NAT

Manage Address Tables:

Check or uncheck the **IP Source Validation** button to respectively enable or disable the IP source validation.

MAC-Encapsulated Routing

MAC-Encapsulated Routing combines routing and bridging so that routing features (i.e., Address Translation, DNS Proxy, DHCP Server, etc.) are available in a bridged environment.

There are no specific changes required in the IP routing configuration to support MAC-Encapsulated Routing.

See "Configuring Bridging" for instructions on how to enable MAC-Encapsulated Routing.

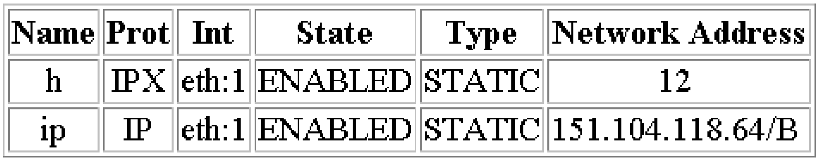
Monitoring

The OfficeConnect Remote 840's IP Routing Table is displayed by accessing the following page: **Monitor > Routes and Services > IP Routes**.

Global IP counters can be displayed through **Monitor > Networks > IP > IP Counters**. This screen indicates the number of frames received and forwarded or discarded.

The active IP interfaces are shown by accessing the following page: **Monitor > Networks > Network Status**.

When a Remote Site has been successfully established and IP is configured, an entry will be displayed with the Remote Site Name followed by a '-ip' suffix. The screen display indicates the local LAN (with name ip) and the Remote Site 'Internet' have active IP interfaces.



Name	Prot	Int	State	Type	Network Address
h	IPX	eth:1	ENABLED	STATIC	12
ip	IP	eth:1	ENABLED	STATIC	151.104.118.64/B

IP Testing (PING)

You can now run a PING to make sure the OfficeConnect Remote 840 can reach the remote router. You can run the PING by using the OfficeConnect Remote 840 Manager, from MS-DOS on a workstation, or through the Internet.

Testing using the OfficeConnect Remote 840 Manager will test the connection from the OfficeConnect Remote 840 to the network.

The DOS PING will check the connection from your PC through the OfficeConnect Remote 840 SDSL Router to the network.

Option 1: OfficeConnect Remote 840 Manager Ping to ISP or Remote Site Network

Open the OfficeConnect Remote 840 Manager and select **Tools > Ping**. Enter the address you wish to ping, whether it is the ISP or a remote site. Click **Submit**.

A Ping Response screen will appear, with the response from the ping. The following responses may occur.

Ping Responses

- **<IPAddress> is alive**

  The PING was successful.

  If a name was entered in the Ping page input field, the corresponding IP address is displayed on the Response page.

- **PING: no route to host**

  A valid IP address or name was entered but the routing table does not indicate how to reach the network that the IP address belongs to.

- **PING: host unreachable**

  This means that an ICMP response was received in response to the PING, indicating that the PING failed because the IP address is currently unreachable. This is indicative of a network problem. If the router could not determine where to send the PING request, the PING: no route to host error would have been generated. Since it was not, the router sent the message either to the specific network to which the IP address belongs or to a default gateway. If it was sent to the specific network and the network was learned via RIP, there is probably a temporary network problem. If the network is a static entry in the routing table (entered by the user, for example), it may have been entered incorrectly. If the network is not in the routing table and the PING request went to a default gateway, then it may be that the network is not supposed to be reachable so this is a reasonable result.

- **PING: timeout waiting for reply from <IP Address>.**

  The host network is probably reachable but there is no answer from this IP Address. There are a couple of possible explanations for this. The IP Address might not be assigned to any unit. The path from the OfficeConnect Remote 840 to the unit is so slow that the PING response did not get back in the allotted time frame. There may be a temporary break in the path.

DNS Errors

- **`Network Name: <name> could not be resolved.`**

- **Network Name: <name> could not be resolved due to a problem interacting with the Name Server.**

The name could not be resolved. Either no DNS server was located or the server(s) did not have the name in the host table list. However, this error will also appear if the user entered an IP address incorrectly - such as 100.100.100.256 (an invalid IP address) so it is interpreted as a name to be resolved by DNS.

- **Network Name: <name> could not be resolved due to a timeout on the request.**

  No response was received from the DNS server to which the DNS request was sent. This could be due to a network connection problem or a very slow line.

Option 2: DOS Ping to ISP or Remote Site Network

From the a workstation on the local LAN, get to an MS-DOS prompt and type **ping <remote IP address> <Enter>** where the remote IP address is the address of a host on the remote network (Ex: ping 10.0.0.12). If no address was provided, contact the ISP or the remote site administrator for an IP address to ping.

The OfficeConnect Remote 840 will call the ISP and send the PING information. A reply from 10.0.0.12 indicates success

An example script of a failed ping is:

```
C:\ping 10.0.0.12
Pinging 10.0.0.12 with 32 bytes of data:
Request timed out.

Request timed out.

Request timed out.

Request timed out.
```

An example script of a successful ping is:

```
C:\ping 10.0.0.12
Pinging 10.0.0.12 with 32 bytes of data:
Reply from 10.0.0.12 bytes=32 time=140ms TTL=240

Reply from 10.0.0.12 bytes=32 time=147ms TTL=240

Reply from 10.0.0.12 bytes=32 time=140ms TTL=240

Reply from 10.0.0.12 bytes=32 time=135ms TTL=240
```

```
C:\_
```

It is not unusual for the first few attempts to time out. If you don't receive a response the first time, try PINGing the router again. If you still don't receive a response, the most likely cause is incorrect routing entries.

Option 3: Internet Browser (Internet Access Only)

If you are connecting to the Internet, start a web browser and enter an address, such as **http://www.3com.com**. If the 3com web site home page comes up, all is configured correctly and you are on your way!

Advanced Troubleshooting

If the 3Com web site home page does not appear, the problem may be incorrect DNS server addresses on your workstation.

For more detailed troubleshooting information, see “Troubleshooting”.

5

CONFIGURING BRIDGING

Introduction

This chapter contains information on configuring bridging for the OfficeConnect Remote 840. If you need more information on the difference between Bridging and Routing, and which one is best for your needs, see Appendix A,"Bridging and Routing".

Overview

A **bridge** connects two or more LANs together at Layer 2 (data link) of the ISO-OSI 7 layer model. A *learning bridge* links networks, but also separates network traffic and forwards only the packets that need to be forwarded based on Media Access Control (MAC) address.

The OfficeConnect Remote 840 can be configured as a learning bridge.

Bridges separate traffic by examining the **MAC** addresses contained in data packets. MAC addresses uniquely identify each machine attached to a network segment. A data packet is not forwarded to another segment if its destination MAC address resides on the same segment as its source.

To efficiently separate traffic, the bridge maintains a **Bridge Forwarding Table**. The table contains a list of MAC addresses and their associated network segments. The table is built dynamically from the source MAC addresses of data packets passing through the bridge.

The OfficeConnect Remote 840 bridge supports the **Spanning Tree Protocol (STP)**. This feature is used when two networks are joined by two bridges forming a looped network. STP prevents data packets from circling the two networks.

The OfficeConnect Remote 840 provides a Bridge Firewall function which allows flexible configuration of simultaneous bridging and routing. For more information on the Bridge Firewall, see Appendix A,"Bridging and Routing".

A boot mode, Default Bridge Mode, can be activated. This automatically configures the unit to bridge all packets (see "Default Bridge Mode").

For more information on bridging, see Appendix A, "Bridging and Routing".

To set up bridging on the OfficeConnect Remote 840, you must:

- "Configuring Bridging for the LAN"
- "Configuring Bridging for the Remote Site Connections"

You may also want to:

- Set up to bridge IP traffic.
- Modify advanced bridging options.
- Use default bridge mode.

If you are planning to use the OfficeConnect Remote 840 to bridge all traffic, you may want to use the boot option Default Bridge Mode (see "Default Bridge Mode").

Configuring Bridging for the LAN

To configure a protocol over the LAN, you need to assign a protocol network to the LAN port by providing a name. After adding a network, you can modify advanced parameters. The network's status appears in the **Monitor > Networks > Network Status** table.

For bridging to take place across the OfficeConnect Remote 840, you also have to enable bridging over the WAN port. See "Configuring Bridging for the Remote Site Connections".

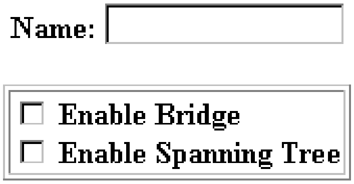
Use the **Local Site (LAN) > Bridge Configuration** screen to define or modify a bridged network over the LAN.

Only one bridged network can be added over the LAN.

Adding a Bridge Network

You may add a bridged network over the Ethernet interface by following these steps:

1. Select **Configuration > Local Site (LAN) > Bridge**.
2. Click **Add**. This accesses a screen containing the following fields.



Name:

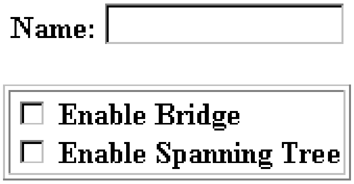
☐ Enable Bridge
☐ Enable Spanning Tree

3. Enter the following:
   - **Name** — Enter a name identifying the bridged network. The name is limited to 32 characters.
4. Check the **Enable Bridge** box and click **Add** when the name has been entered to save your field.
5. Check the **Enable Spanning Tree** box if you wish to enable spanning tree, which is used to eliminate loops in a circular bridged network.

Modifying or Deleting a Bridge Network

To modify information pertaining to an existing Bridge network, or to delete that information from your configuration, follow these steps:

1. Proceed to the **Bridge** screen, following steps 1 and 2 above.
2. Select the bridge network you wish to modify or delete.
3. Click **Modify/Delete**. This accesses a screen containing the following fields:



Name:

□ Enable Bridge
□ Enable Spanning Tree

4. You may uncheck the **Enable Bridge** or **Enable Spanning Tree** boxes if you have previously checked them from this screen, or delete the information about the selected Bridge network by clicking **Delete**.
5. To alter previously set fields, follow step 1 and select a Bridge network in the list and click **Modify**. To delete a network from your configuration, select a network and click **Delete**.
6. Click **Modify** after you have entered the field.

Configuring Bridging for the Remote Site Connections

To set up a protocol over the WAN, a remote site profile must be created and edited for each remote location you want to connect to. With this profile, you specify virtual circuit (VPI, VCI) information, protocols, and addresses that determine the method of connection and communication to that remote site.

The steps you take to assign a network over the WAN are quite different from those to assign a network over the LAN. First you add a remote site profile, and then you modify the profile to enable bridging.

When the remote site connection is established, the bridge network will come up over the WAN interface. The network and its status appears in the **Monitor > Network > Network Status** table.

If you need to connect to multiple remote sites, such as two remote offices, set up a remote site profile for each remote location.

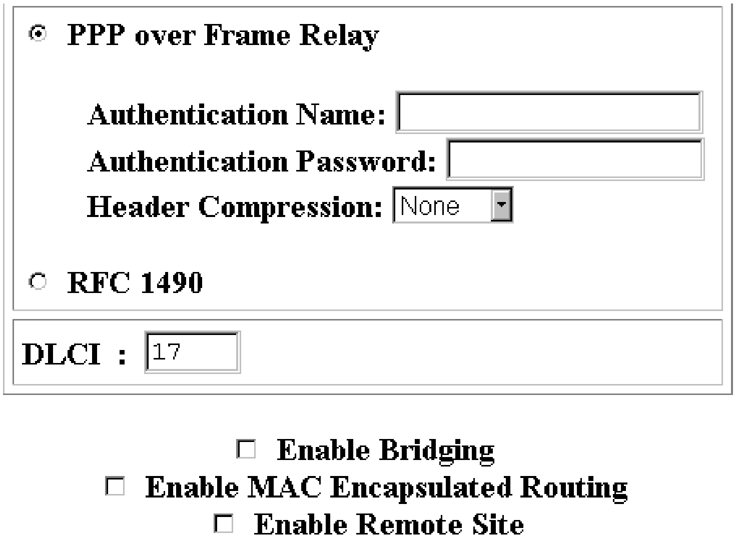
For any routing to take place across the OfficeConnect Remote 840, you also have to set up a corresponding network over the LAN. See "Configuring Bridging for the LAN".

Enabling Bridging

These instructions assume you have already added a remote site profile. If you have not added one, select **Add** instead of **Modify** in step 1 and see "Remote Site Management" for details on other parameters to configure.

To enable bridging:

1 From the OfficeConnect Remote 840 home page, select **Configuration > Remote Sites (WAN)**, select a remote site definition, and click **Modify**. This accesses the **Remote Sites General Modify** screen, containing the following fields:



● **PPP over Frame Relay**

Authentication Name:

Authentication Password:

Header Compression: None

○ **RFC 1490**

DLCI : 17

□ **Enable Bridging**

□ **Enable MAC Encapsulated Routing**

□ **Enable Remote Site**

2 Check the **Enable Bridging** box to enable bridging for this remote site. Then click **Modify**.

Bridging IP Traffic

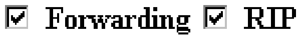
Unless you are using the boot option Default Bridge Mode, the OfficeConnect Remote 840 is set up to **route** IP traffic by default. To **bridge** IP traffic, you must turn off IP Forwarding in the router configuration.

IP Forwarding refers to the routing of IP packets from one interface to another. It does not affect communicating to the OfficeConnect Remote 840 itself. Even when IP Forwarding is disabled, you can perform non-routing functions such as use the OfficeConnect Remote 840 Manager from a Web browser and use PING.

To bridge IP traffic:

1 Add the bridge network over the LAN (see the instructions above).

2 From the OfficeConnect Remote 840 home page, select **Configuration > Global > IP > IP Settings**. This brings up the **IP Settings** screen:



☑ Forwarding ☑ RIP

3 Turn off IP forwarding by unchecking the **Forwarding** check box.

4 Your browser will temporarily lose connection with the OfficeConnect Remote 840. Wait a few seconds, click the browser's **Stop** button; then click **Reload**.

MAC-Encapsulated Routing

Because routers base their forwarding decision on network-level addresses, packets that are routed over a WAN are transmitted without MAC-layer addresses. Additionally, address resolution procedures that can be used to determine the destination MAC address for a packet are not required.

Conversely, packets that are bridged over a Wide Area Connection include MAC-layer information. Address resolution procedures are required.

MAC-Encapsulated Routing uses network-level addresses for forwarding decisions but transmits MAC-layer addresses over the Wide Area Connection. Additionally, address resolution procedures are used. To the remote site, the packets appear as if they had been bridged.

This feature allows the routing features of the OfficeConnect Remote 840 (i.e., address translation, DHCP Server, DNS Proxy, etc.) to be employed in a bridged environment.

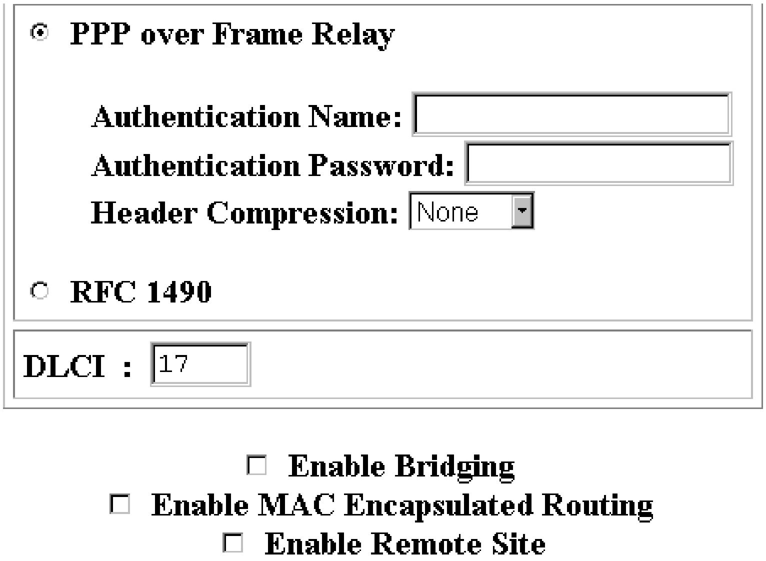
MAC-Encapsulated Routing is specified on a remote site basis. When MAC-Encapsulated Routing is enabled in a remote site profile, packets for the routed protocols configured by the profile (i.e., IP and/or IPX) will be sent using the appropriate bridged encapsulation. If the configured Network Service is PPP, the packets will be encapsulated in BRCP.

MAC-Encapsulated Routing is configured on the **Remote Sites General** screen.

To access the **Remote Sites General** screen:

1 Go to the OfficeConnect Remote 840 home page and select **Configuration > Remote Sites (WAN)**.

2 Select a defined remote site and click **Modify**. This will access the **Remote Sites General Modify** screen, containing the following fields:



● PPP over Frame Relay

Authentication Name:

Authentication Password:

Header Compression: None

○ RFC 1490

DLCI : 17

□ Enable Bridging

□ Enable MAC Encapsulated Routing

□ Enable Remote Site

3 Check the **Enable MAC Encapsulated Routing** box to enable MAC Encapsulated Routing for this remote site.

4 Click **Modify** to save the change.

Bridge Firewall

The OfficeConnect Remote 840 can be configured for simultaneous bridging and routing. IP routing is configured if IP forwarding is enabled (see "Enabling IP Routing" in Chapter 4.)

IPX routing is enabled if an IPX network is present over the Ethernet interface (see "Configuring IPX for the LAN" in Chapter 9). Bridging is enabled by adding a bridge network over the Ethernet interface (see "Configuring Bridging for the LAN"). Routing and bridging are enabled for each destination in its remote site profile.

When configured for simultaneous bridging and routing, packets received from the LAN are first passed through the router for any configured protocols. If the packet can not be routed, it is passed to the bridge depending on the setting of the Bridge Firewall function. The bridge firewall has three modes, which are configured on the Advanced Bridging Options screen.

The three modes are:

1. Discard Routed Protocols (Discard):

> This is the default mode. If a protocol is configured for routing, and a packet for that protocol type is received from the LAN that is not addressed to the MAC address of the OfficeConnect Remote 840, it is discarded. Additionally, broadcasts (including ARPs) for the protocol are not passed to the bridge.

2. Forward Unicast Packets Only (Unicast):

> If a protocol is configured for routing, and a packet for that protocol type is received from the LAN that is not addressed to the MAC address of the OfficeConnect Remote 840, it is bridged. Additionally, ARP broadcasts for IP addresses other than that of the OfficeConnect Remote 840 are also bridged. Other broadcasts for the configured protocol are not bridged.

3. Forward Broadcast/Unicast Packets (All):

> Unicast packets for a configured protocol received from the LAN that are not addressed to the MAC address of the OfficeConnect Remote 840 are bridged. Received broadcasts (e.g., DHCP) are bridged.

Packets received from the WAN do not pass through the Bridge Firewall. Instead, packets received from the WAN are delivered to the router or they are delivered to the router or bridging function based on their encapsulation and on the state of the MAC-Encapsulated Routing parameter in the remote site profile.

In general, a packet received in a routed encapsulation (i.e., IPCP or routed RFC 1483 or RFC 1490) is delivered to the router. A packet received in a bridged encapsulation is passed to the bridge. If MAC-Encapsulated Routing is enabled, the received (bridge-encapsulated) packets are delivered to the router.

Advanced Bridging Options

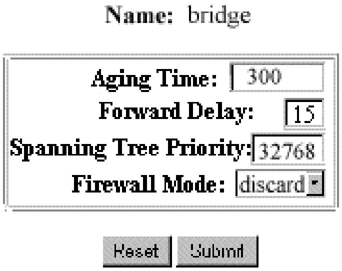
The advanced bridging configuration options are located with the rest of the Local Site configuration options. However, these advanced bridging options function more as global parameters and therefore are applicable to bridging over the WAN as well as the LAN.

Most users do not need to change these values from the defaults.

To alter advanced bridging configurations:

1 Go to the OfficeConnect Remote 840 home page and select **Configuration > Local Site > Bridge**.

2 Click **Advanced** to access a screen containing the following field:



Name: bridge

Aging Time: 300

Forward Delay: 15

Spanning Tree Priority: 32768

Firewall Mode: discard

You may then enter the following fields:

- **Aging Time** — Time (seconds) for aging out forwarding table information.
- **Forward Delay** — Time (seconds) to wait while learning forwarding information before starting to bridge packets.
- **Spanning Tree Priority** — Priority of this spanning tree node. This is used for prioritizing the nodes when spanning tree is enabled (which is determined on either the Bridge Add or Bridge Modify/Delete screens).

If you need to return to the original parameters for this screen, click Reset before you click Submit.

3 Click **Submit** when the fields have been entered to save your customizations.

Default Bridge Mode

Default Bridge Mode Overview

Default Bridge Mode is designed for those who want to use their OfficeConnect Remote 840 to function as a bridge automatically, with no special configuration or software installation required. This mode preconfigures the unit to bridge all packets.

In this mode, you will not be required to use Setup Wizard or install any software from the CD unless you want to change the configuration (you can install from the CD at any time).

There are several different settings for Default Bridge Mode. The different settings control the WAN operational mode; ATM or Frame Relay, and the VPI/VCI or DLCI settings.

If you set the OfficeConnect Remote 840 to this mode and no configuration exists, the OfficeConnect Remote 840 will automatically set up a bridge network on the Ethernet and will create a VC profile that bridges using RFC 1483 or RFC 1490 encapsulation with various VPI/VCI or DLCI values (see "DIP Switch Modes" table in Chapter 1 for details on how to set your router switches to obtain the correct VPI/VCI values for your configuration).

Your OfficeConnect Remote 840 was set in Unconfigured Mode (all switches OFF) before shipping.

The following settings are preconfigured:

- Bridge network on the LAN Interface
- A remote site profile named "Bridge" is set up to bridge all traffic and to use network service RFC 1483, one of several VPI/VCI values, and Unspecified Bit Rate (UBR).
- Spanning Tree Disabled
- Default Login **root** and password **!root**

You will need to tell your service provider to use a connection on VPI / VCI using RFC 1483 or RFC 1490 (bridged).

Boot options only affect the operation of a unit which does not presently have any configuration settings (i.e., the unit is new, the reset button has been clicked, or a delete configuration command has been executed from the CLI or HTML interface). See "Restoring Factory Defaults" in Chapter 2 for more information on how to reset configuration parameters for your OfficeConnect Remote 840.

Installing the OfficeConnect Remote 840 Using Default Bridge Mode

For more instructions on setting up your OfficeConnect Remote 840 using Default Bridge Mode, see the *OfficeConnect Remote 840 SDSL Router Install Guide* that was included the box when you purchased your SDSL router.

Monitoring Bridging

Viewing Bridge Network Status

You can view bridge network status from the **Monitor > Networks > Network Status** screen. This lists the networks (WAN networks incorporate the word "port" in the name) and shows you their states.

Viewing Bridge Forwarding Table

The Bridge Forwarding Table is displayed in the **Monitor > Routes and Services > Bridge Forwarding** screen. In addition to listing the MAC addresses, it provides counters for traffic passing through the bridge to and from the addresses.

Viewing Bridge Counters

General bridge transmit and receive counters are located in the **Monitor > Networks > Bridge** screen.

Testing Bridging

To test bridging:

- Attempt to communicate with the remote location using any bridged protocol. For example, if IP is bridged, try to PING across the WAN connection.
- If IPX is bridged, try to reach a remote server.
- If NetBEUI is bridged, open the Windows 95 or 98 Network Neighborhood to see remote Windows 95, 98, and NT machines.

If you have problems with bridging IP, check that IP Forwarding is *disabled* on the **Configuration > Global > IP > IP Settings** screen. Also, be sure that your LAN IP Addresses belong to the same IP network as the remote site.

6 NETWORK ADDRESS TRANSLATION USING THE OFFICECONNECT REMOTE 840

Introduction

This chapter contains information on address translation using the OfficeConnect Remote 840. It is comprised of the following sections:

- "Selecting Address Translation"
- "Configuring the PAT Default Address"
- "Configuring Static PAT Port Entries"
- "Configuring NAT"
- "Monitoring"

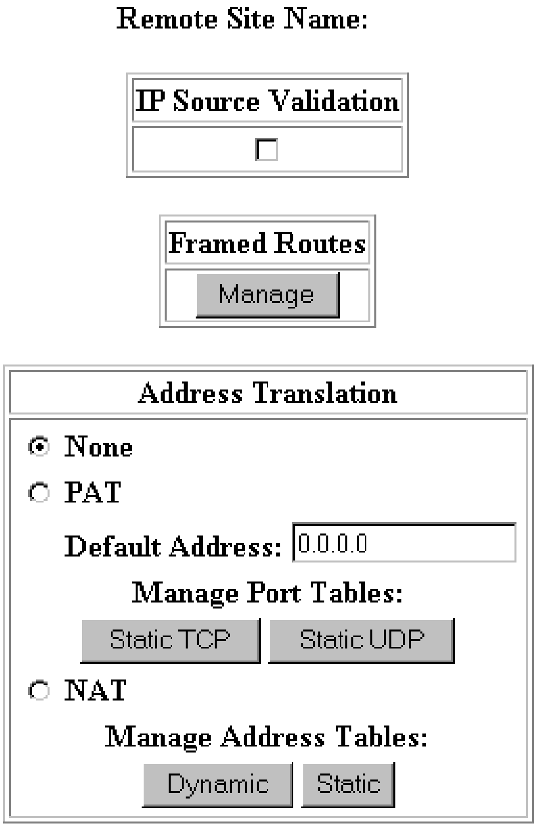
Selecting Address Translation

You must have a Remote Site Profile already defined to set up address translation for this remote site.

1 From the OfficeConnect Remote 840 Manager "home page," select **Configuration > Remote Sites > IP Advanced Modify**.

2 Select the defined site profile and press the **Modify** button.

3 You will then need to advance through the screens by pressing the **Next** button until you reach the **IP Advanced Modify** screen:



Remote Site Name:

IP Source Validation

☐

Framed Routes

Address Translation

● None

○ PAT

Default Address: 0.0.0.0

Manage Port Tables:

○ NAT

Manage Address Tables:

4 Under Address Translation, select **Port Address Translation (PAT)**, **Network Address Translation (NAT)**, or **None** (if you are not using address translation).

If you selected PAT, you must enter the default IP address that will be used. Next you will click either Static TCP or Static UDP to select the Port Table type to be managed.

If you selected NAT, click either Dynamic or Static for the IP Address Table to be managed.

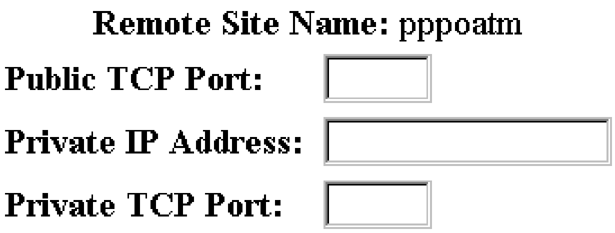
Configuring the PAT Default Address

When PAT is enabled, the default PAT address can be configured. This field should be set to the private address of a workstation on the local LAN. If a data packet is received on the WAN port and a port mapping does not exist, the frame will be translated using the PAT default address.

Press the **Modify** button to set the address.

Configuring Static PAT Port Entries

Press the **Static Transmission Control Protocol (TCP)** or **Static User Data Protocol (UDP)** button to access the static port tables.



Remote Site Name: pppoatm

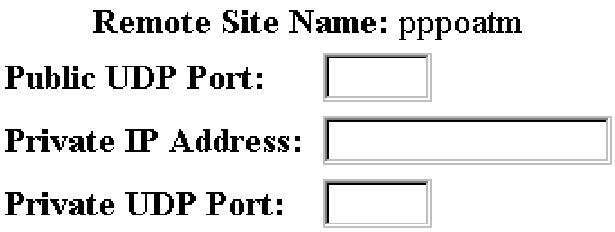
Public TCP Port:

Private IP Address:

Private TCP Port:

- **Static TCP** — Press this button to access the static PAT TCP table (above). Using this table, you can map public TCP ports to private IP address / TCP port pairs.

  This is useful for controlling access to the LAN by remote users. For example, an entry containing public TCP port 80, the IP address of a web server on your LAN, and the private TCP port 80 allows controlled access to the web server but not the rest of your LAN. (For a list of assigned port numbers, see RFC-1700, Assigned Numbers document which is available from the Internet.)



Remote Site Name: pppoatm

Public UDP Port:

Private IP Address:

Private UDP Port:

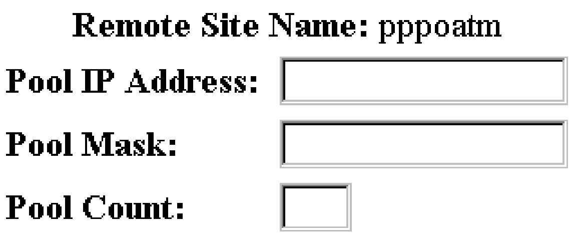
- **Static UDP** — Press this button to access the static PAT UDP table (above). Using this table, you can map public UDP ports to private IP address / UDP port pairs. This is useful for controlling access to the LAN by remote users. (For a list of assigned port numbers, see RFC-1700, Assigned Numbers document which is available from the Internet.)

After Static Port Entries have been configured, return to the **IP Advanced Modify** screen and press the **Modify** button for the changes to take effect.

Configuring NAT

When NAT is configured, static mappings and/or dynamic pools of addresses must be configured. Static assignments permanently map a private address to a public address. Dynamic pools consist of a start IP address, number of addresses in the pool, and a mask to be used for Routing Information Protocol (RIP) messages if the public addresses are to be advertised. Multiple pools can be assigned and static assignments may exist within a pool range.

- **Dynamic** — Press this button to **Add**, **Delete**, or **Modify** the fields in the Dynamic NAT table:



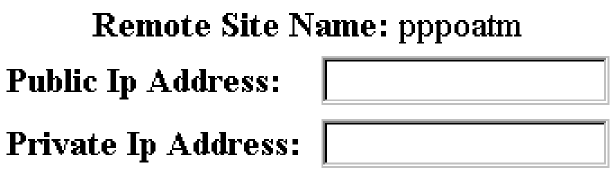
Remote Site Name: pppoatm

Pool IP Address:

Pool Mask:

Pool Count:

- **Static** — Press this button to **Add**, **Delete**, or **Modify** the fields in the Static NAT table:



Remote Site Name: pppoatm

Public Ip Address:

Private Ip Address:

After Static Port Entries have been configured, return to the **IP Advanced Modify** screen and press the **Modify** button for the changes to take effect.

Monitoring

If PAT is used, the active port mappings are shown in the **Monitor > Networks > NAT/PAT > Port Assignments** screen. Only those mappings for the specified Remote Site will be displayed. This screen shows the active port mappings for both TCP and UDP connections. Each entry consists of the public and the private ports, the remote address and port number, and the value of the inactivity timer.

For both NAT and PAT, the active address mappings are shown in the **Monitor > Networks > NAT/PAT > Mapped Addresses** screen. Only those mapping for the specified Remote Site will be displayed. This screen shows the active private addresses, the associated public address, and the number of active TCP and UDP connections. When PAT is configured, each entry will have the same public address.

For more information on these monitoring screens, see "Monitoring the OfficeConnect Remote 840" in Chapter 11.

7 CONFIGURING DHCP

Introduction

This chapter provides information on configuring the DHCP options for the OfficeConnect Remote 840.

- "DHCP Overview"
- "Configuring the DHCP Mode"
- "Configuring the DHCP Server"
- "Configuring the DHCP Relay"
- "Monitoring DHCP"
- "DHCP Smart Mode Overview"

DHCP Overview

Dynamic Host Configuration Protocol (DHCP) is designed to provide a centralized approach to configuring IP addresses and parameters.

When a workstation is configured for automatic assignment of IP addresses, it broadcasts a request out on the LAN. The DHCP Server responds with:

- An IP address for the workstation.
- The domain name.
- The IP addresses of the default router, two DNS Servers, and two WINS Servers.

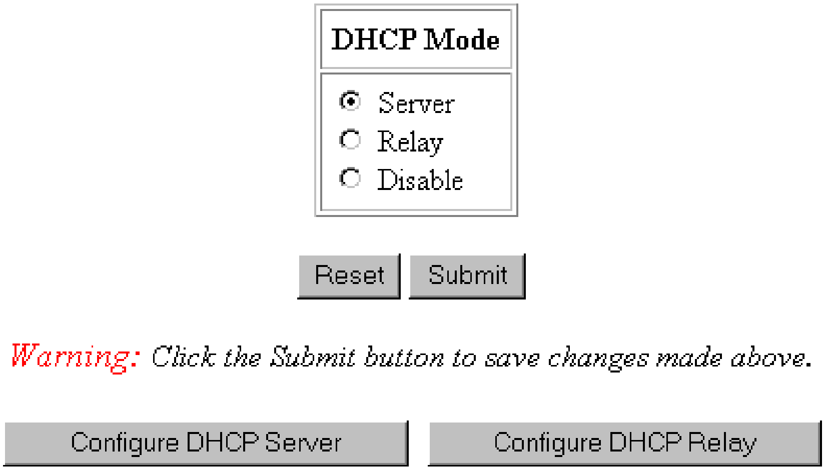
The assignment of an IP address to the workstation is for a specified period of time, referred to as the lease period. Before the lease is set to expire, the workstation will send a request to the server to extend the lease period. The server maintains a list of assigned IP addresses and the duration period of leases. When a lease expires, the corresponding IP address can be reassigned to another workstation.

The OfficeConnect Remote 840 can be configured to support up to 40 workstations on the local LAN. In addition, the OfficeConnect Remote 840 can be configured to be a **DHCP Relay.**

When enabled, the Relay will process the broadcast request from the local workstation and send it to one or two remote DHCP servers. The response from the remote DHCP servers is processed and forwarded to the local workstation.

Configuring the DHCP Mode

The OfficeConnect Remote 840 has three DHCP modes; Server, Relay, and Disable. To configure the mode, select **Configuration > Global > DHCP** from the home page. The following screen will be shown:



DHCP Mode

● Server
○ Relay
○ Disable

Warning: Click the Submit button to save changes made above.

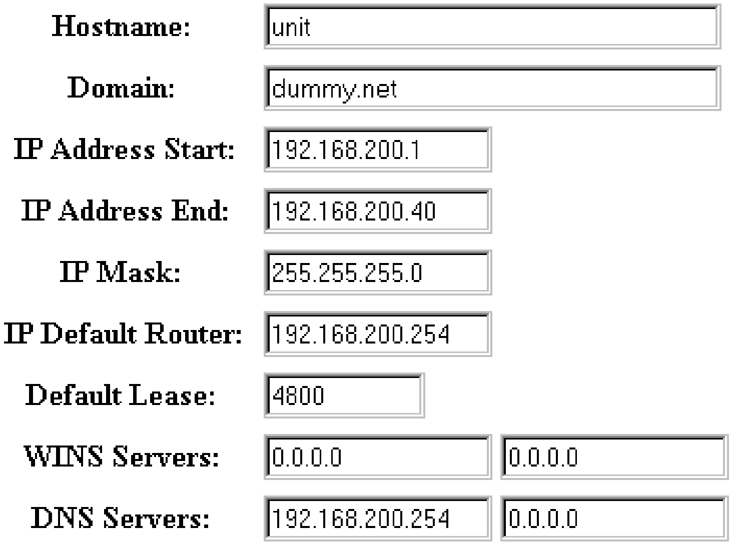
To configure the OfficeConnect Remote 840 as a Server, select **Server > Submit > Configure DHCP Server** to proceed with Server specific settings (see "Configuring the DHCP Server").

To configure the OfficeConnect Remote 840 as a Relay, select **Relay > Submit > Configure DHCP Relay** to proceed with Relay specific settings (see "Configuring the DHCP Relay").

Select the **Disable** button and press the submit button to disable the OfficeConnect Remote 840's DHCP functionality.

Configuring the DHCP Server

The DHCP Server configuration screen contains the following fields:



Hostname:	unit	
Domain:	dummy.net	
IP Address Start:	192.168.200.1	
IP Address End:	192.168.200.40	
IP Mask:	255.255.255.0	
IP Default Router:	192.168.200.254	
Default Lease:	4800	
WINS Servers:	0.0.0.0	0.0.0.0
DNS Servers:	192.168.200.254	0.0.0.0

The OfficeConnect Remote 840's local LAN IP address should be entered in as the IP Default Router and also as the DNS Server if the DNS Proxy functionality is enabled. (For information on DNS Proxy, see "DNS Overview" in Chapter 8.) If you do not know the OfficeConnect Remote 840's local LAN address, refer to the **Configuration > Local Site (LAN) > IP screen**.

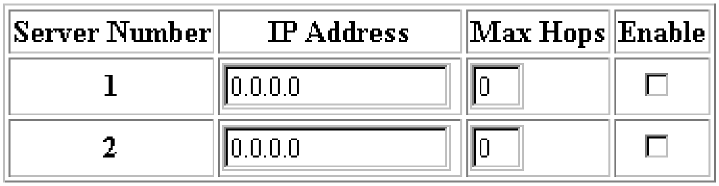
The *Hostname* field is the base name assigned to the workstation. A numeric suffix is appended to the base name and incremented after each assignment. For example, if the Hostname unit is configured, the first workstation will be assigned the Hostname unit01, the second workstation will be assigned unit02 and so forth.

The IP address pool is defined by its the starting and ending IP address. The pool is continuous and has a maximum range of 40. The subnet IP mask entered should correspond with the local LAN's IP mask.

Remaining fields include the **Default Lease** period which is specified in seconds and the WINS Server(s) addresses. If your network does not use a WINS Server, enter in 0.0.0.0 to disable assignment of this parameter.

Configuring the DHCP Relay

If you selected **Relay on the main DHCP** screen, press the Configure DHCP Relay button. This screen contains the following fields:



Server Number	IP Address	Max Hops	Enable
1	0.0.0.0	0	□
2	0.0.0.0	0	□

Enter the IP Addresses of one or two remote DHCP servers and specify the Max Hops (the maximum number of hops through other routers) to reach them. Enable or disable the relay service to them as needed and press the Submit button.

Monitoring DHCP

The OfficeConnect Remote 840's monitoring capability allows you to display DHCP protocol counters and current lease information.

To display the DHCP protocol counters, access the **Monitor > Networks > DHCP > DHCP counters** screen**.**

To display the OfficeConnect Remote 840's DHCP Server lease table, access the **Monitor > Networks > DHCP > DHCP leases** screen.

DHCP Smart Mode Overview

To simplify the installation/configuration process, the OfficeConnect Remote 840 can be initialized with a set of pre-configured parameters.

When the OfficeConnect Remote 840 is first booted in the DHCP Smart Mode, the following DHCP and DNS fields will be automatically configured:

```
IP LAN address: 192.168.200.254
DHCP
IP address start: 192.168.200.1
IP address end: 192.168.200.40
IP Mask: 255.255.255.0
IP Default Router: 192.168.200.254
Default Lease: 4800
WINS Servers: 0.0.0.0 0.0.0.0
DNS Servers: 192.168.200.254 0.0.0.0
DNS Static Host entry:
Domain Name: ocrdsl-3com.com
IP address: 192.168.200.254
```

If you choose DHCP Smart Mode, you should set up the workstations on the OfficeConnect Remote 840's LAN to automatically obtain their IP address. This is the default setting in Windows 95.

If you have configured IP addresses manually on your LAN, you should follow the procedure explained in the Workstation Configuration section of Chapter 3 of the *OfficeConnect Remote 810 Installation Guide* to allow each workstation to automatically learn the new addresses instead.

8 CONFIGURING DNS

Introduction

This chapter provides information on configuring the DNS options for the OfficeConnect Remote 840.

- "DNS Overview"
- "Configuring DNS"
- "Configuring Remote DNS Servers"
- "Configuring Static DNS Host Entries"

DNS Overview

A Domain Name Server (DNS) provides an IP address to a host computer for a given domain name. A DNS Proxy receives requests and attempts to find an entry in its local tables, and if one is not found, forwards the request to a remote server. The remote DNS Server can be learned dynamically through PPP or it can be statically assigned.

The OfficeConnect Remote 840's DNS Proxy enables you to configure remote DNS Servers for specific domains. For instance, assume you have two remote sites configured, one to the Internet and the other to a corporate site which has a domain name of **3com.com**. Two DNS remote servers can be configured, one which uses the corporate site for **3com.com** and the other to use the Internet as the default.

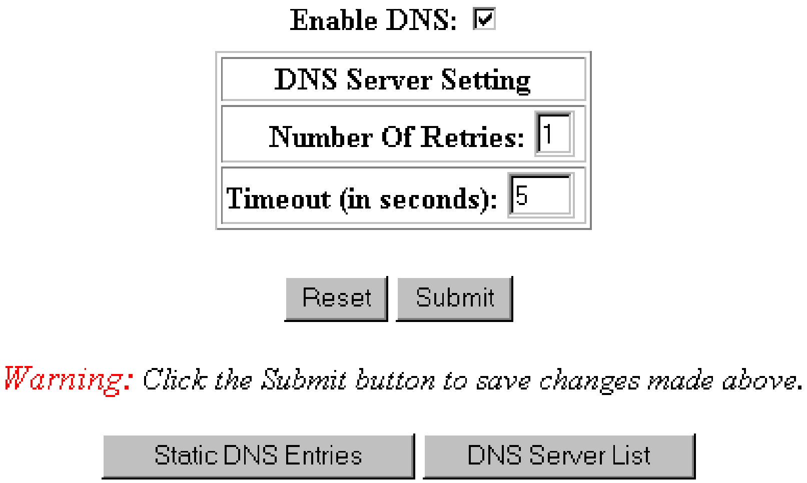
The OfficeConnect Remote 840's DNS Proxy also enables you to configure static host entries. The static table is checked first before the DNS request is forwarded on to the remote server.

If the OfficeConnect Remote 840 was first booted in the DHCP Smart Mode, an entry of **ocrdsl-3com.com** was added which maps to the OfficeConnect Remote 840's local LAN IP address. This entry was added to simplify access to the OfficeConnect Remote 840 Manager.

Configuring DNS

To access the DNS configuration screens, go to the OfficeConnect Remote 840 Manager and select **Configuration > Global > DNS**.

This screen contains the following fields:



Enable DNS: ☑

DNS Server Setting

Number Of Retries: 1

Timeout (in seconds): 5

Warning: Click the Submit button to save changes made above.

1. To enable DNS services, check the **Enable DNS** box.
2. To specify the number of times the OfficeConnect Remote 840 will attempt to reach a primary or secondary DNS server, enter the number in the **Number of Retries** field.
3. To specify the amount of time to wait for a timeout when the OfficeConnect Remote 840 attempts to reach a primary or secondary DNS server, enter the number of seconds in the **Timeout** field.
4. Click **Submit**.

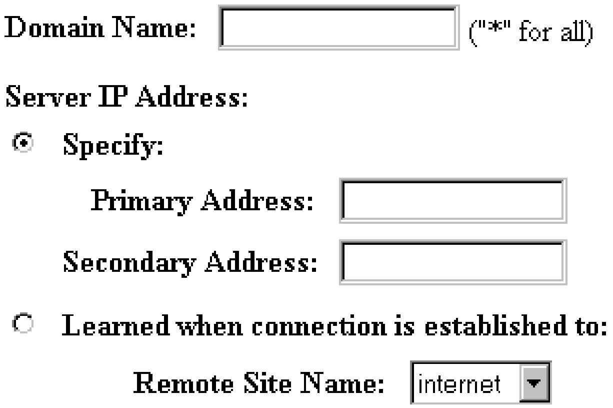
Configuring Remote DNS Servers

When the OfficeConnect Remote 840's DNS Proxy cannot find a domain name in its *local* static entries, it will forward the request to one or two remote servers. The remote DNS Server can be learned dynamically if the remote site is configured for PPP, otherwise it must be specified. Up to two servers may be specified per domain name.

Multiple DNS remote server entries can be added. The server is chosen based on the requested domain name. If a match is not found, the default entry is chosen. The default entry has a domain name of '*'.

1 Select the **DNS Server List** button from the DNS page.

2 To add a new entry, click **Add**. The following screen appears:



Domain Name: ("*" for all)

Server IP Address:

● Specify:

Primary Address:

Secondary Address:

○ Learned when connection is established to:

Remote Site Name: internet

3 Enter the domain name for the entry, enter * for the default.

If the remote site uses PPP, the DNS remote servers can be learned dynamically.

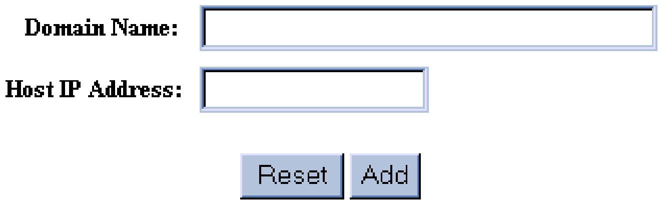
4 Choose the remote site name from the selection box. Otherwise they must be specified. Select **Specify**, and enter the IP addresses of servers.

5 Click **Add**.

Configuring Static DNS Host Entries

The OfficeConnect Remote 840 can function as a DNS server.

1 If you want to configure any **Static DNS Entries**, select Static DNS Entries and click **Add**.



2 Then enter the **Domain Name** and the **Host IP Address** of the machine that has that domain name and click **Add**.

9 CONFIGURING IPX ROUTING

Introduction

This chapter provides an overview on configuring IPX routing for the OfficeConnect Remote 840.

Overview

The OfficeConnect Remote 840 can be configured as a router to forward packets between the local LAN interface and one or more remote sites. A forwarding table is maintained that specifies which interface to route an IPX packet based on the destination IPX network number.

Entries into the forwarding table are either static or dynamic. Static entries are based on the LAN's network number, the remote site WAN interface number, and user configured static routes. Dynamic entries are added when RIP is enabled and routes are learned from neighboring routers.

To configure IPX routing, IPX must be defined on both the LAN interface and one or more remote sites. On the LAN, an IPX network must exist with a specified IPX network number. On the remote sites, IPX forwarding needs to be enabled, and the WAN interface address need to be configured. The WAN interface can be unnumbered (set to 0), numbered, or dynamically learned (if PPP is used).

Configuring IPX for the LAN

To configure IPX over the LAN, assign an IPX network to the LAN port by providing a name and a network address. After adding a network you can modify advanced parameters.

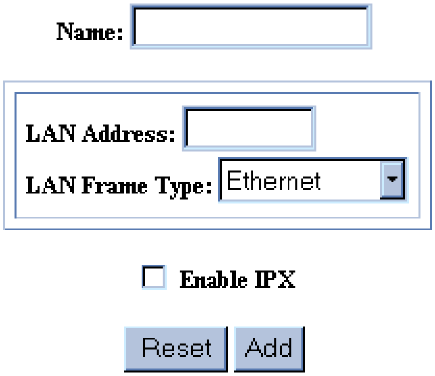
In order for the OfficeConnect Remote 840 to route traffic, you also have to set up a corresponding network over the WAN port. (See "Configuring IPX for Remote Sites Connection".)

Use the **Configuration > Local Site (LAN) > IPX** screen to define or modify all IPX networks over the LAN. Note that each IPX network defined over the LAN must support a different frame type.

Adding a Local IPX Network

To add a Local IPX network:

1 From the OfficeConnect Remote 840 home page, select **Configuration > Local Site (LAN) > IPX**. Click **Add**. This brings up a screen with the following fields:



Name:

LAN Address:

LAN Frame Type: Ethernet

2 Enter a name for the network, the IPX address of the network, and the frame type of the network running on the LAN. Check the **Enable IPX** box.

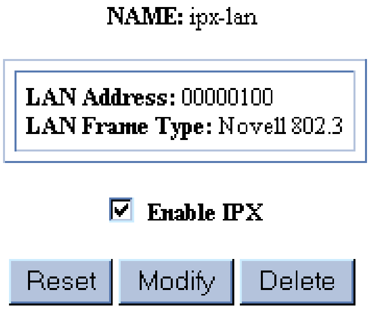
3 Click **Add** to add this defined IPX network.

For information of configuring the IPX RIP and SAP, see "Configuring IPX RIP and SAP".

Modifying or Deleting an IPX Network

To modify information pertaining to an existing IPX network or to delete that information from your configuration, follow these steps:

1. Proceed to the IPX screen, following steps from the previous section.
2. Select an IPX network you wish to modify or delete.
3. Click **Modify/Delete**.This brings up the **IP Modify/Delete** screen containing the following fields:



NAME: ipx-lan

LAN Address: 00000100
LAN Frame Type: Novell 802.3

☑ **Enable IPX**

4. You may enable or disable the selected IPX network by clicking **Modify** or **Delete**.
5. Click **Modify** after you have entered your fields.

   If you need to return to the original parameters for this screen, click the **Reset** button before you click **Modify**.

Configuring IPX for Remote Sites Connection

To set up a protocol over the WAN, a remote site profile must be created and edited for each remote location you want to connect to. With this profile, you specify virtual circuit (VPI, VCI) information, protocols, and addresses that determine the method of connection and communication to that remote site.

The steps you take to assign a network over the WAN are quite different from those to assign a network over the LAN. First you add a remote site profile, then you modify the profile to include the WAN network information, such as IPX addresses and IPX routing.

If you need to connect to multiple remote sites (i.e., two remote offices) you can set up a remote site profile for each remote location.

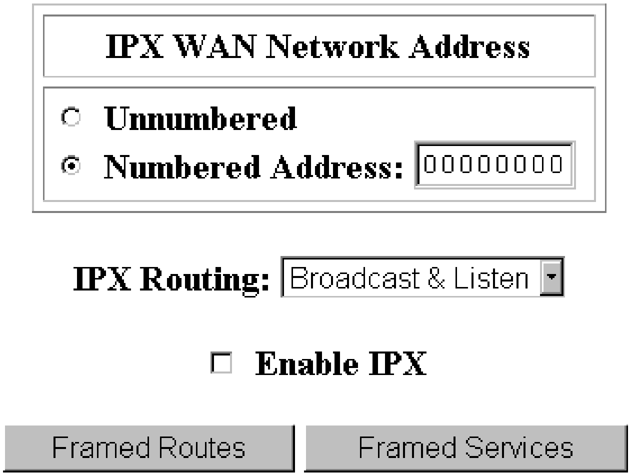
For any routing to take place across the OfficeConnect Remote 840, you also have to set up a corresponding network over the LAN. See "Configuring IPX for the LAN" for details.

The IPX configuration for the remote site begins at the **IPX Modify screen.**

These instructions assume you have already added a remote site profile. If you need to add a remote site profile, see "Remote Site Management" in Chapter 3 for details on adding a remote site profile.

Configure the Remote Site IPX Network Information

1. Access this screen by going to the OfficeConnect Remote 840 "home page." Select **Configuration > Remote Sites (WAN)**.
2. Select a profile and click **Modify**. This will access the **Remote Sites General Modify** screen.
3. Continue clicking **Next** to advance through the ATM Modify, IP Modify, and IP Advanced Modify screens.
4. Click **Next** to proceed to the **IPX Modify** screen.



IPX WAN Network Address

○ Unnumbered
● Numbered Address: 00000000

IPX Routing: Broadcast & Listen

□ Enable IPX

5 Check the correct box in the IPX WAN Network Address box.

- Select **Unnumbered** to use the IPX address that is assigned to the Ethernet port,

  OR

- If the remote site's network administrator provided you with a WAN IPX address, select **Numbered Address**. Enter the IPX address assigned to the WAN port.

6 To automatically learn IPX RIPs and SAPs, set the IPX Routing option to **Both**.

7 Check the **Enable IPX** checkbox.

8 Remember to save the configuration by clicking **Save** on the sidebar.

Configuring IPX Static and Framed Routes

A static route is a configured route that will remain in the routing table until deleted. Static routes differ from dynamic routes in that dynamic routes are learned from real-time via RIP or when new connections are established.

A framed route is much like a static route in that you manually configure the route. The difference is that a static route is defined for the LAN while a framed route is associated with a remote site. Also, while a static route is active when the LAN is connected, a framed route is active only when the connection to the associated remote site is active.

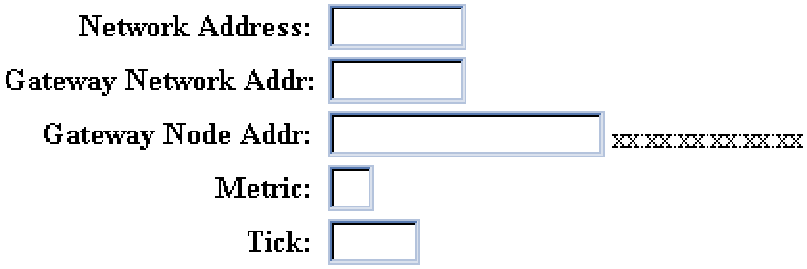
Use static and framed routes only for networks not learned using RIP.

Adding a Static IPX Route to the Local Site (LAN)

To add, modify, or delete a static route to the LAN, follow these steps:

1 From the OfficeConnect Remote 840 home page, select **Configuration > Global > IPX > IPX Static Routes**.

2 Click **Add**. This accesses a screen containing the following fields:



Network Address:

Gateway Network Addr:

Gateway Node Addr: xx:xx:xx:xx:xx:xx

Metric:

Tick:

3 Define the Route by entering the following fields:

- **Network Address** — The address of the network.
- **Gateway Network** — The address of the router that joins the networks.
- **Gateway Node Address** — The hardware address of the gateway node.
- **Metric** — The number of routers (1-15) through which data packets travel before reaching their destination.
- **Tick** — A tick represents how far away the destination is for a data packet (in seconds).

4 Click **Submit**. To clear the fields, click **Reset**.

5 To delete a route from your configuration, select the route and click **Delete**.

Adding a Framed IPX Route to a Remote Site (WAN)

To add, modify, or delete a framed route to a Remote Site, follow these steps:

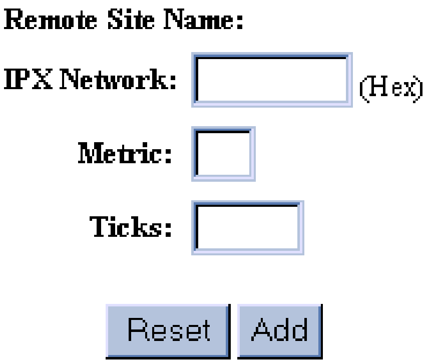
1 Select **Configuration > Remote Sites (WAN)**.

2 Select the remote site to modify, and click **Modify**.

3 Continue clicking **Next** to advance through the **ATM Modify**, **IP Modify**, **IP Advanced Modify** screens to get to the **IPX Modify** screen.

4 Click **Framed Routes**.

5 Click **Add** to define the following parameters:



Remote Site Name:

IPX Network: (Hex)

Metric:

Ticks:

- **IPX Network** (address) — The IPX address of the network.
- **Metric** — The number of routers (1-15) through which data packets travel before reaching their destination.
- **Ticks** — A tick represents how far away the destination is for a data packet (in seconds).

6 After you have entered the fields, click **Submit**.

7 Click **Modify** to change the fields, the **Details** button to view the fields, and the **Delete** button to erase the parameters you have set.

Configuring IPX Static and Framed Services

The services table contains IPX server names, the services they provide, their network and node addresses, and their relative distances. Examples of services include file servers and printers.

A static service entry will remain in the service table until deleted. Static services differ from dynamic services in that dynamic services are learned real-time via SAP packet exchange between routers.

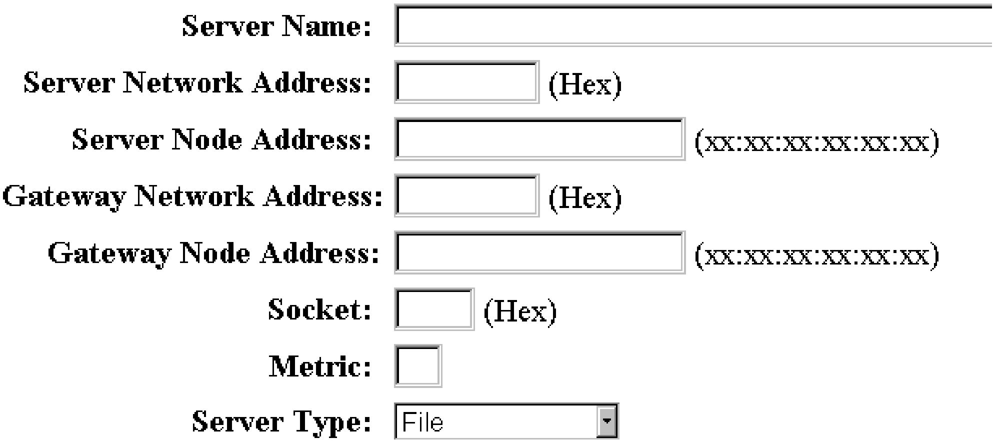
A static service entry is a manually configured service accessible over the LAN. A framed service is a manually configured service accessible from a remote site. A framed service is active only when the connection to the associated remote site is active.

Use static and framed services only for servers not learned using SAP.

Adding a Static IPX Service to a Local Site (LAN)

To add a static IPX Service to a LAN:

1. Select **Configuration > Global > IPX > IPX Services**.
2. Click **Add** to define the following parameters of a static service:



Server Name:		
Server Network Address:		(Hex)
Server Node Address:		(xx:xx:xx:xx:xx:xx)
Gateway Network Address:		(Hex)
Gateway Node Address:		(xx:xx:xx:xx:xx:xx)
Socket:		(Hex)
Metric:		
Server Type:	File	

- **Server Name** — The name of the remote server.
- **Server Network Address** — The network address of the remote server.
- **Server Node Address** — The node address of the remote server.
- **Gateway Network Address** — The network node address of the gateway.
- **Socket** — The socket number on the server.
- **Metric** — The number of routers (1-15) through which data packets travel before reaching their destination. This value represents how far the server is in hops through other routes. Metric is also referred to as hop count.
- **Server Type** — Select the type of server the framed service is connected to.

3. After you have entered the fields, click **Add**.

Adding a Framed IPX Service to a Remote Site (WAN)

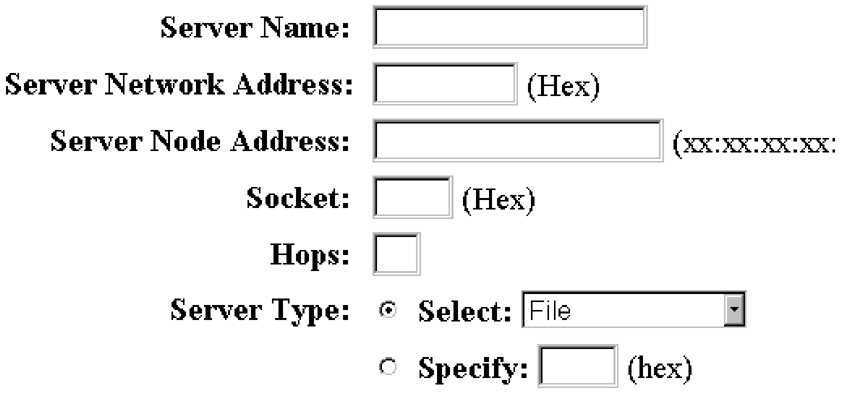
To add, modify, or delete a framed service for a remote site:

1 Select **Configuration > Remote Sites (WAN)**.

2 Select the remote site to modify, and click **Modify**.

3 Continue clicking **Next** to advance through the **ATM Modify**, **IP Modify**, **IP Advanced Modify** screens to get to the **IPX Modify** screen.

4 Click **Framed Services**.



Server Name:

Server Network Address: (Hex)

Server Node Address: (xx:xx:xx:xx:

Socket: (Hex)

Hops:

Server Type: ● **Select:** File

○ **Specify:** (hex)

5 Click **Add** to define the following parameters:

- **Server Name** — The name of the remote server.
- **Server Network Address** — The network address of the remote server.
- **Server Node Address** — The node address of the remote server.
- **Socket** — The socket number on the remote server.
- **Hops** — The number of routers (1-15) the packets travel through before reaching their destination server.
- **Server Type** — You can either select the type of server the framed service is connected to, or enter a hex value for the server type.

6 After you have entered the fields, click **Submit**.

Configuring IPX RIP and SAP

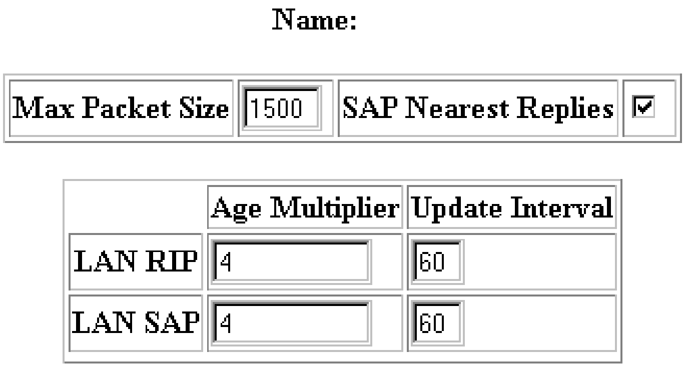
RIP is utilized as a means of communicating routing information between routers. This is done to keep the routers updated on information. Service Advertising Protocol (SAP) is a protocol used by IPX servers and routers to exchange information about the location of servers.

Local Site (LAN) RIP and SAP

IPX RIP and SAP parameters can be configured in the advanced IPX options for the local site (LAN).

1 Select **Configuration > Local Site > IPX**.

2 Select the **Local Site** definition from the list and click **Advanced** to access the **IPX Advanced** screen containing the following parameters:



Name:

Max Packet Size	1500	SAP Nearest Replies	☑

	Age Multiplier	Update Interval
LAN RIP	4	60
LAN SAP	4	60

- Your network performance may be degraded if you set the IPX maximum packet size to less than 500 bytes. It is not generally recommended to modify the IPX maximum packet size.
- Checking the **SAP Nearest Replies** box requests the nearest server for routing information.

3 Enter the value for the **LAN RIP** and **LAN SAP Age Multipliers**. These are values by which to multiply the corresponding update interval to obtain the length of time (seconds) before aging out entries in either the RIP or SAP database.

4 Enter the **Update Intervals** for the LAN RIP and LAN SAP. These are the intervals (seconds) for how often the LAN should send out periodic RIP or SAP updates.

5 Click Submit when the values on the screen have been correctly entered.

Remote Site (WAN) RIP and SAP

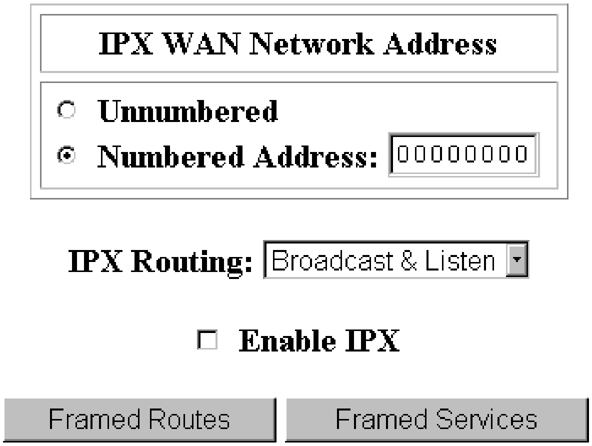
IPX RIP and SAP parameters can be configured on the remote site IPX Modify screen.

Access this screen by going to the OfficeConnect Remote 840 home page.

1 Select **Configuration > Remote Sites (WAN)**, and click **Modify**. This will access the **Remote Sites General Modify Screen**.

2 Continue clicking **Next** to advance through the **ATM Modify**, **IP Modify**, and **IP Advanced Modify** screens.

3 Click **Next** to proceed to the **IPX Modify** screen.



IPX WAN Network Address

○ Unnumbered

● Numbered Address: 00000000

IPX Routing: Broadcast & Listen

□ Enable IPX

4 Using the **IPX Routing** box, select the mode for RIP and SAP operation:

- **Broadcast** — Send RIP and SAP packets.
- **Broadcast & Listen** — Learn from RIP and SAP packets and send RIP and SAP packets.
- **Listen** — Learn from received RIP and SAP packets.
- **Respond Only** — Only respond to received RIP and SAP packets.
- **None** — Neither send nor receive RIP and SAP packets.

IPX Routing Configuration to Support MAC-Encapsulated Routing

Media Access Control (MAC)-Encapsulated Routing combines routing and bridging so that routing features (i.e., Address Translation, DNS Proxy, DHCP Server, etc.) are available in a bridged environment.

There are no specific changes required in the IPX routing configuration to support MAC-Encapsulated Routing. See "Configuring Bridging" in Chapter 5 for instructions on how to enable MAC-Encapsulated Routing.

Monitoring IPX

- To display the forwarding table:

  Go to the **Monitor > Routes and Services > IPX Routes** screen.

- To display the SAP table:

  Go to the **Monitor > Routes and Services > IPX Services** screen.

- To display the Global IPX counters:

  Go to the **Monitor > Networks > IPX > IPX Counters** screen (indicates the number of data packets received and forwarded or discarded).

- To display the IPX interfaces:

  Go to the **Monitor > Networks > Network Status** screen. When a remote site has been successfully established and IPX is configured, an entry will be displayed with the Remote Site Name followed by an "-ipx" suffix.

IPX Testing

If the IPX routing has been setup correctly and if the remote network is functioning, you should be able to access remote Novell servers or perform other IPX tasks.

If you have problems, you should check the **Monitor > Routes and Services > IPX Routes** and **IPX Services** screens to see if the expected routes and services have been learned via RIP and SAP.

If remote routes and services have not been learned, check the **Configuration > Remote Sites (WAN) > IPX** screens and ensure that **IPX Routing** is set to **Listen** or **Listen and Broadcast**.

For more information on these monitoring screens, see "Monitoring the OfficeConnect Remote 840" in Chapter 11.

10 UPGRADING OPERATIONAL SOFTWARE FOR THE OFFICECONNECT REMOTE 840

Introduction

This chapter details the updating of the OfficeConnect Remote 840 software. It is divided into the following sections:

- "Obtaining Updated OfficeConnect Remote 840 Software"
- "Installing Operational Software to the OfficeConnect Remote 840 Unit"

Obtaining Updated OfficeConnect Remote 840 Software

The OfficeConnect Remote 840 operational software is stored in the unit's FLASH memory. In order to update the operational software, you must first obtain and copy it to your PC's hard drive. You can then install it into FLASH memory on the OfficeConnect Remote 840.

The method of obtaining the latest versions of the OfficeConnect Remote 840 Operational Software is either via the 3Com website, **www.3com.com/ocr840** or via the CD. Install the latest version software from the website or the OfficeConnect Remote 840 CD. Type ***show system***, using the CLI interface, to verify the version software installed on your OfficeConnect Remote 840.

If you have erased the operational software from your OfficeConnect Remote 840, you will need to reinstall the software using a utility on your CD. Follow the procedure described in "Installing Software via DOS".

Once you obtain the OfficeConnect Remote 840 operational software, there are two methods of installing the software into the FLASH memory.

- OfficeConnect Remote 840 Manager Software Update (preferred method).
- DOS Update.

OfficeConnect Remote 840 CD

If you have obtained an updated OfficeConnect Remote 840 CD, or if you have erased the copy of the OfficeConnect Remote 840 Operational Software from your hard drive, you need to copy the operational software from the CD to your hard drive.

1. Insert the OfficeConnect Remote 840 Installation CD in your PC's CD drive.
2. Click **Start > Run**.
3. Type ***x*:\setup.exe** (where x is the letter of your CD drive) and click **OK** to start the OfficeConnect Remote 840 software installation.

Follow the prompts on your screen to finish the software installation. In addition to installing the OfficeConnect Remote 840 operational software, this will also install the utilities, HTML help, and printable documentation.

*The OfficeConnect Remote 840 operational software (the *.nac file) included on the CD is copied to your hard drive and not the OfficeConnect Remote 840 unit. It is installed to **C:\Program Files\3Com\ocr840**.*

Installing Operational Software to the OfficeConnect Remote 840 Unit

After you have obtained the operational software using one of the described methods, it will reside on your computer's hard drive in a file with an extension of '.nac' (a NAC file). You can install this software in the FLASH memory of the OfficeConnect Remote 840 using one of the following methods.

- OfficeConnect Remote 840 Manager — This is the preferred method of installing the operational software. Because the installation occurs via the browser's file upload capability, it is the fastest and most convenient method.
- DOS Update — This method uses a DOS-based utility program to install the new software using a serial connection between your PC and the OfficeConnect Remote 840's console port. This method is much slower than installing with the OfficeConnect Remote 840 Manager.

Installing Software via OfficeConnect Remote 840 Manager

Installation of the operational software using the OfficeConnect Remote 840 Manager is a three-part process. First, the current software must be erased from the FLASH memory of the OfficeConnect Remote 840. Once the current software has been erased from the unit you will provide the browser with the pathname of the new NAC file. The browser will then load this file into the unit's FLASH memory. Finally, you will reboot the unit to allow the new operational software to become active.

The software update process does not change configuration of the OfficeConnect Remote 840. However, since a reboot is needed at the end of the process, you should make sure to save the current configuration.

Your browser must support RFC1867 File Upload. This requires Microsoft Internet Explorer version 3.02 (with the file upload add-on installed) or Netscape Navigator 3.0 or higher. You can install Internet Explorer 4 and the file upload add-on from the OfficeConnect Remote 840 Installation CD.

To update the software, go to **Tools > Software Update** from the OfficeConnect Remote 840 Manager home page. You will be guided through the update process.

When browsing for the update file, select 'All files (.*)' on the file type pull-down menu.*

Installing Software via DOS

Your OfficeConnect Remote 840 Installation CD installs a DOS-based utility program onto your hard drive. This utility program, **PCSDL.EXE**, is invoked by a DOS-batch file, **DL.BAT**, which has also been installed to your drive.

In order to use PCSDL to load code to your OfficeConnect Remote 840, use the console port straight-through console cable (provided) between your workstation's serial port and the unit's console port.

To update the software from DOS, perform the following:

1. Using a terminal application such as HyperTerminal to test the serial connection, set up the terminal application with the following settings:

   9600 baud, No stop bits, 8-bit characters, no parity

2. Press Enter on your workstation. If the terminal application displays the **OfficeConnect Remote 840>** prompt, the serial connection is operational.
3. Power off your OfficeConnect Remote 840.
4. Open a DOS window on your workstation.

5 Change to the directory containing the new operational software. If you obtained the software from the Installation CD or using Instant Update the default directory is **c:\Program Files\3Com\ocr840**.

The DL.BAT batch file uses the Com 1 port by default. You can change the port used by editing the DL.BAT file. The relevant lines of the file are shown below.

```
REM
REM Edit the pcsdl command line -v parameter so that it includes
REM the REM version number of the NAC file. The version number of
REM the NAC file is part of the filename. The filename syntax is:
REM
REM vaxxyyzz where xx = major version number
REM yy = minor version number
REM zz = revision number
REM
REM Release 1.0.1 would have a filename of va010001.
REM
REM
REM Change the -p option on the pcsdl command line to use the
REM proper COM port.
pcsdl -p1 -r%BAUDRATE% -vNA1.0.5 -vSD0.1.1 -nSD%2 -nNA%2
```

6 Execute the batch file with the following command: **dl 115 ms**

7 When **Establishing Communications...** appears in your DOS window, plug the OfficeConnect Remote 840 back into the outlet.

8 Wait for the download to complete.

11 MONITORING THE OFFICECONNECT REMOTE 840

Introduction

This chapter describes the details for performing the system monitoring on the OfficeConnect Remote 840.

- "Overview"
- "Throughput Performance"
- "Ethernet Interface"
- "Interface Status"
- "Remote Site Connection"
- "IP"
- "DHCP"
- "Address Translation"
- "IPX"
- "Bridge"
- "The following screen capture shows a successful connection to a remote site named red using PPP network service. Critical Events Log"

Overview

The OfficeConnect Remote 840 Manager provides a wide range of monitor screens, including real-time throughput graphs, routing tables, and interface and protocol counters. The screens help to troubleshoot connection problems and are grouped by topic below.

Throughput Performance

Real-time throughput graphs display both the transmit and receive ATM throughput for up to four remote site connections. To access this screen, go to the OfficeConnect Remote 840 Manager home page and select **Monitor > ATM Throughput.**

The throughput is displayed as line graphs that move from left to right across the screen. The color-coded list of remote site names to the right of the graphs correspond to the colored lines on the graph. A maximum of four remote sites are monitored simultaneously. Performance is measured in kilobytes per second (Kbps), with samples taken every five seconds. The maximum throughput for all remote site connections combined is determined by the service provider when the SDSL link comes up. This maximum can be calculated from the negotiated SDSL baud and constellation rates (see ATM Interface section below.)

Because the SDSL link is shared by all remote site connections, the throughput for a specific connection varies depending on the traffic of the other connections. If one connection is using most of the bandwidth, there is less available for the other connections. Throughput also depends on the type of traffic on the connection. For example, downloading a text file from the Internet may generate a very low volume of incoming traffic, while receiving high resolution graphics display will cause the received throughput to increase dramatically.

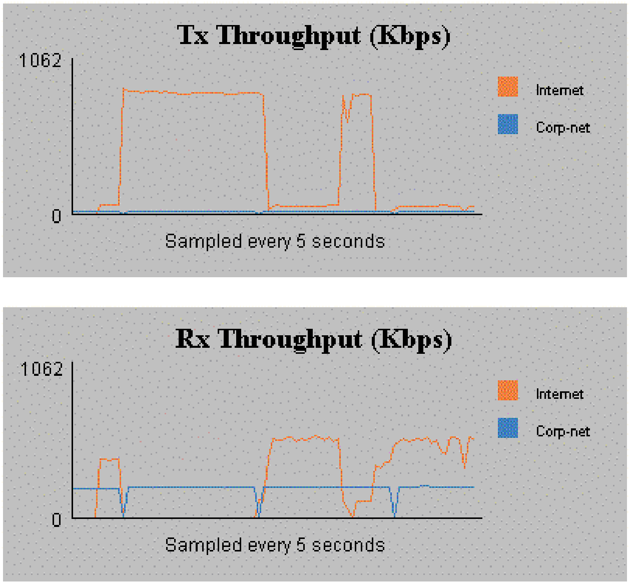


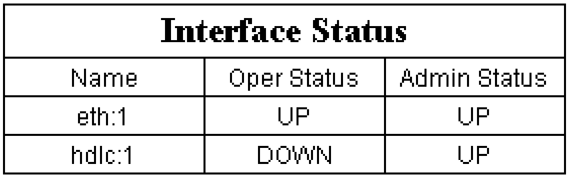
Figure 11–1 Throughput Graphs

Ethernet Interface

Interface Status

The Interface Status screen provides real-time information about the interfaces. To bring up this screen, from the OfficeConnect Remote 840 Manager home page, select **Monitor > Interface Status**. Ethernet interface information is displayed in the row containing the interface name **eth:1**.

The **Oper Status** column indicates whether the interface link is operationally up or down. If it is down, there may be a cabling problem. The **Admin Status** is set to ***up*** by default. If the **Admin Status** is ***down***, then the interface has been disabled by a user and will not operate until it is re-enabled. (Use CLI to enable or disable the operational state.)



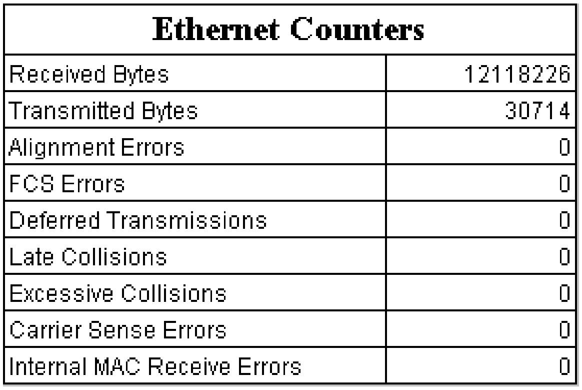
Interface Status		
Name	Oper Status	Admin Status
eth:1	UP	UP
hdlc:1	DOWN	UP

Ethernet Counters

The Ethernet counters screen shows real-time counters based on data packets that cross the Ethernet interface. Access this screen from the OfficeConnect Remote 840 Manager home page by selecting **Monitor > Ethernet**.

The counters displayed include the number of bytes transmitted, bytes received, and errors.

Error counters may not increment consistently. For example, rebooting the device may generate a few interface errors as the hardware resets. Errors that increase rapidly and consistently indicate a problem, either in the LAN connection, a connected device, or the OfficeConnect Remote 840 hardware.



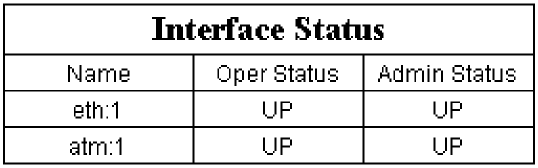
Ethernet Counters	
Received Bytes	12118226
Transmitted Bytes	30714
Alignment Errors	0
FCS Errors	0
Deferred Transmissions	0
Late Collisions	0
Excessive Collisions	0
Carrier Sense Errors	0
Internal MAC Receive Errors	0

Interface Status

ATM Status

The Interface Status screen provides real-time information about the interfaces. To bring up this screen, from the OfficeConnect Remote 840 Manager home page, select **Monitor > Interface Status**. ATM interface information is displayed in the row containing the interface name **atm:1** or **hdlc:1**.

The **Oper Status** column indicates whether the interface link is operationally up or down. If it is down, there may be a cabling problem. The **Admin Status** is set to ***up*** by default. If this field says ***down***, then the interface has been disabled by a user and will not operate until it is re-enabled. Use CLI to enable or disable the operational state.



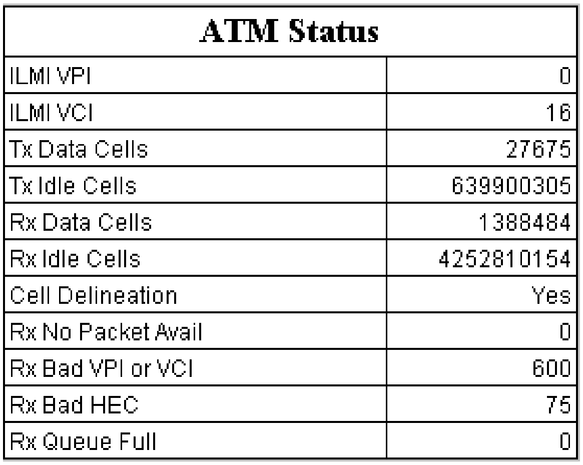
Interface Status

Name	Oper Status	Admin Status
eth:1	UP	UP
atm:1	UP	UP

ATM Cell Status

You can view real-time cell status from the ATM Status screen. To access this screen from the OfficeConnect Remote 840 Manager home page, select **Monitor > ATM**.

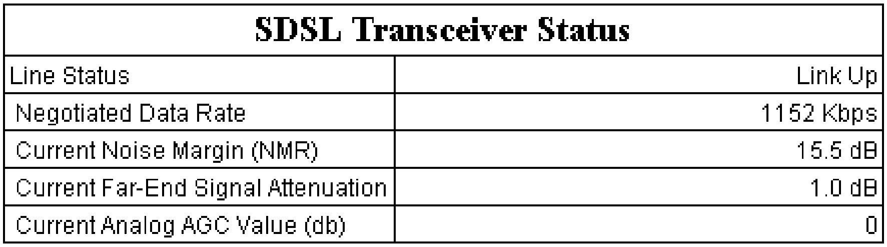
The information includes Cell Delineation status, Data and Idle Cell counters, and error detection, all of which are used to determine the health of your ATM link. A few error counts are not unusual but errors which increment consistently should be reported to your service provider.



ATM Status	
ILMI VPI	0
ILMI VCI	16
Tx Data Cells	27675
Tx Idle Cells	639900305
Rx Data Cells	1388484
Rx Idle Cells	4252810154
Cell Delineation	Yes
Rx No Packet Avail	0
Rx Bad VPI or VCI	600
Rx Bad HEC	75
Rx Queue Full	0

SDSL Transceiver Status

The transceiver status screen provides line information that can be useful to the service provider when you experience line problems. Access this information in the **Monitor > SDSL > Transceiver Status** screen.



SDSL Transceiver Status	
Line Status	Link Up
Negotiated Data Rate	1152 Kbps
Current Noise Margin (NMR)	15.5 dB
Current Far-End Signal Attenuation	1.0 dB
Current Analog AGC Value (db)	0

When the line is up, the Link Status is "Link Up." Any other status should be reported to the service provider. Other values may help the service provider identify line problems.

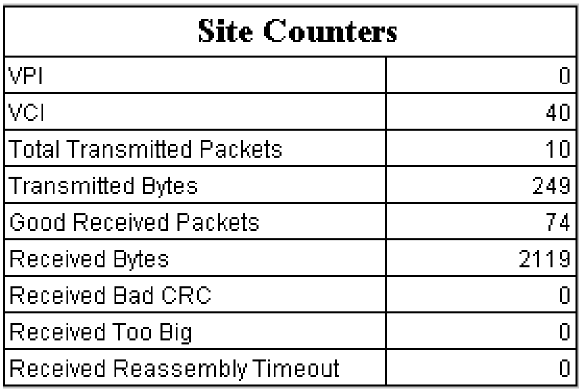
Remote Site Connection

Connection Traffic/Error Counters

You can view remote site connection traffic and error counters. From the OfficeConnect Remote 840 Manager home page select **Monitor > Remote Sites > Remote Site Counters**. Then select the remote site name from the list and press the **Show** button.

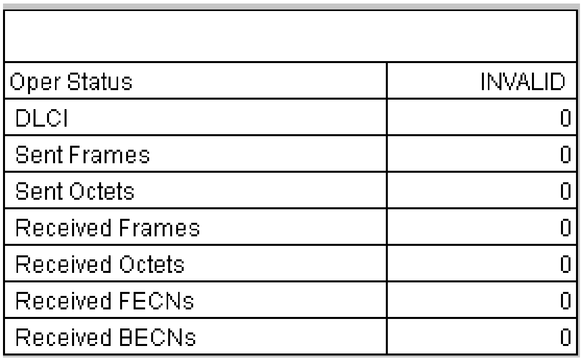
The counters include the number of packets and bytes transmitted and received and error counters. The error counters may increment occasionally, and should be ignored unless they increment quickly and consistently. Rapidly increasing errors should be reported to the service provider

ATM Site Counters



Site Counters	
VPI	0
VCI	40
Total Transmitted Packets	10
Transmitted Bytes	249
Good Received Packets	74
Received Bytes	2119
Received Bad CRC	0
Received Too Big	0
Received Reassembly Timeout	0

Frame Relay VC Site Counters

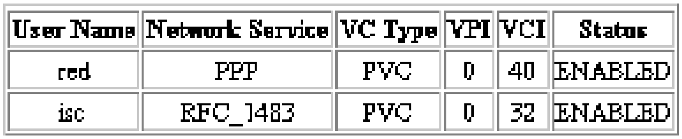


Oper Status	INVALID
DLCI	0
Sent Frames	0
Sent Octets	0
Received Frames	0
Received Octets	0
Received FECNs	0
Received BECNs	0

Remote Site Status Table

To view a complete list of configured remote site profiles and their status, access the Remote Site Status screen by selecting **Monitor > Remote Sites > Remote Site Status**.

The status table includes the configured network service, VPI and VCI for each remote site as well as the operational status of the profile.



User Name	Network Service	VC Type	VPI	VCI	Status
red	PPP	PVC	0	40	ENABLED
isc	RFC_1483	PVC	0	32	ENABLED

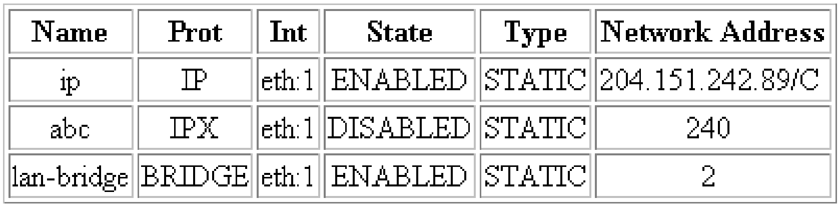
IP

IP Networks

IP networks are created when you configure IP over the LAN and when a remote site connection is configured to route IP traffic. To view the list of IP networks and their status, bring up the **Network Status** screen. This screen lists the status of all OfficeConnect Remote 840 IP, IPX, and Bridge networks. To see this screen, go to the OfficeConnect Remote 840 Manager home page and select **Monitor > Networks > Network Status**.

The network status table shows the network name, the protocol, the interface over which the network runs (eth:1 for LAN, atm:1 or hdlc:1 for WAN), how the network was created (static for LAN, dynamic for WAN) and the network address assigned to the connection. IP and IPX WAN network names incorporate the name of the remote site profile.

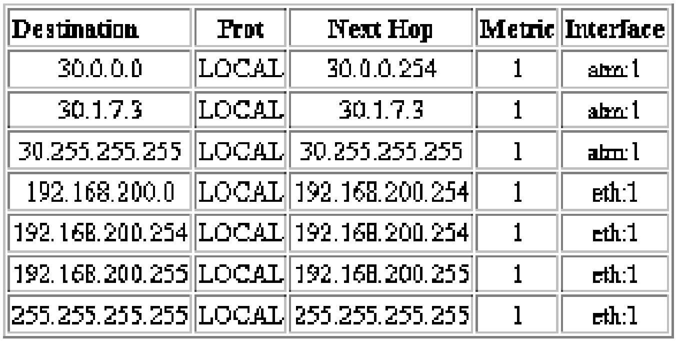
Below is an example of a network status table. IP Routing Table:



Name	Prot	Int	State	Type	Network Address
ip	IP	eth:1	ENABLED	STATIC	204.151.242.89/C
abc	IPX	eth:1	DISABLED	STATIC	240
lan-bridge	BRIDGE	eth:1	ENABLED	STATIC	2

The IP routing table contains the list of all IP routes known by the OfficeConnect Remote 840. To view the IP routing table, go to the OfficeConnect Remote 840 Manager home page and select **Monitor > Routes and Services > IP Routes**.

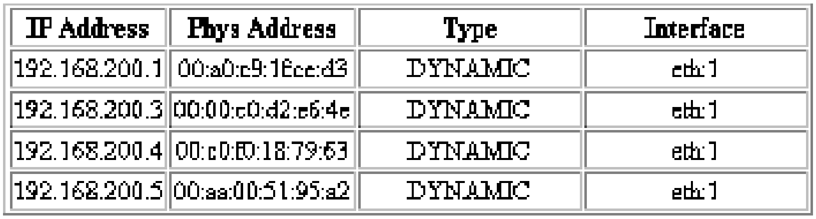
Routes that were put in the table when a network came up have the protocol type of LOCAL. STATIC routes are those that have been configured statically. The protocol type of RIP indicates routes that were learned from IP RIP information exchange with other routers. The interface indicates whether the network is accessible from the LAN (**eth:1**) or WAN (**atm:1 or hdlc:1**) interface.



Destination	Prot	Next Hop	Metric	Interface
30.0.0.0	LOCAL	30.0.0.254	1	atm:1
30.1.7.3	LOCAL	30.1.7.3	1	atm:1
30.255.255.255	LOCAL	30.255.255.255	1	atm:1
192.168.200.0	LOCAL	192.168.200.254	1	eth:1
192.168.200.254	LOCAL	192.168.200.254	1	eth:1
192.168.200.255	LOCAL	192.168.200.255	1	eth:1
255.255.255.255	LOCAL	255.255.255.255	1	eth:1

ARP Table

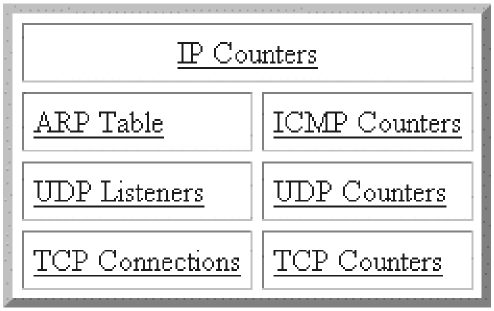
The Address Resolution Protocol (ARP) table displays the list of IP addresses and their associated hardware addresses that have been learned using ARP. The table is built dynamically. To view this table, go to the OfficeConnect Remote 840 Manager home page and select **Monitor > Networks > IP > ARP Table**.



IP Address	Phys Address	Type	Interface
192.168.200.1	00:a0:c9:1f:cc:d3	DYNAMIC	eth:1
192.168.200.3	00:00:c0:d2:e6:4e	DYNAMIC	eth:1
192.168.200.4	00:c0:f0:18:79:63	DYNAMIC	eth:1
192.168.200.5	00:aa:00:51:95:a2	DYNAMIC	eth:1

IP, TCP, UDP, ICMP Counters and Tables

The OfficeConnect Remote 840 Manager provides various counters and tables for the IP, TCP, UDP and ICMP protocols. To get to the counter and table screens, go to the OfficeConnect Remote 840 Manager home page and select **Monitor > Networks > IP**. Select the desired counters from the screen shown below:



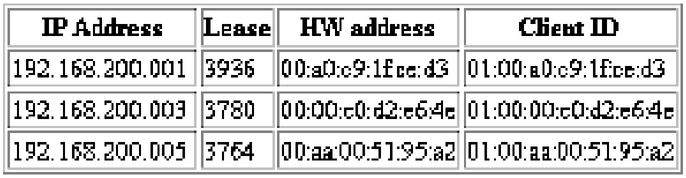
DHCP

DHCP Lease Table

Workstations on the LAN 'lease' IP addresses from the OfficeConnect Remote 840 when it is the DHCP Server.

You can view all of the currently outstanding leases by examining the DHCP Lease Table. From the OfficeConnect Remote 840 Manager home page select **Monitor > Networks > DHCP > DHCP Leases**.

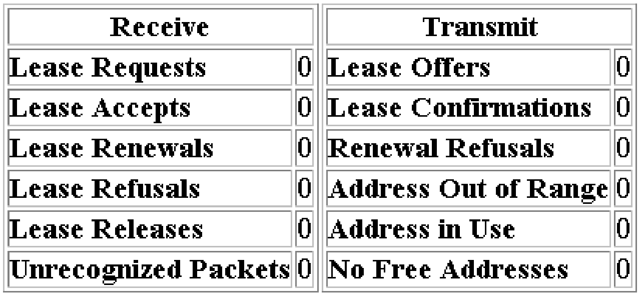
Each lease table entry lists the IP address and lease duration assigned to each client hardware (MAC) address.



IP Address	Lease	HW address	Client ID
192.168.200.001	3936	00:a0:c9:1f:ce:d3	01:00:a0:c9:1f:ce:d3
192.168.200.003	3780	00:00:c0:d2:e6:4e	01:00:00:c0:d2:e6:4e
192.168.200.005	3764	00:aa:00:51:95:a2	01:00:aa:00:51:95:a2

DHCP Counters

You can obtain detailed statistics and error counters for the DHCP protocol. Access this screen from the OfficeConnect Remote 840 Manager home page by selecting **Monitor > Networks > DHCP > DHCP Counters**.



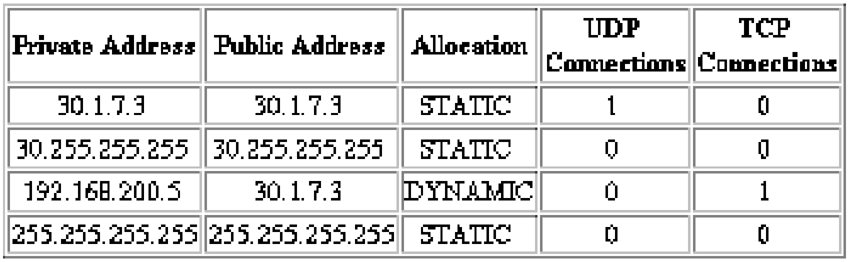
Receive		Transmit	
Lease Requests	0	Lease Offers	0
Lease Accepts	0	Lease Confirmations	0
Lease Renewals	0	Renewal Refusals	0
Lease Refusals	0	Address Out of Range	0
Lease Releases	0	Address in Use	0
Unrecognized Packets	0	No Free Addresses	0

Address Translation

Table of Mapped Addresses

You can view the dynamic Network Address Translation (NAT) and Port Address Translation (PAT) mapped address table. To access this table from the OfficeConnect Remote 840 Manager home page, select **Monitor > Networks > NAT/PAT**. Select the remote site profile whose address translations you want to look at, and then select **Mapped Addresses**.

This table is created when the OfficeConnect Remote 840 is configured to use address translation before routing IP packets to the remote location. The mapped addresses table keeps track of private-to-public address mappings.

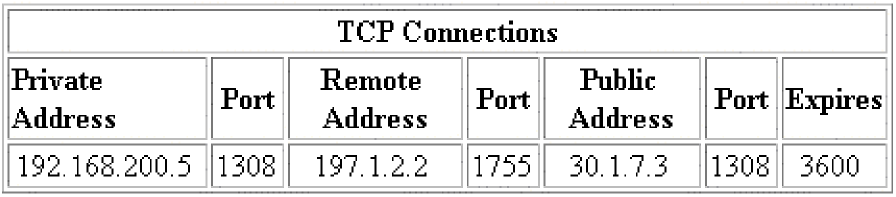


Private Address	Public Address	Allocation	UDP Connections	TCP Connections
30.1.7.3	30.1.7.3	STATIC	1	0
30.255.255.255	30.255.255.255	STATIC	0	0
192.168.200.5	30.1.7.3	DYNAMIC	0	1
255.255.255.255	255.255.255.255	STATIC	0	0

Table of Port Assignments

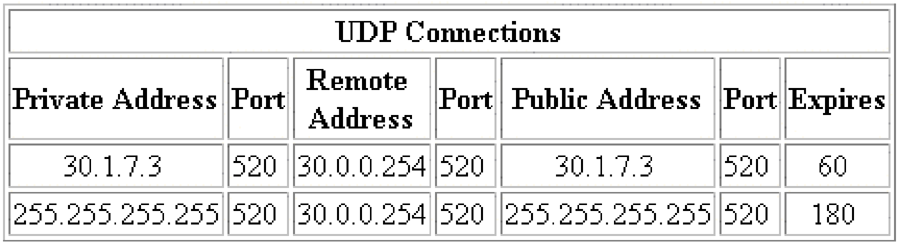
The OfficeConnect Remote 840 address translation process also creates a dynamic port assignment table when NAT or PAT is used. To access this table from the OfficeConnect Remote 840 Manager home page, select **Monitor > Networks > NAT/PAT**. Select the remote site profile whose address translations you want to look at, and then select **Port Assignments**.

This table is created when the OfficeConnect Remote 840 is configured to use address translation before routing IP packets to the remote location. The port address translation table keeps track of private-to-public address and port mappings and shows the length of time (seconds) before the translation expires.



TCP Connections

Private Address	Port	Remote Address	Port	Public Address	Port	Expires
192.168.200.5	1308	197.1.2.2	1755	30.1.7.3	1308	3600



UDP Connections

Private Address	Port	Remote Address	Port	Public Address	Port	Expires
30.1.7.3	520	30.0.0.254	520	30.1.7.3	520	60
255.255.255.255	520	30.0.0.254	520	255.255.255.255	520	180

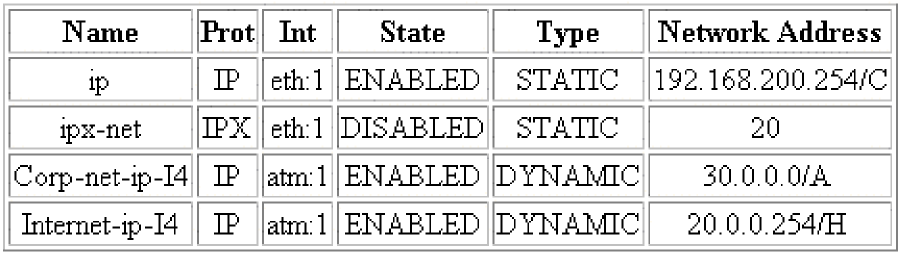
IPX

IPX Networks

IPX networks are created when you configure IPX over the LAN and when a remote site connection is established that is configured to route IPX traffic. To view the list of IPX networks and their status, bring up the **Network Status** screen. This screen list the status of all OfficeConnect Remote 840 IP, IPX, and Bridge networks. To see this screen, go to the OfficeConnect Remote 840 Manager home page and select **Monitor > Networks > Network Status**.

The network status table shows the network name, the protocol, the interface over which the network runs (eth:1 for LAN, atm:1 or hdlc:1 for WAN), how the network was created (static for LAN, dynamic for WAN) and the network address assigned to the connection. IP and IPX WAN network names incorporate the name of the remote site profile.

An example of the network status table is provided below.

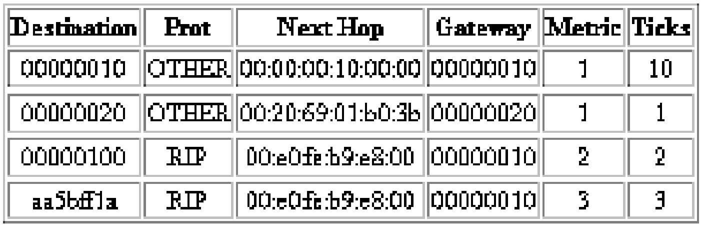


Name	Prot	Int	State	Type	Network Address
ip	IP	eth:1	ENABLED	STATIC	192.168.200.254/C
ipx-net	IPX	eth:1	DISABLED	STATIC	20
Corp-net-ip-I4	IP	atm:1	ENABLED	DYNAMIC	30.0.0.0/A
Internet-ip-I4	IP	atm:1	ENABLED	DYNAMIC	20.0.0.254/H

IPX Routes

The IPX routing table contains the list of all IPX routes known by the SDSL router. To view the IPX routing table, from the OfficeConnect Remote 840 Manager home page, select **Monitor > Routes and Services > IPX Routes**.

Routes that were put in the table when a network came up have the protocol type of OTHER. STATIC routes are those that have been configured statically. The protocol type of RIP indicates routes that were learned from IPX RIP information exchange with other routers.

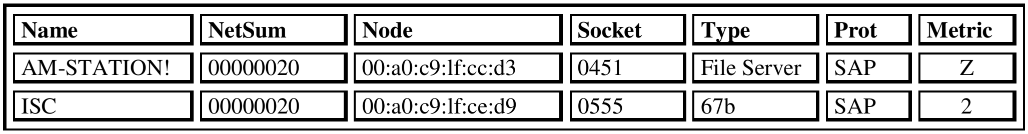


Destination	Prot	Next Hop	Gateway	Metric	Ticks
00000010	OTHER	00:00:00:10:00:00	00000010	1	10
00000020	OTHER	00:20:69:01:b0:3b	00000020	1	1
00000100	RIP	00:e0fe:b9:e8:00	00000010	2	2
aa5bff1a	RIP	00:e0fe:b9:e8:00	00000010	3	3

IPX Services

The IPX services table contains the list of all IPX servers known to the OfficeConnect Remote 840. To view the IPX services table, go to the OfficeConnect Remote 840 Manager home page and select **Monitor > Routes and Services > IPX Services**.

The services table contains statically configured services as well as those learned through SAP. If the server type is a well known type, it is displayed in text, otherwise its hex value is displayed.



Name	NetSum	Node	Socket	Type	Prot	Metric
AM-STATION!	00000020	00:a0:c9:lf:cc:d3	0451	File Server	SAP	Z
ISC	00000020	00:a0:c9:lf:ce:d9	0555	67b	SAP	2

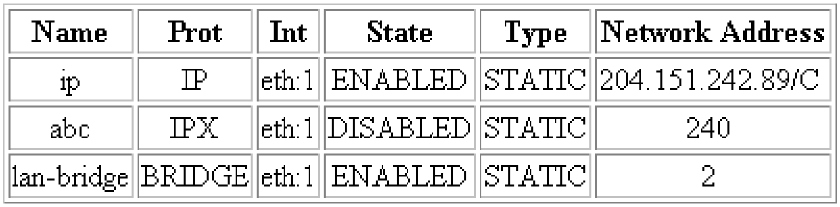
Bridge

Bridge Networks

Bridge networks are created when you configure bridging over the LAN and when a remote site connection is established that is configured to bridge traffic. To view the list of bridge networks and their status, bring up the **Network Status** screen. This screen lists the status of all OfficeConnect Remote 840 IP, IPX, and bridge networks. To see this screen, from the OfficeConnect Remote 840 Manager home page, select **Monitor > Networks > Network Status**.

The network status table shows the network name, the protocol, the interface over which the network runs (**eth:1** for LAN, **atm:1** or **hdlc:1** for WAN), how the network was created (static for LAN, dynamic for WAN) and the network address assigned to the connection.

The screen capture below provides an example of the network status table.

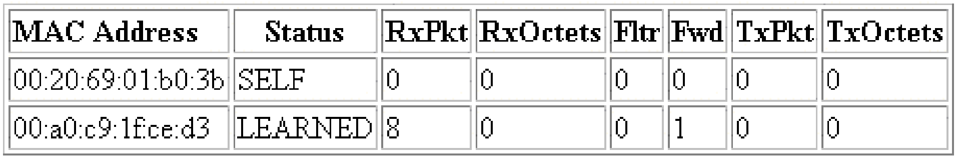


Name	Prot	Int	State	Type	Network Address
ip	IP	eth:1	ENABLED	STATIC	204.151.242.89/C
abc	IPX	eth:1	DISABLED	STATIC	240
lan-bridge	BRIDGE	eth:1	ENABLED	STATIC	2

Forwarding Table

The bridge forwarding table is used for forwarding packets and contains the list of learned media access control (MAC) addresses. To access this table, go to the OfficeConnect Remote 840 home page and select **Monitor > Routes and Services > Bridge Forwarding Table**.

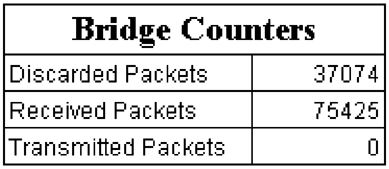
The table contains the learned MAC addresses and counters for data traffic that has been received, forwarded or not forwarded (filtered), and transmitted.



MAC Address	Status	RxPkt	RxOctets	Fltr	Fwd	TxPkt	TxOctets
00:20:69:01:b0:3b	SELF	0	0	0	0	0	0
00:a0:c9:1f:ce:d3	LEARNED	8	0	0	1	0	0

Bridge Counters

Bridge counters provide transmit and receive counts for the bridge process. To view the counters table, from the OfficeConnect Remote 840 home page, select **Monitor > Networks > Bridge**.



Bridge Counters	
Discarded Packets	37074
Received Packets	75425
Transmitted Packets	0

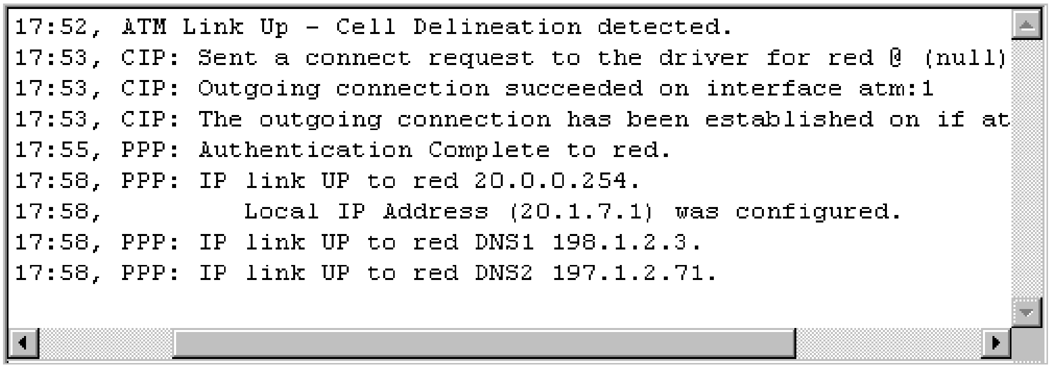
Events Logs

The Office Connect Remote 840 router maintains logs of certain events. These logs contains a running list of text messages generated during connection to the WAN or whenever a critical event happens.

Connection Event Log

The connection event log contains a text description of WAN interface events. This includes cell delineation detection as well as the progress of remote site connections. To access this log, from the OfficeConnect Remote 840 Manager home page, select **Monitor > Events > Connection Events**.

The following screen capture shows a successful connection to a remote site named red using PPP network service. Critical Events Log



```
17:52, ATM Link Up - Cell Delineation detected.
17:53, CIP: Sent a connect request to the driver for red @ (null)
17:53, CIP: Outgoing connection succeeded on interface atm:1
17:53, CIP: The outgoing connection has been established on if at
17:55, PPP: Authentication Complete to red.
17:58, PPP: IP link UP to red 20.0.0.254.
17:58,        Local IP Address (20.1.7.1) was configured.
17:58, PPP: IP link UP to red DNS1 198.1.2.3.
17:58, PPP: IP link UP to red DNS2 197.1.2.71.
```

Critical Events Log

The Critical Event Log contains a running list of text messages generated by the OfficeConnect Remote 840 when a critical event occurs. To access this log, from the OfficeConnect Remote 840 Manager home page, select **Monitor > Events > Critical Event Log**. Critical events are rare and may indicate an operational problem.

12 CONFIGURING FILTERS

Introduction

The OfficeConnect Remote 840 provides an extensive set of data filtering capabilities. For instance, filters can accept packets only from specific addresses to provide added security, or filters can be added to reduce network traffic and improve overall performance.

This chapter contains information on the filtering capabilities for your OfficeConnect Remote 840. It is divided into the following sections:

- "Filtering Overview"
- "Filtering Capabilities"
- "Creating Filters Overview"
- "Creating Filters Using the OfficeConnect Remote 840 Manager"
- "Step-by-Step Guide to Creating Filters Using the OfficeConnect Remote 840 Manager"

Filtering Overview

Filters can provide added security by accepting packets only from specific addresses or they can be added to reduce network traffic and improve overall performance.

Packet filters control inter-network data transmission by accepting or rejecting the passage of specific packets through network interfaces based on packet header information. When data packets are received by a network interface such as an Ethernet LAN or WAN port, a packet filter analyzes packet header information against a set of rules you define. A filter then lets the packet pass through or discards it.

Filtering Capabilities

The OfficeConnect Remote 840 provides an extensive set of data filtering capabilities. The OfficeConnect Remote 840 supports the following filtering capabilities:

- Input and output data filtering.
- Source and destination address filtering.
- Protocol filtering.
- Source and destination port filtering. A packet filter can control what services local or remote users can access.
- Route filtering can filter source and destination addresses in packets that exchange routing table information.
- Established session filtering. A packet filter can permit users to connect with a remote network without letting remote users have access to the local network (or vice versa).

Filter Classes

The OfficeConnect Remote 840 supports three filter classes:

- **Input data** — filter packets as they enter.
- **Output data** — filter packets as they exit.
- **Embedded bypass** — for periodic router protocol packets (IP RIP, IPX RIP and IPX SAP)

Each filter class can be identified further by the following types:

Filter Types

Filters can be classified by the following types:

- **Data filters** — based on protocol-specific packet information.
- **Advertisement filters** — based on broadcast packet information (IP RIP, IPX RIP, and IPX SAP).
- **Generic filters** — based on packet structure.

Data Filters

Data filters control network access based on the protocol, source / destination address, and port designation (e.g., TCP and UDP port designations) of the packet. The following table describes the data filters supported.

Table 12–1 Data Filters

Filter	Action
IP	Controls network access based on the protocol and source/destination address. IP filter rules allow filtering based on the source address, destination address, protocol type, source port, and port designation of the IP packet.
IPX	Controls network access based on the protocol and source/destination network. IPX filter rules allow filtering based on the source network, destination network, protocol type, source socket, destination socket, source node, and node designation of the IPX packet.
Bridge	Controls network access based on the source and destination MAC addresses.

Advertisement Filters

Advertisement filters operate on network protocol packets that contain varying information such as SAP or RIP. Filtering of these packets is performed by the specific protocol process. The following table describes the advertisement filters supported:

Table 12–2 Advertisement Filters

Filter	Action
IP-RIP	Controls the content of IP Routing Information Protocol (RIP) packets that are sent out or received on specific ports. The IP RIP filtering process filters addresses from the RIP packet upon transmission, and does not enter routes into the routing table upon receipt.
IPX-SAP	Controls the content of Service Advertising Protocol (SAP) packets that are sent out or received on specific ports. The IPX-SAP filter rules allow filtering on service type, server name, network address, node address, and socket number fields of the service entry. The forwarding process uses the filter information to prevent the service information from being included in the SAP packet.
IPX-RIP	Controls the content IPX RIP packets that are sent out or received on specific ports. The IPX RIP filtering process filters addresses from the RIP packet upon transmission, and does not enter routes into the routing table upon receipt.

Generic Filters

Generic filters are protocol-independent and are specified by byte and offset values in a packet. Packets are filtered by comparing each packet's offset value and byte information with the values that you define in the filter. The router will accept or reject the packet based on the result.

Creating generic filters can be a complex task. Only experienced users should employ generic filters, and strictly in cases where data and advertising filters cannot provide the filtering capabilities that you require.

Creating Filters Overview

Filters can be set one of two ways in the OfficeConnect Remote 840:

- Using Command Line Interface (CLI). (See **Appendix D** for instructions to access the CLI.)
- Using the OfficeConnect Remote 840 Manager.

The more flexible way of setting filters is through the Command Line Interface (CLI). Both data and advertisement filters can be set using CLI.

For more information on accessing CLI, refer to the *OfficeConnect Remote 840 SDSL Router CLI User's Guide*.

If you want to set up filters using the OfficeConnect Remote 840 Manager, go to the "Step-by-Step Guide to Creating Filters Using the OfficeConnect Remote 840 Manager"section.

Creating Filters Using the OfficeConnect Remote 840 Manager

The OfficeConnect Remote 840 Manager supports data filters only (not advertisement filters). Data filters are used to remove packets from the normal flow of data traffic. They can be applied to IP, IPX, and/or Bridge traffic.

Filters affect only those protocols which are currently active in the OfficeConnect Remote 840.

Therefore, if the unit is set up to Bridge only, only bridge filters have an effect on the data traffic; IP and IPX filters have no effect even if IP or IPX traffic is being bridged. Internally (for greater efficiency), filters are examined when a data packet is being processed by the protocol, not as the packet enters or exits the unit (even though when filters are set up, it looks like they take effect at the interface level). For example, when IPX traffic is bridged, it is processed by the bridge protocol in the unit, not by the IPX protocol. Therefore, a filter on IPX traffic would have to be a bridge filter in this example.

There are two sets of criteria used in determining whether a filter affects a packet.

The first is the direction/location of the packet. There are four static direction/locations on which filters can be activated: incoming LAN traffic, outgoing LAN traffic, incoming WAN traffic and outgoing WAN traffic. Additionally, there are two for each Remote Site, traffic coming from and going to each one.

The second criteria is whether the packet contains data that matches the condition(s) in the filter. Conditions are defined based on protocol specific information such as IP source address or IPX source socket number.

All filters are set up to discard packets (data filters). However, there are two ways of specifying these actions: a "negative" and a "positive" way. The negative action specifies that the packet or information is discarded if the filter criteria met. The positive action specifies that the packet or information is kept if the criteria is met. The positive way implies that all packets or information not meeting the criteria are discarded. Either method can be used for most filters. However, one or the other is almost always more logical.

For example, imagine a small office with 20 workstations on the LAN. The LAN is connected to a remote corporate office using an OfficeConnect Remote 840. Two of the LAN workstations are used by contractors who are not given access to the corporate office. To prevent traffic from the two workstations from passing through the OfficeConnect Remote 840, a filter is set up on the incoming/LAN direction/location. The most logical filter is a "negative" filter that says "discard packet if IP source address is equal to xxx.xxx.xxx.xxx or IP source address is equal to xxx.xxx.xxx.yyy". Of course you could write a "positive" filter which would say "forward packet if IP source address is equal to <list of the 18 IP addresses that are allowed to send traffic>". However, you can see that the negative filter is shorter (more efficient to apply) and easier to write and therefore the better one to use.

Each direction/location can have up to fifteen filters. Each filter can have up to six conditions. As you create the filter, you can select whether to logically "and" or "or" conditions together. If you need a filter with more than six conditions, you can create multiple filters that will be looked at by the OfficeConnect Remote 840 as if they were one filter. The only requirement is that the basic filter information (i.e., the protocol and the action) must be the same in each of the filters. The filters will be "or"ed together when they are merged internally.

Example: To prevent seven individual PCs on the LAN from accessing a remote site, create the following two filters:

Filter for Packets: Going to Remote Site Vienna
Filter Name: Block PCs 1-6 Protocol: IP Enabled: Yes
Discard Packet if IP Source Address is Equal to 192.168.200.41
or if IP Source Address is Equal to 192.168.200.50
or if IP Source Address is Equal to 192.168.200.66
or if IP Source Address is Equal to 192.168.200.42
or if IP Source Address is Equal to 192.168.200.88
or if IP Source Address is Equal to 192.168.200.90

Filter Name: Block PC 7 Protocol: IP Enabled: Yes
Discard Packet if IP Source Address is Equal to 192.168.200.102

The filters BLOCK PCs 1-6 and BLOCK PC 7 both use the IP protocol and the same action, "Discard Packet if..."

Therefore, when they are applied, they are "or"ed together. The resultant filtering is the same as you would get if you were allowed to create a single filter that contained all seven conditions.

OfficeConnect Remote 840 Manager Filter Screens

The OfficeConnect Remote 840 Manager (HTML) filter screens provide an easy to use menu system for specifying the direction/location of the traffic to be checked and for creating and editing filter conditions. The filter screens are set up to allow you to create sentences that describe the filter action. For example, a filter that prevents IPX packets from Jan and Bob's PCs from being sent to Remote Site Vienna would look something like this:

Filter for Packets: Going to Remote Site Vienna
Filter Name: Block Jan and Bob
Discard Packet if IPX Source Node is Equal to 00-20-69-00-23-99
or if IPX Source Node is Equal to 00-20-69-11-45-88

The sentence is built up over a number of screens. Most filters can be easily created by selecting from the provided condition sentences. Each sentence has pull down boxes for selecting condition keywords (IP Destination Address / IP Source Address, etc.) and condition operations (is Equal to / is Not Equal to, etc.) Where appropriate, the additional flexibility of generic filters is available. With generic filters, you specify an offset into the packet and the hex value to compare the packet content to. This allows you to go beyond the bounds of the “canned” condition sentences.

An overview and description of each filter screen is provided below:

You can get out of any screen by using the HTML side bar links. If you are in the process of creating a new filter when you do this, and haven't yet pressed the ***Save Filter*** *button on the* ***Filter Condition Summary*** *screen, the new filter information is lost.*

Filter Screens

- **Filter Index**

  Index screen that allows you to either view the Filter Status or Filter Create/ Modify screens.

- **Filter Status**

  Shows which direction/locations have filters.

- **Filter Create/Modify**

  Prompts you to select on which direction/location you are going to setup or change a filter. Pressing the “Next” button brings up the Filter Summary page.

- **Filter Summary**

  Shows you a summary of previously defined filters for this direction/location and whether or not the filters are active.

  Pressing the **Create** button brings up the **Filter Action** screen.

  Selecting a filter name and pressing the **Delete/Modify** button brings up the **Filter Delete/Modify** screen.

- **Filter Protocol**

  Prompts you to:

  - Provide a name for the filter (must be unique within this direction/location as well as across all direction/locations). The name may contain blanks but may not contain any of the following characters: # ; | [ ] { }
  - Supply a name that can be up to 32 characters long. It is useful to use the name field as a description field that summarizes the purpose of the filter.

  - Enable or disable the filter. (You may want to create a disabled filter, then enable it when you are satisfied that the filter conditions are complete.)
  - Select the protocol for the filter being added. The protocols are: Basic IP, Advanced IP, Basic IPX, Advanced IPX, Basic Bridge, and Advanced Bridge.
  - Pressing the **Next** button brings up the condition screen for the selected protocol.

- **Condition Screens**

  These screens have a common structure but differ in content. The common features include the condition number (1-6) of the condition being created and, for condition numbers 2-6, the selection via radio buttons for "And"ing and "Or"ing the condition to the previous condition.

  For condition number 1, the user is prompted to select the action of the filter: "Discard Packet" or "Forward Packet". Also common is the **Next** button, which takes you to the **Condition Summary** screen.

  Basic IP Condition has the following condition sentences to select from:

Table 12–3 Basic IP Condition

Destination Address	Is Equal to	______IP address
Source Address	Is Not Equal to	
Destination Network	Is Equal to	______IP address
Source Network	Is Not Equal to	______(Mask)

Advanced IP Condition has the following condition sentences to select from:

Table 12–4 Advanced IP Condition

	Destination Address	Is Equal to	____IP address
	Source Address	Is Not Equal to	
	Destination Network	Is Equal to	______IP address
	Source Network	Is Not Equal to	______(Mask)
Protocol Type		Is Equal to	TCP
		Is Not Equal to	UDP
			ICMP

TCP	Destination Port	is Equal to	______
	Source Port	is Not Equal to	(1 - 65536)
		is Greater Than	
		is Greater Than or Equal to	
		is Less Than	
		is Less Than or Equal to	
UDP	Destination Port	is Equal to	_____
	Source Port	is Not Equal to	(1 - 65536)
		is Greater Than	
		is Greater Than or Equal to	
		is Less Than	
		is Less Than or Equal to	
Generic Byte Filter	Origin: IP Header / IP Data		_____
	Offset _____ (0- 1514 bytes)		(hex value**)
	Length _____ (1-48 bytes)		
	Masked With ____ (0's or F's*)		
	is equal to		

Basic IPX Condition has the following condition sentences to select from:

Table 12–5 Basic IPX Condition

Destination Node	Is Equal to	______IPX network address (1-FFFF)
Source Node	Is Not Equal to	
Destination Network	Is Equal to	______IPX node [MAC] address:
Source Network	Is Not Equal to	xx-xx-xx-xx-xx-xx

Advanced IPX Condition has the following condition sentences to select from:

Table 12–6 Advanced IPX Condition

Destination Node	Is Equal to	______IP address
Source Node	Is Not Equal to	
Destination Network	Is Equal to	______IP address
Source Network	Is Not Equal to	______(Mask)

	Destination Socket	is Equal to	_____
	Source Socket	is Not Equal to	(1 - FFFF)
		is Greater Than	
		is Greater Than or Equal to	
		is Less Than	
		is Less Than or Equal to	
	Destination Port	is Equal to	_____
	Source Port	is Not Equal to	(1 - 65536)
		is Greater Than	
		is Greater Than or Equal to	
		is Less Than	
		is Less Than or Equal to	
Generic Byte Filter	Origin: IP Header / IP Data		_____
	Offset ____ (0- 1514 bytes)		(hex value**)
	Length ____ (1-48 bytes)		
	Masked With ___ (0's or F's*)		
	is equal to		

*whose length is 2x Length field: two mask numbers for each byte)
** whose length is not greater than 2x Length field.

- Condition Summary

  This screen shows the filter conditions that have been created so far. It allows you to select any undefined condition to add, or to select any defined condition to delete (You can not modify a condition - you must delete the condition then add a new one to make changes). You do not have to add filters in consecutive order (that is, you can skip condition numbers.) And you can delete conditions from the middle. The conditions are used in the filter in order of smallest condition number to greatest condition number and unused condition numbers are simply ignored.

  - The **Add** button returns you to the appropriate filter condition screen so you can define the next condition.
  - The **Delete** button returns you to this screen unless you have just deleted the last condition, in which case you go to the **Delete Filter/Add Condition** screen.
  - When you are finished defining conditions, press the **Save Filter** button. This completes the filter and takes you to the **Filter Summary** screen.

- Use the **Cancel** button to cancel any changes since the last time you saved.

When you have a filter that contains "And"ed and "Or"ed conditions together, the summary may display extra blank lines between conditions. This is to help you understand exactly what the filter means.

Look at this filter (without the extra separator):

Discard packet if IP Destination Address is Equal to 30.0.0.1
and IP Protocol is Equal to TCP
or IP Protocol is Equal to UDP.

This can be misinterpreted to mean:

– discard any TCP packet whose destination address is 30.0.0.1
– and
– discard any UDP packet whose destination address is 30.0.0.1.

Now look at the filter with the extra separator:

Discard packet if IP Destination Address is Equal to 30.0.0.1
and IP Protocol is Equal to TCP
or IP Protocol is Equal to UDP.

It clarifies the meaning as:
– discard any TCP packet whose destination address is 30.0.0.1
– and
– discard all UDP packets

- **Delete Filter /Add Condition**

  You get to this screen after deleting the last condition in a filter. You have the choice of deleting the filter or of adding a condition. To delete it, press the **Delete Filter** button (which takes you to the **Filter Summary** screen.) To add condition number 1, press the **Add Condition** button to bring up the appropriate condition screen (i.e. Basic IP, Advanced IP, etc.).

- **Filter Delete/Modify**

  You reach this screen from the **Filter Summary** screen if you wish to modify an existing filter. This screen allows you to change the filter name and it's enabled/disabled status. From this screen, select **Delete** to delete the displayed filter and return to the **Filter Summary** screen. Select **Modify** to save any changes you made on this screen to the Filter Name or Enabled/Disabled status. Or select the **Add/Delete Conditions** button to go to the **Condition Summary** screen, where you can add or delete conditions as needed.

Step-by-Step Guide to Creating Filters Using the OfficeConnect Remote 840 Manager

Filters can be tricky to define so spend time before accessing the screens thinking about what you want the filter to do.

First determine which direction and location of the data path you want to apply the filter to: for example, do you want to filter packets as they enter from the Ethernet ports, or as they go to all of the Remote Sites, or as they exit to go to a specific Remote Site?

Next, think about the desired results of the filtering, that is, which data packets are to be removed from the traffic (ex: if bridging, perhaps all IPX packets, or if routing IP, maybe all packets from a specific machine or group of machines.)

For more information on designing filters, see “Filtering Overview”.

1 Go to **Configuration > Global > Filters**. Select **Create/Modify Filters**. On the **Create/Modify** screen, select the direction/location of the data traffic where the filter will be activated. Press the **Next** button to bring up the **Filter Summary** screen for this direction/location.

2 On the **Filter Summary** screen, press the **Create** button to bring up the **Filter Action** screen.

3 On the **Filter Action** screen, enter a name for the filter and select the desired protocol. Then press the **Next** button to bring up the appropriate protocol condition screen.

4 On the protocol condition screen, select the action of the filter (discard or forward packet) and the first condition sentence for your filter.

5 Use the pull down boxes as needed to create your filter by selecting keywords (such as IP Destination Address / IP Source Address) and operations (is Equal to / is Not Equal to).

6 Then enter the value to be filtered against, that is, the IP address, Port number, etc. that finishes the condition information needed for the filter. Then press the **Next** button to see the **Condition Summary** screen.

From the **Condition Summary** screen, add more conditions as needed by selecting a condition number and pressing the **Add** button. This takes you back to the protocol condition screen.

This screen is the same as for the first condition except that now you can choose to logically “And” or “Or” this new condition to the previous condition.

As before, select the condition sentence, choose the keyword and operation and enter the filter value then press "Next" to see the Condition Summary screen again.

7 When you are satisfied that this filter is complete, press **Save Filter** on the **Condition Summary** screen. This causes the OfficeConnect Remote 840 to write the filter to file and activates the filter. You are returned to the **Filter Summary** screen. Now you can add another filter if you want.

Modifying an Existing Filter Using the OfficeConnect Remote 840 Manager

1 Go to **Configuration > Global > Filters**.

2 Select **Create/Modify Filters**. On the **Create/Modify** screen, select the direction/location of the data traffic where the filter is activate.

3 Press the **Next** button to bring up the **Filter Summary** screen for this direction/location.

4 To delete or modify the filter, select the filter from the pull down box and press **Delete/Modify**. This brings up the **Filter Delete/Modify** screen. You can delete the filter, modify the name, the enable/disable status and/or edit the conditions from this screen.

Turning a Filter Off Using the OfficeConnect Remote 840 Manager

1 Go to **Configuration > Global > Filters**.

2 Select **Create/Modify Filters**. On the **Create/Modify** screen, select the direction/location of the data traffic where the filter is active.

3 Press the **Next** button to bring up the **Filter Summary** screen for this direction/location.

4 To turn off an individual filter, select that filter in the pull down box and press the **Delete/Modify** button. On the **Filter Modify** screen, disable the filter by unchecking the **Enable Filter** checkbox and pressing **Modify**. Return to the summary screen by pressing **< Prev**.

13 TROUBLESHOOTING

Introduction

This chapter contains information on the troubleshooting tools and the troubleshooting areas for your OfficeConnect Remote 840. It is divided into the following sections:

- "Troubleshooting Tools"
- "LAN Connection Problems"
- "LAN Connection Problems"
- "IP Wizard and Web Browser Problems"
- "WAN Connection Problems"
- "General Network Connection Problems"
- "IP Network Connection Problems"
- "IPX Network Connection Problems"
- "Bridge Connection Problems"

Troubleshooting Tools

The OfficeConnect Remote 840 has a number of features which can be used to help troubleshoot problems. They are especially useful if the OfficeConnect Remote 840 is not visible during the troubleshooting session.

- OfficeConnect Remote 840 Manager's Configuration Audit (**Home > Tools > Configuration Audit**) — The audit provides information about real and potential problems in the OfficeConnect Remote 840's current configuration. You are advised to run the audit after each configuration change.
- OfficeConnect Remote 840 Manager's Monitor Features (**Home > Monitor**) — This provides many windows into the current state of the OfficeConnect Remote 840. Refer to "Monitoring the OfficeConnect Remote 840".

- CLI Traces — Tracing can be turned on for various OfficeConnect Remote 840 software components using the CLI *set facility* command. This feature is for advanced troubleshooting and should only be used after all other methods for isolating the problem have been tried. You may find the trace statements to be cryptic.

CLI traces are not accessible through the OfficeConnect Remote 840 Manager. Refer to the *OfficeConnect Remote 840 SDSL Router CLI User's Guide* for more information.

Troubleshooting Tables

The troubleshooting tables are organized in a "bottom-up" fashion. The hardware and line problems are listed first, then the higher level router configuration problems are covered.

How to Use these Tables

If you are having any type of connection problem, e.g., the workstations on the local LAN cannot connect to the remote network, you should work your way down the tables to eliminate any low-level problem before working through the WAN connection problems.

LAN Connection Problems

Symptom	Possible Causes	Corrective Action
The LAN LED is **Off**. The OfficeConnect Remote 840 Manager Interface status indicates Ethernet interface is down.	The LAN cable is not connected.	Check that one end of the LAN cable is fully plugged into the LAN port. Check that the other end is fully plugged into the local LAN connection.
	The LAN cable has been damaged.	Replace the cable with another LAN cable.
	The MDI/X switch on the back of the unit is set for connecting Port 1 to a single workstation but the cable is connected to a hub (or vice versa).	Press the switch in to connect to a hub and out to connect to a workstation.

IP Wizard and Web Browser Problems

Symptom	Possible Causes	Corrective Action
The IP Wizard does not find the OfficeConnect Remove 840 on the local LAN.	There is a LAN connection problem.	See "LAN Connection Problems".
	The OfficeConnect Remove 840 already has an IP address.	Only unconfigured OfficeConnect Remote 840s are detected using the IP Wizard. If your OfficeConnect Remote 840 has a LAN IP address already assigned, it will not appear in the IP Wizard list.

Symptom	Possible Causes	Corrective Action
	The workstation does not have an IP address.	If the workstation is supposed to learn its address from the OfficeConnect Remote 840, check that the unit is set up in DHCP Smart Mode. If not, set to DHCP Smart Mode and reset. If the workstation was booted before the OfficeConnect Remote 840, reboot the workstation now. If the workstation is supposed to have a specified address, configure the workstation and run IP Wizard again.
Your Web browser does not find the OfficeConnect Remote 840 using its LAN IP address.	There is a LAN connection problem.	See “LAN Connection Problems”.
	The OfficeConnect Remote 840 and the workstation are attached to the same LAN, but not assigned IP addresses from the same subnetwork.	Either: **1** Set up a workstation to be on the same IP subnet as the OfficeConnect Remote 840. Then connect and use the OfficeConnect Remote 840 Manager. **2** Use CLI to add an IP network over the Ethernet interface using an IP address from the same subnet as the workstation. Then connect and use the OfficeConnect Remote 840 Manager. **3** Use the factory reset button on the back of the 840 to delete the configuration. For an unconfigured unit, use the IP Wizard to reassign a new IP address. For a unit using DHCP Smart Mode, connect using the IP Address 192.168.200.254.
	The OfficeConnect Remote 840 address was entered incorrectly when the IP Wizard was used.	Use the factory reset button on the back of the 840 to delete the configuration. for an unconfigured unit, use the IP Wizard to reassign a new IP address. For a unit using DHCP Smart Mode, connect using the IP Address 192.168.200.254.

Symptom	**Possible Causes**	**Corrective Action**
The Web browser does not find the OfficeConnect Remote 840 using its DNS name (DHCP Smart Mode in use).	There is a problem with the LAN connection.	See "LAN Connection Problems".
	The workstation is on a different IP subnet from the 840's subnet.	Set the workstation IP configuration to automatically learn its IP address from the 840.
	The DNS host configuration has been changed.	Connect to the OfficeConnect Remote 840 using the unit's IP address, 192.168.200.254 and correct the DNS information.
	DHCP Smart Mode is not really in use.	Press the reset button on the back of the 840 while rebooting to delete the current configuration and select DHCP Smart Mode.
Unable to log in to the OfficeConnect Remote 840.	You did not enter a valid administration login name and password.	Use the system default login name **root** and password **!root**.
	The unit has no login name or password defined.	Do one of the following: **1** Use CLI to add an administration login profile. **2** Restore the system default login by deleting the current configuration using the reset button on the back of the unit. If DHCP Smart Mode is used, the default name **root** and password **!root** are set for you. If resetting to Unconfigured Mode, run the IP Wizard to assign an IP address and configure the default login name and password.

WAN Connection Problems

Symptom	Possible Causes	Corrective Action
SDSL LED is **Off**. OfficeConnect Remote 840 Manager Interface Status indicates that interface atm:1/hdlc:1 is down.	WAN (modem) cable is not connected.	Check that one end of the WAN cable is fully plugged into the wall. Check that the other end is fully plugged into the SDSL port in the back of the OfficeConnect Remote 840.
	WAN cable has been damaged.	Replace the cable with another DSL cable.
	There is a problem at the other end of the SDSL connection that causes the SDSL negotiation to fail.	Contact your service provider.
SDSL LED is **Off** or goes **On** briefly then turns **Off**.	SDSL link is down.	Contact your service provider.
OfficeConnect Remote 840 Manager ATM status cell delineation fails and no idle cells are being received.	SDSL link is down.	Contact your service provider.
	There is a problem at the central office equipment (the other end of the SDSL line) such that no idle cells are being transmitted or there is a corrupt line.	Report the problem to your service provider.

General Network Connection Problems

Symptom	Possible Cause	Correction Action
Remote network is not responding (e.g. to PINGs or the Web browser connection requests.)	LAN or WAN connection problem.	**1** See "LAN Connection Problems" and "WAN Connection Problems". **2** Go to Monitor > Networks > Network Status to view more detailed problem, then take corrective action.
	Incorrect Virtual Circuit (VC) information has been entered. Use the Monitor > ATM screen to observe ATM error counts. If the BadVPI or VDI error count is incrementing, the problem may be an incorrect VC identifier.	Check the VC information and correct as needed.
	Network Service (RFC 1483 or PPP) on OfficeConnect Remote 840 is incompatible with that used on remote site ATM router.	RFC 1483 and PPP network service run above ATM. If you select PPP and RFC 1483 is running on the remote site router, you will not be able to successfully access the remote network. Change the network service to agree with the remote router network service.
	The remote site profile may not be enabled. Check the Monitor> Remote Sites > Remote Sites Configured to see if the remote site status is ENABLED.	Enable the remote site profile.

Symptom	Possible Cause	Correction Action
	If your Network Service is PPP, the PPP Authentication information may be incorrect. Check connection event log (Monitor > Events > Connection Event Log) to see if the PPP connection could not be established due to a PAP or CHAP mismatch.	Enter the appropriate PPP Username and Password in the remote site profile.
Remote network is not responding (e.g. to PINGs or the Web browser connection requests.)	Remote location may be off-line.	The machine you are trying to connect to may not be running or may be busy processing other requests. Try reaching another remote machine.
The remote network is responding intermittently or not at all. Monitor > ATM shows ATM cell delineation successful but Hec sound is high.	There is a corrupt line causing the ATM data cells to fail the header error test.	Contact the service provider for verification. A lower speed connection may solve the problem.
The remote network is responding intermittently or not at all. ATM cell delineation achieved but Monitor > Remote Sites > Remote Site Counters shows that many packets are being received with Bad CRC.	ATM cells are being dropped by a device in the path to the remote site.	Contact your service provider.

Symptom	Possible Cause	Correction Action
Accessing remote information is slower than expected.	The SDSL settings indicate that a slower baud rate than expected was negotiated for the downstream traffic.	Reset the SDSL link to cause re-negotiation through one of the following steps: ■ If the OfficeConnect Remote 840 is accessible, disconnect the SDSL line for a few seconds. ■ Save the current configuration and reboot. If a faster connection was not negotiated, contact your service provider. They may able to check the physical connection for excess noise which may be the reason the negotiated numbers are low.

IP Network Connection Problems

Symptom	Possible Cause	Corrective Action
Remote IP network is not responding (ex., to PINGs or the web browser connection requests).	LAN or WAN connection problem.	See "LAN Connection Problems", "WAN Connection Problems", and "General Network Connection Problems".
	IP Forwarding is turned off.	From the OfficeConnect Remote 840 Manager home page, access the Global > IP > IP Settings screen. Ensure that IP Forwarding is enabled.
	PC or workstation does not have the OfficeConnect Remote 840 listed as a gateway.	Reconfigure the PC or workstation to use the OfficeConnect Remote 840's IP LAN address as its gateway.

Symptom	Possible Cause	Corrective Action
	Some remote sites use the RIP protocol to advertise your IP address to other routers. It may take more than 30 seconds for the IP route to the OfficeConnect Remote 840 to be propagated throughout the remote network.	Wait 30 seconds and try to access remote site again.
	IP routing table does not show a route to the remote network, indicating a configuration problem.	One of the following may solve the problem: Remote WAN IP addresses are entered incorrectly. Check the addresses and reconfigure as needed. RIP may be turned off. Set RIP to Listen mode to automatically learn routes to remote networks. A static route (global config.) or framed route (remote site config.) is needed to reach the remote network. Add the route and check the IP routing table to confirm the entry. No default gateway has been configured that would allow the OfficeConnect Remote 840 to automatically look for the remote network. Enable the default IP gateway option in the remote site profile.

Symptom	Possible Cause	Corrective Action
My video application does not run when Port Address Translation (PAT) is enabled.	Some video applications using UDP streaming have two connections, a TCP connection for control and a UDP stream for data. The TCP connection is initiated from the privately addressed workstation but the video stream may be initiated from the remote server. Because a mapping does not already exist for the UDP data stream, the data can not be mapped to a private address unless a static PAT port has been defined or the PAT default address is configured.	First verify the possible cause stated above is actually the problem. Set the Remote Site's PAT default address to your workstation's LAN address, then try to run your video application again. If it works, check to see if your video application allows you to specify a static UDP port. Microsoft NetShow allows you to configure a static UDP port in the Properties > Advanced screen. After setting a static port for the video application, you must add a corresponding static port entry on the OfficeConnect Remote 840. Set your Remote Site default PAT address to 0.0.0.0 before you try the static port. If you cannot setup a static port on the Video application, check to see if the Video application allows you to specify TCP rather than UDP. TCP streams are typically initiated from the private side. If you still are unsuccessful, the video application may be embedding address and port information within the data portion of the frame. If this is the case, consult your application vendor for possible workarounds.

IPX Network Connection Problems

Symptom	Possible Cause	Corrective Action
Remote IPX network is not responding (ex., can't find a Novell server).	LAN or WAN connection problem, or a general configuration problem.	See "LAN Connection Problems", "WAN Connection Problems", and "General Network Connection Problems".
	IPX is not enabled over both the LAN and the WAN.	Check the Local Site > IPX and Remote Site > IPX screens and ensure that IPX is enabled on both interfaces.
	IPX routing table does not show a route to the remote network, indicating a configuration problem.	One of the following may solve the problem: Remote WAN IPX addresses are entered incorrectly. Check the addresses and reconfigure as needed. RIP may be turned off. Set RIP to Listen mode to automatically learn routes to remote networks. A static route (global config.) or framed route (remote site config.) is needed to reach the remote network. Add the route and check the IPX routing table to confirm the entry.

Bridge Connection Problems

Symptom	Possible Cause	Corrective Action
Remote network is not responding.	LAN or WAN connection problem, or a general configuration problem.	See "LAN Connection Problems", "WAN Connection Problems", and "General Network Connection Problems".
	Bridging is not enabled over both the LAN and the WAN.	Check the Local Site > Bridge and Remote Site > Modify screens and ensure that bridging is turned on over both interfaces and that the remote site is enabled.
	The IP network is not responding because the OfficeConnect Remote 840 is trying to route IP packets, instead of bridging them.	Check the Global > IP > IP Settings screen and ensure that IP Forwarding is disabled.
	The IP network is not responding because the LAN IP addresses are assigned on a different network than the remote address.	When bridging IP, the local network becomes part of the remote network and must be assigned addresses on the same network or sub-net.

A

BRIDGING AND ROUTING

Introduction

During the initial configuration of the OfficeConnect Remote 840, you must decide whether to configure the unit as a bridge or as a router. If you are unsure which option you should choose, this section will help you decide.

Bridges and routers are used to connect networks together. The cost of connecting networks together is generally proportional to the distance over which the network extends and the amount of bandwidth required. Large amounts of bandwidth can be provided easily within a LAN by connecting different segments together with a local bridge. However, it becomes impractical and expensive to extend this bandwidth over larger distances, and it is, therefore, usual to interconnect local high-speed networks using bridges or routers connecting over slower speed terrestrial and satellite links.

In the following sections we describe the concepts behind bridging and routing, and discuss the different ways in which LANs can be configured and operated to optimize performance and minimize disruption of traffic on each individual LAN.

Bridging and Routing Concepts

A bridge connects one or more LANs together. It examines each data frame received at a LAN port and forwards any frames that it assumes are for a destination device not connected to that LAN port. The bridge is able to do this by learning which devices are connected to each LAN port.

A router learns much more about the networks connected to it and is able to be much more selective about the data it passes on to other networks and to which network it transmits. By default routers reject or filter data unless it matches predefined attributes (for example, specific protocols or destination network addresses). In large interconnected networks, a router selects the best route for data to travel.

Guidelines for Choosing Bridging or Routing

The list below outlines some of the reasons you might choose to configure the OfficeConnect Remote 840 as a bridge or a router. Read through the rest of this section for more explanation and to help decide which of the above conditions apply to your network.

- A bridge is simpler to configure, but a router can provide more security on a busy network and filter unwanted data transmissions more effectively.
- If your network consists of only one or two links between different sites and is not heavily loaded, in most circumstances you can configure your OfficeConnect Remote 840 units as bridges.
- If your network structure is complicated and consists of a mixture of leased-line and modem links, or if it uses several different protocols, you may obtain better performance from the OfficeConnect Remote 840 units if you configure them as routers.
- If you are connecting to a routed corporate network that is already routing the IP protocol, or if you are using the OfficeConnect Remote 840 to connect to the Internet, you must configure the unit as a router.
- If you want to link networks that the OfficeConnect Remote 840 is not routing, you must configure bridging. The OfficeConnect Remote 840 may serve as an IP router and a bridge simultaneously.

How Bridges Learn

When a bridge is first powered on, it does not know the number or the locations of stations that are connected to the LAN. To minimize the amount of data passed over the bridge, it must learn the whereabouts (address) of stations to ensure that it passes only the data that is necessary to be passed over the bridge.

Like the envelope of a letter, the header of each frame of data transmitted on the network has a From (source) address and a To (destination) address. This ensures that data reaches its destination on the LAN and that the receiving station can reply. The bridge reads every frame of data received at the LAN port and extracts the source address of the frame. From this information it builds an address table of stations it knows to be on the LAN.

To decide if data should be passed over the bridge, the bridge examines the destination address of the frame. If the address is already in its address table, the bridge knows the destination is on the LAN and therefore discards or filters the frame.

If the destination address is not in the address table, the bridge transmits the data across the bridge. It does this even if the destination device is on the local LAN because it does not recognize the destination station as local. However, if the destination device is on the local LAN, once it replies to the original source station, its own source address is part of the data frame and it is learned by the bridge and added to the address table.

By operating in this way, the amount of data forwarded by the bridge is kept to a minimum. Traffic that is for devices on the attached LAN is rarely forwarded over the bridge.

A bridge can be configured to forget or age a station's address after a period of inactivity, a facility that is used to ensure that stations that are no longer attached to the LAN, do not remain in the bridge's address table, using up space that may be required for other station's addresses.

Some bridges allow address information to be manually configured into the bridge, provided the automatic learning facility is turned off. This will not normally prove necessary unless specific traffic filtering is required.

You can also configure a number of other features to improve the performance and operation of the OfficeConnect Remote 840. These include sophisticated filtering techniques so that only certain types of frames, or those associated with particular work groups, are passed between specific segments.

Bridging Between Remote Sites

The OfficeConnect Remote 840 is able to send frames between LANs that may be separated by considerable physical distances. It achieves this by making use WAN links. WANs can be established by using either digital leased lines, ISDN lines, or analog (modem) lines and are usually operated by telephone companies or other service providers.

Figure A-1 shows two LAN segments, A and B, which are connected by a pair of OfficeConnect Remote 840 units, 1 and 2. The type of link between the two depends on the WAN services available at each of the remote bridge locations, and the price the network administrator is willing to pay for those services.

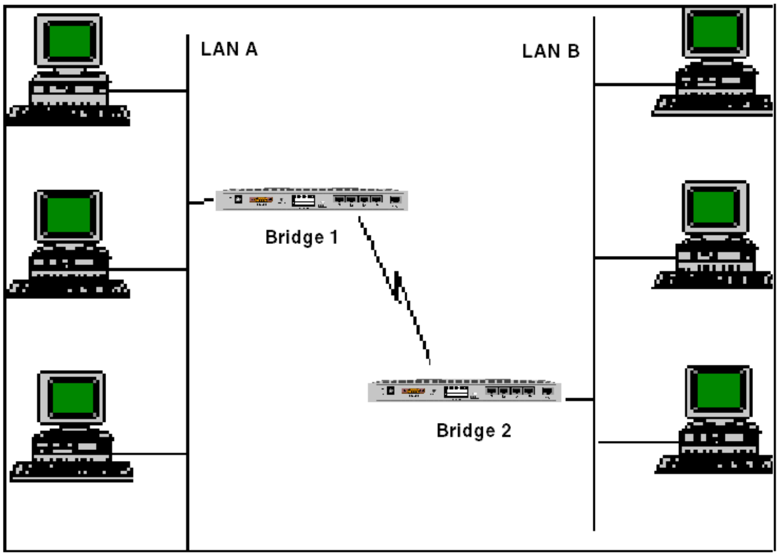


Figure A–1 Simple Remote Bridging

The OfficeConnect Remote 840 uses RFC 1483 or PPP encapsulation to connect with other OfficeConnect Remote 840 or third party devices.

Building a Larger Network

Large networks of interconnected LANs can be established by using multiple bridges as illustrated in Figure A-2.

The bridges build up their address tables. In Figure A-2, Bridge 1 examines packets from its WAN ports. If the destination unit is not registered as being accessed via the bridge's LAN interface, the frame will not be placed on LAN A. Therefore, frames passing between LAN B and LANs C or D will not impact the overall performance of the LAN.

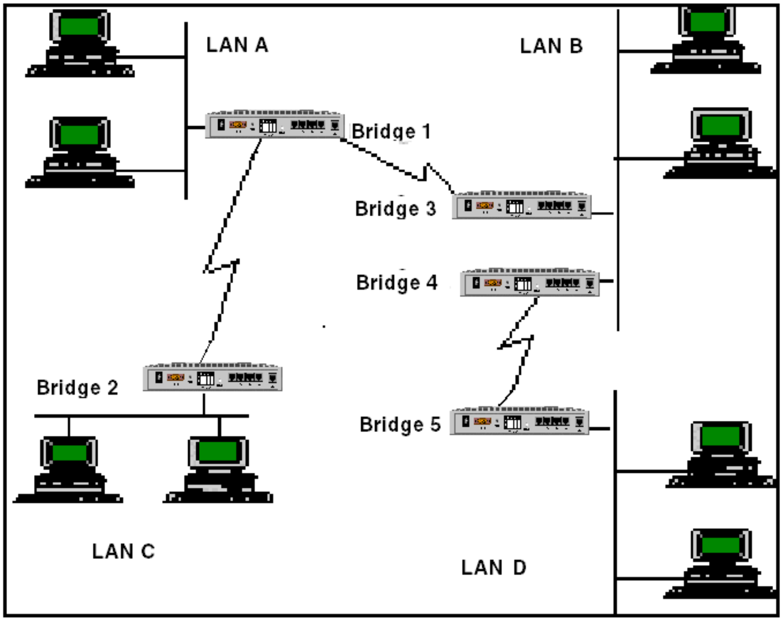


Figure A–2 Multiple Remote Bridge

Multiple Paths Between Bridge LANs

With only a single physical path between LANs, the network is susceptible to link and bridge failures. In the event of a failure, the connection between any of the LANs upstream or downstream from the point of failure will be broken. A more resilient network of interconnected LANs can be established by providing more than one link between any two of the LANs.

Normally, this network would soon encounter serious problems resulting from a loop, around which frames could endlessly travel if precautions aren't taken by the bridges. To prevent loops, you can enable the Spanning Tree Protocol (STP).

When STP is enabled, the bridges send out frames to inquire if there are other bridges on the network. By exchanging information, the bridges block ports that cause the loops and ensure that there is only ever one active path through the network. If one of the links or bridges fail, the other bridges detect this and reconfigure their ports so that there is once again an active data path through the network.

Network Topology

If your network topology is star shaped, a combination of analog modems and bridging is usually the most efficient and successful option. Routing is a better solution if your network is a complex mix of WAN interconnects and/or multiple protocols.

Broadcast Storms

Bridges are programmed to forward data packets automatically by default while routers filter data packets by default. These attributes have an impact on the overall flow of data across the network. Much has been made of broadcast storms in connection with bridged networks, where the broadcast signals from bridges propagate to fill all of the wide area bandwidth, and bring the network down. Broadcast storms cannot be attributed to installation of bridges or routers, but by poor protocol implementation and network design. However the deployment of routers can effectively firewall one logical network from another.

Optimum Use of Resource

Bridged networks use Spanning Tree Protocol (STP) to provide network resilience, by retaining redundant links on standby, in case the primary link fails. This means that you are not making maximum use of available resources.

Routing protocols make each node aware of the primary and alternate routes available, ensuring that resources (particularly WAN links) are not wasted.

Routers have been designed to provide the optimum route through the network from the workstation through to the destination resource with which the user wishes to communicate. In a very large network there could be multiple paths available, and these could change as links go in or out of service. These changes in network topology are handled by routing protocols.

Network Organization, Structure, and Physical Layout

Some organizations are structured into departments determined by the physical layout of their work environment, so it is natural to divide the corporate network into separate logical networks. Routing becomes the obvious candidate for handling these individual LANs.

The Internet

The protocol adopted by the Defense Data Network (DDN) for the Internet, is based on obtaining and abiding by, a registered Internet address range. This makes a router the ideal choice for accessing the Internet. Unfortunately, new applicants are only likely to get a Class C registered Internet address, preventing more than 254 connections on one bridged IP LAN.

Routing IP

Running a bridged network allows workstations to communicate directly between one another. A PC user wishing to communicate with a remote network server is totally unaware of any intervening bridges. This is known as transparent operation.

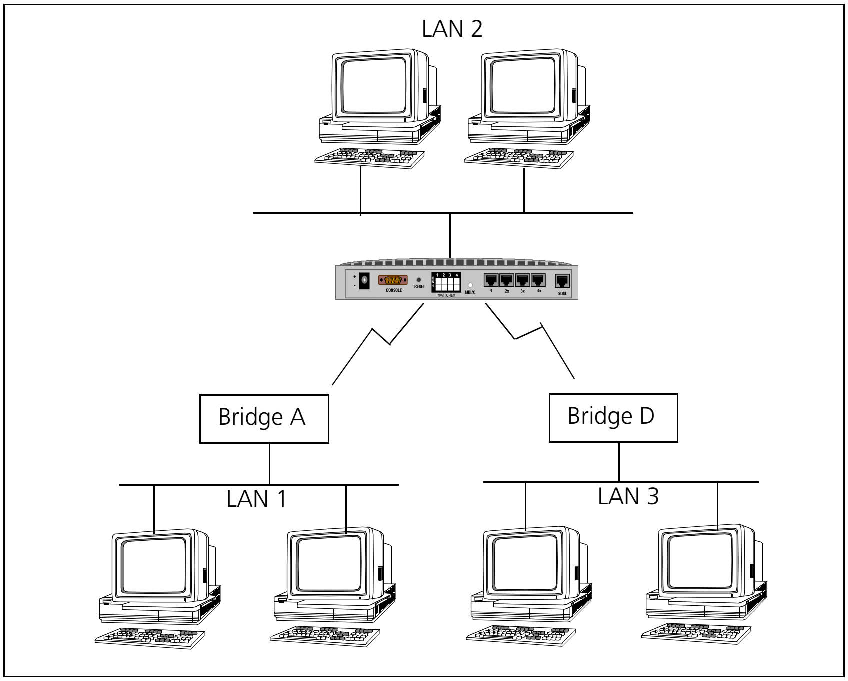


Figure A–3 Example Network

It is important to understand that in a bridged network the addressing structure for IP relates to a single network. If the units above were bridges and not routers, then an IP node on LAN A could, for example, have an address 140.56.10.1, the node on LAN B an address of 140.56.10.2, and the node on LAN C, an address of 140.56.10.3. All the nodes, therefore, are able to share the same Class B network address, regardless of their location on the bridged network.

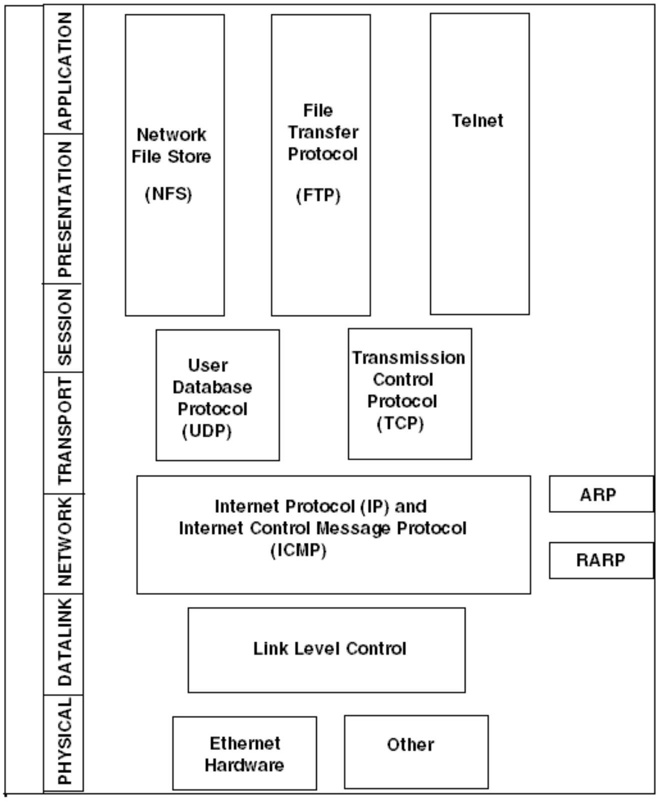

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATALINK
PHYSICAL
Network File Store (NFS)
File Transfer Protocol (FTP)
Telnet
User Database Protocol (UDP)
Transmission Control Protocol (TCP)
Internet Protocol (IP) and Internet Control Message Protocol (ICMP)
ARP
RARP
Link Level Control
Ethernet Hardware
Other

Figure A–4 Open Systems Interconnection Network Layer Model

Open Systems Interconnection Network Layer Model

A routing environment allows stations to communicate indirectly. Following the example in under “Routing IP”, let us assume that a station on LAN 1 wants to communicate with a network server on LAN 2. The station on LAN 1, constructs a Layer 2 datalink header (see Figure directly above), with the source station's hardware address, and also the destination hardware address of the local router. To direct the packet to its final network destination, the source station must complete the Layer 3 network header with the destination network address of LAN 2.

Once the packet is received by the Router A, attached to LAN 1, it strips off the network header (refer to Figure above) and examines the Layer 3 header information. It then reviews its routing tables in order to establish where to forward the data packet. It is possible that the LAN 1 router has multiple outgoing ports that would allow different transmission routes to the destination network. In our example using Figure A-3, a packet could go via Router D to get to Router B, or it could go more directly across a single direct link between Router A and Router B.

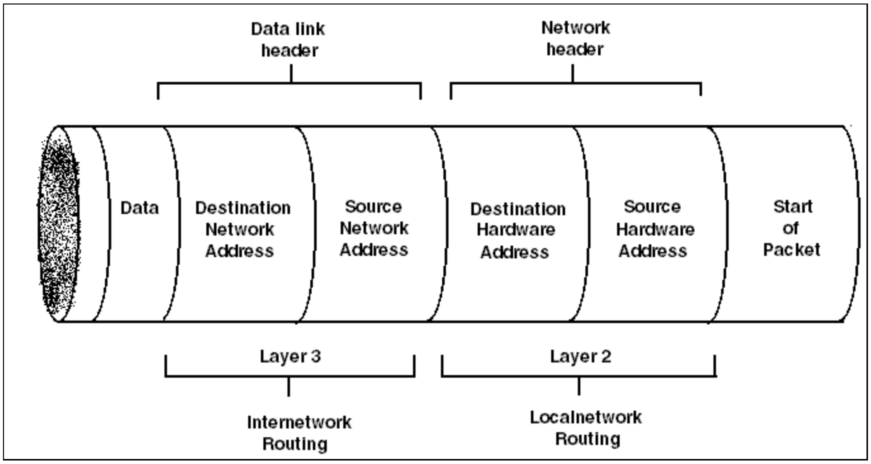


Figure A–5 Data Packet Containing Hardware and Software Addresses

IP Routing

The local router contains, within its routing table, information that will allow it to determine the best data transmission route. The type of information the router uses to make these assessments is protocol-dependent, and some communications protocols may employ a range of routing algorithms, and accompanying routing protocols. In the case of the TCP/IP protocol suite, the OfficeConnect Remote 840 utilizes RIP. RIP is also known as a distance vector protocol.

Different protocols use different networking characteristics or metrics when making routing decisions. The metric employed by RIP is a hop count. A hop count is defined by the number of routing nodes there are between the source and destination units. In our example, there are two hops between LAN 1 and LAN 2 going via Routers A and B. If traffic was directed via Routers A,D, and then B, this would be three hops.

The algorithm will automatically select to forward the data packet via Router A, as this route contains the least number of hop counts which makes it the preferred direct route.

Every thirty seconds (by default), each IP router will advertise, via RIP datagrams, to all other routers on the Internetwork, how many hops it takes to reach all connected logical networks, based on the routers network position and the state of its physical links.

It is also possible to assign what are known as static routes, which are manually entered fixed routes. The network manager may be aware of specific traffic patterns, or need to enforce a particular routing policy. Static routes provide an option to force traffic through the network in a particular way. The disadvantage with this approach is that routing protocols dynamically update all the routers on the network with the current network topology, enabling backup routes to be deployed. In a static route situation, if the WAN links in that routing definition are down, then traffic cannot be passed. Implementing a static route prohibits the router from being able to offer alternative data paths.

B IP ADDRESSING

Introduction to IP Addressing

This section contains a brief introduction to the IP addressing scheme for administrators that are new to the IP protocol.

IP Addressing Basics

IP addresses are 32 bits long and generally written in what is called dotted decimal notation: four decimal values separated by periods. For example: 192.77.203.5.

Address Classes

In IP, the same 32 bits can be divided in a number of different ways to indicate networks and sub-networks of different sizes. The IP Network is identified by the number of bits in the network mask. The node addresses are not physical addresses of your network interface cards, but arbitrary numbers that are mapped to those physical addresses later. This allows you to accommodate varying network structures from a small number of network segments with huge numbers of nodes to large numbers of networks with only a few nodes.

Subnetting

A large IP network can be subdivided into smaller subnetworks. This is done using a subnet mask (in this text, often called netmask), which tells a routing device how to further subdivide the Host ID portion of an IP address.

A subnet mask is a 32-bit value which also can be written in dotted decimal notation. It contains a number of bits set to 1 (indicating the network portion of an address) followed by a number of bits set to 0 (indicating the host portion of an address).

For example, a netmask of 255.255.255.0 on a Class B network would indicate that the network is divided into 254 sub-networks of 254 nodes each (0 and 255 are reserved numbers). For example, 128.5.63.28 would be host 28 on subnetwork 63 of that network. The network itself would be called 128.5.0.0 (Class B network number 5).

Notice that by using subnet masks, you can define a natural hierarchy in which the addresses themselves indicate how a packet is to be routed. However, all routing devices on an IP network must be using the same subnetting scheme.

Also note that a subnet mask for a given network segment is not part of the address and is not transmitted with every packet. It is simply a value which is known to all the routing devices adjacent to that segment.

Subnets of Class C networks

Since Class C networks are by far the most common, we will take a closer look at subnetting in a Class C network. Table B-1 is a listing of all possible values for the last octet (byte) in a Class C subnet mask.

Table B–1 Class C Subnet Masks

Mask	Binary	Subnets	Hosts/Subnet
128	10000000	0	0
192	11000000	2	62
224	11100000	6	30
240	11110000	14	14
248	11111000	30	6
252	11111100	62	2
254	11111110	126	0

One important thing must be noticed about the address divisions created by a subnet mask.

- RFC 950 requires that the first and last subnet created by a mask are reserved. So, the number of usable subnets is always 2 less than the number of divisions created. This makes 128 an unusable netmask because it has no legal subnets! The first and last host address in each subnet are also reserved (see Reserved Addresses below). This means 254 is also an unusable subnet mask because there are no legal host addresses.

Reserved Addresses

In most IP machines, setting all the bits in the host portion of an IP address to 1 indicates a broadcast to all nodes on the network. In the

Class B network described above, an address of 128.5.255.255 is a broadcast address meaning the packet is destined for all nodes on the entire Class B network. 128.5.63.255 would be a broadcast address indicating that the packet is destined for all nodes on subnet 63 of that Class B network.

However, one rare version of TCP/IP instead considers an address in which the host bits are all set to 0 a broadcast address. On the OfficeConnect Remote 840, you configure for this difference as part of the Advanced Parameters in the IP LAN setup.

On networks with a "high" broadcast address, setting all bits to 0 simply means "this host" or "this network" and is usually used only when a node does not know its own network or node address (and is probably requesting that information).

One other reserved address is 127.x.x.x. The contents of the last three bytes are not important. This is a loopback address used for troubleshooting. It allows you to verify that a device can send something to itself. A packet with this address should never actually leave the machine that originated it.

Supernetting (Advanced TCP/IP)

Because Class B Internet addresses are in short supply, larger networks are now usually granted a contiguous block of several Class C addresses. Unfortunately, this creates very large routing tables since multiple Class C routes have to be defined for each network containing more than 254 nodes. Larger routing tables mean more work for the routers and, therefore, poorer performance.

Supernetting (Classless InterDomain Routing) is a technique that allows each of these larger networks to be represented by a single routing table entry.

To do this, supernet addressing does something very different from traditional TCP/IP routing (which allows only one netmask per network). In supernet routing, each supernet can be assigned its own netmask. Supernetting is defined in RFC 1519.

Since supernet addressing is a fairly complex mechanism, the easiest way to understand it is to walk through the setup process.

You must first select a netmask for each supernet. Each supernet must have a netmask assigned to it. The netmask for an individual supernet can be, but does not have to be, the same as the netmask for any other supernet.

As in subnetting, a netmask creates a division between the network portion of an address and the host portion of an address. However, since the network you are defining is larger than a Class C network, the division you are creating is not in the fourth octet of the address. For this example, we'll be creating supernets composed of fewer than 254 Class C networks. So, their netmasks will actually be splitting up the third octet in their IP addresses.

The number of zero bits in the third octet will actually dictate the number of Class C networks in the supernet. Each zero bit makes the supernet twice as large. So, a supernet composed of 8 Class C networks would actually have 3 zeroes (8 = 23).

This would seem very limited since it restricts you to using groups that nicely fit into a power of 2 (1, 2, 4, 8, 16...). However, inconveniently-sized supernets can be accommodated because of a simple fact: a netmask with more 1 bits will override a netmask with fewer 1 bits.

This allows a smaller supernet to share the address space of a larger supernet. If, for example, you had a supernet of size 6 and a supernet of size 2, you could assign the larger supernet an 8 network address space and assign the smaller supernet the portion of that address space that the larger supernet was not using. Because the smaller supernet's netmask has more 1 bits, packets whose address was part of its address space would be routed to the smaller supernet even though the address is also part of the address space dictated by the larger supernet's netmask.

You must select a range of addresses for each supernet. The range of addresses in a supernet must fit exactly into a space that can be described by its netmask. This means that the zero bits in the netmask must also appear in the first address of the supernet block. For this to be true, the third octet in the address must be an even multiple of the same power of 2 used to form the netmask. For example, if you had created a block of 8 networks, the third octet in the first address will be an even multiple of 8.

Supernetting and the OfficeConnect Remote 840

In order to define a supernet on the OfficeConnect Remote 840, you must add the network address and its netmask. You have two options with OfficeConnect Remote 840. The first option permits you to set the subnet via numerical (8-30 bits) designation. For example:

```
add ip network houston address 192.75.202.99/23
```

Secondly, you can specify a class designation: A, B, or C. You can also leave the subnet value blank and let the OfficeConnect Remote 840 choose it for you. In this case, however, OfficeConnect Remote 840 will specify a class setting based on the IP address. For example:

```
add ip network houston address 192.75.202.99/C
```

To avoid confusion when configuring an IP address and subnet mask for a user, as opposed to a network, be aware that some user commands (e.g.: set network user) offer the option of H for the subnet class designator. This value can be used only when the station being identified is a host. Networked nodes still require class or numeric (8-32 bits) subnets. For example:

```
set vc same remote_ip_address 234.170.168.0/h
```

IP Subnet Mask Address

Subnet masking is used to expand the number of networks due to the 32-bit limitation of an IP's address field. When assigned an address by the NIC, the address can be further broken down to expand the single net number to many more by using host bits.

IP Planning

If you are not very familiar with IP addressing, read the following sections to gain a better understanding before assigning addresses.

Assigning IP Addresses and Subnetting

In IP, every “interface” typically gets an address. Interface, in this context, tends to mean “IP port.” Your workstations each have one IP port--its Ethernet adapter card, which is connected to an Ethernet hub by a twisted-pair cable. The OfficeConnect Remote 840, however, has multiple ports: one ethernet and one for each virtual circuit over the ATM WAN interface. An OfficeConnect Remote 840's LAN (Ethernet) port must be assigned an address, but assigning the WAN ports an address is optional. Not providing a WAN IP address creates and unnumbered WAN interface. This feature simplifies configuration but is not always available because it must be used at both ends of the connection. For more information on unnumbered interfaces see the last section in this appendix, “IP Numbered and Unnumbered Links”.

To route IP, the two networks to be linked by the OfficeConnect Remote 840 (local LAN and the ISP's or remote site's network) must be on separate IP subnets. For example, all local LAN devices could be on subnet 192.168.1 and all devices in at the remote site could be on subnet 192.168.2. Put another way, all devices connected to the local LAN must be assigned IP addresses that begin with 192.168.1, for example 192.168.1.1, and all devices on the remote LAN must be assigned addresses that begin with 192.168.2, for example, 192.168.2.1.

Each IP address uniquely identifies a machine on an IP network. Therefore, to avoid duplication, IP addresses are regulated and are ultimately purchased from an organization (see the previous section). You probably won't need to purchase your own IP addresses for your home/office LAN. If you are connecting to the Internet, the ISP will provide you with one or more addresses. If you are connecting to a remote office, the network administrator should be able to provide you with a subset of addresses from the set that were assigned to the remote office.

Single IP Address

If you are provided with a single IP address, you'll use the OfficeConnect Remote 840's Port Address Translation (PAT) feature. The IP address will be assigned to the OfficeConnect Remote 840's local WAN interface.

PAT allows you to make up an IP network for your LAN, using IP addresses of your own choosing. This network is hidden from the ISP or remote site because all data traffic going out the OfficeConnect Remote 840's WAN port will carry the assigned IP address. Since it is hidden, it does not matter if the addresses you use are duplicated elsewhere. Using PAT, the OfficeConnect Remote 840 keeps track of mapping the data packets to their rightful owners, the workstations on the LAN.

For more information on PAT, see the "Address Translation Tutorial".

Range of IP Addresses

If you are provided with a range of IP addresses, it may be given to you in the form of an IP address and netmask.

Example: We were given the IP address 2xx.xxx.188.176 with mask 255.255.255.248.

The first task is to understand our IP address range and decide which addresses to assign to the workstations and which address to assign to the OfficeConnect Remote 840. We take our first address, 2xx.xxx.188.176, and the subnet mask, 255.255.255.248, together to determine the number of addresses we had to work with.

First, we convert the last octet (the eight-bit decimal equivalent) of the IP address (176) and the last octet of the subnet mask (248) to binary:

176

1	0	1	1	0	0	0	0

248

1	1	1	1	1	0	0	0

The 0s in the subnet mask define our address range, and their three binary positions (23) yield eight addresses. The addresses that contain all zeroes and all ones (2xx.xxx.188.176 and 2xx.xxx.188.183, respectively--see the table below) are reserved as broadcast addresses and cannot be used.

Also, we were told that 2xx.xxx.188.177 would be assigned to the OfficeConnect Remote 840's LAN interface, so we can't assign it to any other computer(s) on the LAN.

Table B-2 IP Addresses

Last Octet (In Binary)	Last Octet (In Decimal)	Status
10110 000	176	Reserved - broadcast address
10110 001	177	To be assigned to OfficeConnect Remote 840
10110 010	178	Available
10110 011	179	Available
10110 100	180	Available
10110 101	181	Available
10110 110	182	Available
10110 111	183	Reserved - broadcast address

IP Numbered and Unnumbered Links

The OfficeConnect Remote 840 supports two types of IP addressing on the Remote Site links: numbered and unnumbered. A numbered link exists when an IP address identifies the interface as belonging to a specific IP network or subnet (See Figure B-1).

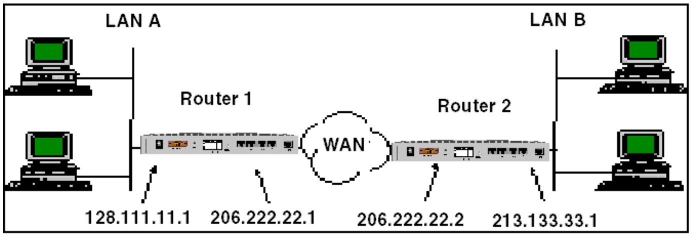


Figure B–1 Numbered WAN Interfaces

An unnumbered link exists when the IP address 0.0.0.0 is assigned and indicates the interface does not belong to a specific network (see Figure B-2).

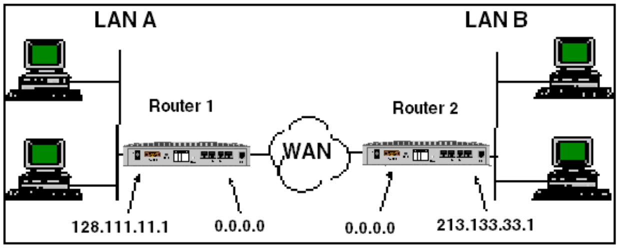


Figure B-2 Unnumbered WAN Interfaces

The major advantage of using unnumbered links is that you save scarce IP address space. Looking at Figure B-1, you can see that three IP networks are in use, 128.111.11.x (LAN A), 206.222.22.x (WAN), and 213.133.33.x (LAN B). The WAN network numbers are not needed when unnumbered is used. If the unnumbered scheme is used at only one end of the WAN link, a single IP address is saved. If it is used at both ends of the WAN link, an entire IP subnet will be saved.

At first glance it seems that unnumbered addressing would cause problems for routers. One expects each interface to be assigned an IP address. When the router sends router-generated packets (such as RIP packets or PINGs) the source IP address in the packet is typically the address of the interface the packet goes out. There could also be a concern about how to route packets to an unnumbered interface.

There are a few rules which take care of the problems. The Ethernet interface cannot be unnumbered. The router adopts a “router id,” which for the OfficeConnect Remote 840 is the IP address assigned to the

Ethernet interface. This IP address is the source IP address for router-generated packets going out unnumbered interfaces. The router's routing tables and default gateway settings take care of getting the data traffic to the correct remote destinations. Therefore, although you cannot PING or TELNET to the WAN interface when unnumbered is in use, you can PING or TELNET the router using the IP address of a numbered interface.

Unnumbered does not mean unconfigured. An OfficeConnect Remote 840 with factory default configuration will not provide an unnumbered link - you must configure the remote site local WAN IP address as unnumbered (equal to 0.0.0.0).

C

ADDRESS TRANSLATION TUTORIAL

Overview

Public IP addresses are registered and can be used within a public network, such as the Internet. Due to the limitation of IP version 4 address space and the growth of the Internet, public addresses are becoming more scarce.

One solution to this problem is to use private addresses on small LANs and to use Address Translation when accessing devices on the public network. Address Translation changes a private address to a public address at the gateway of a public network.

There are two types of address translation, Network Address Translation and Port Address Translation:

- "Network Address Translation (NAT)"
  - "NAT Example"
  - "Dynamic NAT"
  - "Static NAT"
- "Port Address Translation (PAT)"
  - "PAT Example"
  - "Dynamic PAT"
  - "Static PAT"
  - "Default PAT"

Network Address Translation (NAT)

With NAT, a pool of public addresses is configured and dynamically mapped to a private workstation address when accesses are made through the gateway to a public network. The public-to-private address mapping remains active until the privately-addressed workstation stops accessing the public network. The public address is then returned to the available pool of addresses.

When NAT is configured, static mappings and/or dynamic pools of addresses must be configured. Static assignments permanently map a private address to a public address.

Dynamic pools consist of a start IP address, the number of addresses in the pool, and a mask to be used for RIP messages if the public addresses are to be advertised. Multiple pool and static assignments may exist within a pool range.

NAT Example

Your remote site administrator or ISP provides a pool of addresses for your local LAN.

If there are enough addresses for each machine and your OfficeConnect Remote 840, you do not need to use NAT. Simply assign each machine an address from the pool. If the number of machines is greater than the number of available addresses, use NAT. As with PAT, you make up a private IP network for the LAN and assign an IP address from that network to each workstation and the OfficeConnect Remote 840 (LAN IP address). RIP (if enabled) must be set to “listen only” so the OfficeConnect Remote 840 will learn routing information from the WAN but will not broadcast the private network information. Doing this provides a firewall and hides the private local network from the outside world.

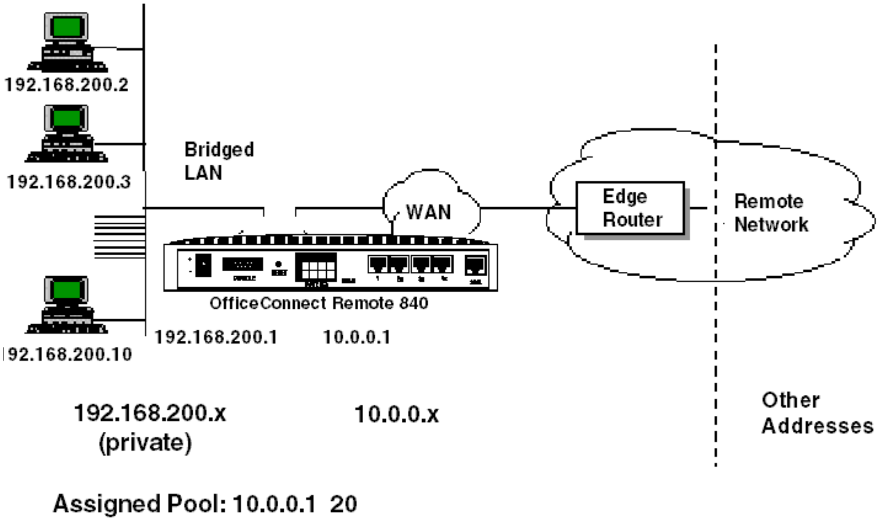


Figure C–1 NAT Example

Dynamic NAT

When a local PC sends a packet destined for the WAN, the OfficeConnect Remote 840 puts the private source IP address and an IP address from the pool into an address translation table. A change is made in the data packet: the private source IP address is replaced by the IP address from the pool and sent to the WAN. When the reply returns, it contains the IP address from the pool. This address is used to search the address translation table for the original private IP address. The private IP address is put into a reply packet and sent to the Ethernet.

When all the pool addresses are in use, any new requests are rejected and the workstation on the LAN has to wait until one of the pool addresses is free for use. To ensure that addresses are not held indefinitely, a timer is associated with each table entry. An entry is freed after 5 minutes of inactivity or if the session between the workstation and the remote site is ended.

This method requires initiating incoming packets from the LAN. Packets from the WAN are rejected unless they have an IP address number that is in the pool and is currently in the address translation table.

Static NAT

Static NAT operates like Dynamic NAT except you may add entries to the address translation table and indicate specific IP addresses from the pool to map to specific private LAN IP addresses. This allows controlled access by the outside world.

Port Address Translation (PAT)

PAT is used when several privately addressed workstations share a single public address. PAT uses the TCP and UDP port numbers to map multiple private addresses to the single public address. For normal applications such as web browsing and FTP transfers, PAT can be configured by just enabling the feature. When accesses are originated from the private addressed LAN, a mapping is established between the source port number and the source private address. When the response is received on the public addressed WAN port, the destination port is mapped back to the private address.

Static PAT port mappings or the PAT default address need to be configured when an application will initiate a TCP or UDP connection from the public network. If a publicly accessible server resides on a privately addressed LAN, static ports can be defined for the applications they are running.

For example, TCP port 80 for a Web Server and TCP port 21 for a FTP server can be statically assigned. The PAT default address can be used with, or instead of, static port assignments, and is set to the private address of a workstation on the local LAN.

If an incoming IP data packet is received on a WAN port and there is no existing dynamic or static port mapping, the packet will be translated using the PAT default address.

PAT Example

Your remote site administrator or ISP provides one address for the OfficeConnect Remote 840's Local WAN IP address (In the example above, 10.0.0.1). You make up a private IP network for the LAN and assign an IP address from that network to each workstation and to the OfficeConnect Remote 840 (LAN IP address).

RIP (if enabled) must be set to “listen only” so the OfficeConnect Remote 840 will learn routing information from the WAN but will not broadcast the private network information.

Doing this provides a firewall and hides the private local network from the outside world.

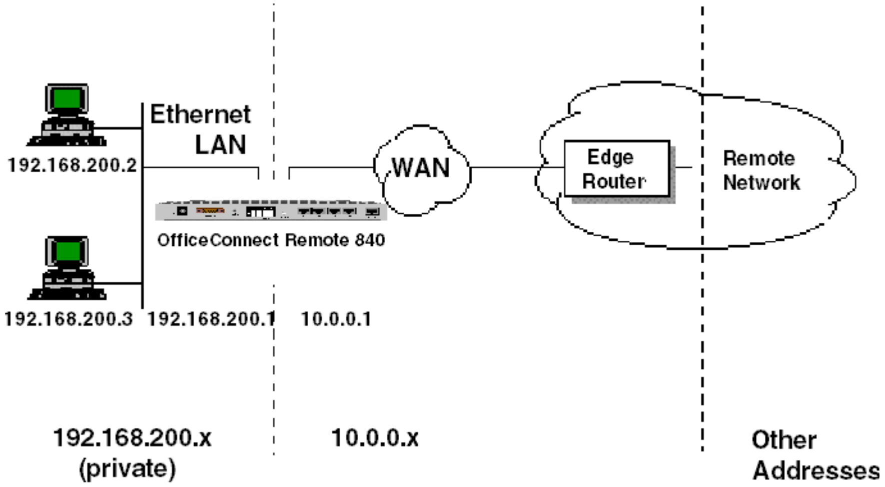


Figure C–2 PAT Example

Dynamic PAT

When a local PC sends a packet destined for the WAN, the OfficeConnect Remote 840 puts its source IP address and a port number into an address translation table. The port number is also placed into the data packet.

An additional change is made to the packet: the original (private) source IP is replaced by the OfficeConnect Remote 840 WAN IP address. Then the packet is sent to the WAN.

The reply will contain the OfficeConnect Remote 840 WAN IP address and port number. The port number is used to search the address translation table for the original private IP address.

The original IP address is then put in a reply and sent to the Ethernet.

This method requires initiating incoming packets from the LAN. Packets from the WAN are rejected unless they currently have a port number in the table.

Static PAT

Static PAT operates like Dynamic PAT except you may add entries to the address translation table and specify which port numbers to map to which private IP addresses. This allows controlled access by the outside world. You would select the port numbers based on the type of access needed. For example, if you had a local WEB server, you would select the IP address of your server and the port number 80, which is the UDP and TCP port number used to indicate HTML traffic.

Default PAT

Default PAT operates like Dynamic PAT except you may specify a default private IP address for all traffic whose port numbers are not in the address translation table. However, this may remove the Firewall. With a default IP address, all traffic initiated on the WAN and not sent to other private IP addresses will go to this IP address. In Dynamic and Static PAT, traffic from the LAN, not the WAN, determines the use of the address translation table.

D

USING THE CLI GUIDE

Overview

The preferred method of configuring and managing the OfficeConnect Remote 840 SDSL Router is the Web Browser based Remote 840 Manager. It also comes with a sophisticated Command Line Interface (CLI).

A command line interface will require you to type in individual commands on the screen. You can view and print the *OfficeConnect Remote 840 SDSL Router CLI User's Guide* (in pdf format) from the CD supplied with your unit, or from the 3Com website **http://www.3com.com/support/ocr840/index.html** under **User Documentation**.

Accessing the CLI from the OfficeConnect Remote 840 Manager

To use this feature, from the Home page, select the “**Tools**” link, then select the new “**Command Line Interface**” link. On the next screen select the “**Start CLI**” button. This starts a separate (not within the browser) Telnet window that automatically Telnets to the IP address of the OCR unit that the browser is using. The browser stays open, too. Telnet asks the user to login before presenting the CLI prompt. The login/password are the same as those used for accessing the HTML screens with the browser.

E

CONFIGURATION (NON-SETUP WIZARD) OF THE OFFICECONNECT REMOTE 840

This chapter describes the details for performing the initial configuration of a OfficeConnect Remote 840 when the unit has not been configured or has been restored to factory defaults. This installation method does not use the Setup Wizard. If you want to use Setup Wizard, please refer to the printed Installation Guide that came with your OfficeConnect Remote 840.

- "Instructions for Internet Access"
- "Instructions for Telecommuting / Remote Office Access"
- "Using the Configuration Audit"
- "Saving the Configuration"
- "Testing the Configuration"

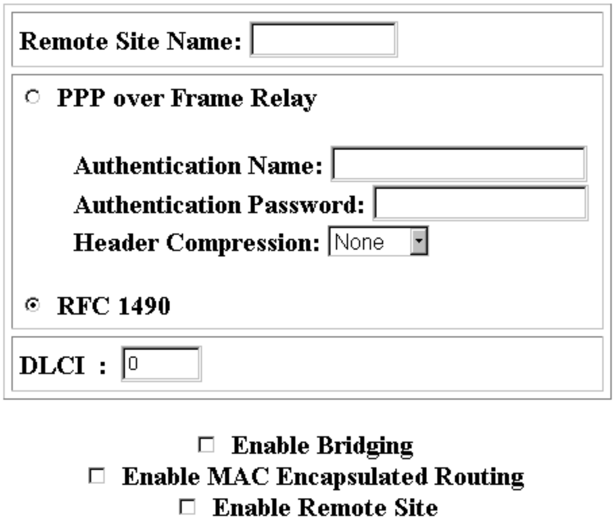
Instructions for Internet Access

Before you configure your OfficeConnect Remote 840 for Internet Access, make sure you have completed the appropriate Internet Configuration Planning Form by entering information from your service provider. (For your convenience, the forms have been reproduced in **Chapter 1** of the of the *OfficeConnect Remote 840 SDSL Router Install Guide*.)

Step 1: Configuring Remote Site General Information

1 Add a remote site by going to the OfficeConnect Remote 840 home page. Select **Configuration > Remote Sites (WAN) > Add**.

If your unit is using Frame Relay, this will access the Remote Sites General Add screen, containing the following fields:



Remote Site Name:

○ **PPP over Frame Relay**

Authentication Name:

Authentication Password:

Header Compression: None

● **RFC 1490**

DLCI : 0

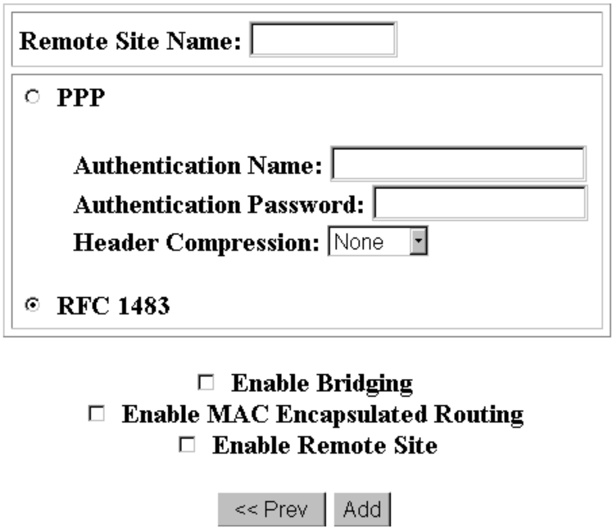
□ **Enable Bridging**

□ **Enable MAC Encapsulated Routing**

□ **Enable Remote Site**

- Enter a name to identify the remote site.
- Enter the Max Packet Size.
- Set **Network Service** to **PPP over Frame Relay** or **RFC 1490**.
- Enter the **DLCI**.
- Check the **Enable Bridging** and **Enable MAC Encapsulated Routing** boxes according to your service provider’s directions.
- Check the **Enable Remote Site** box.

If your unit is using ATM, the Remote Sites General Add screen will contain the following fields:



Remote Site Name:

○ PPP

Authentication Name:

Authentication Password:

Header Compression: None

● RFC 1483

□ Enable Bridging

□ Enable MAC Encapsulated Routing

□ Enable Remote Site

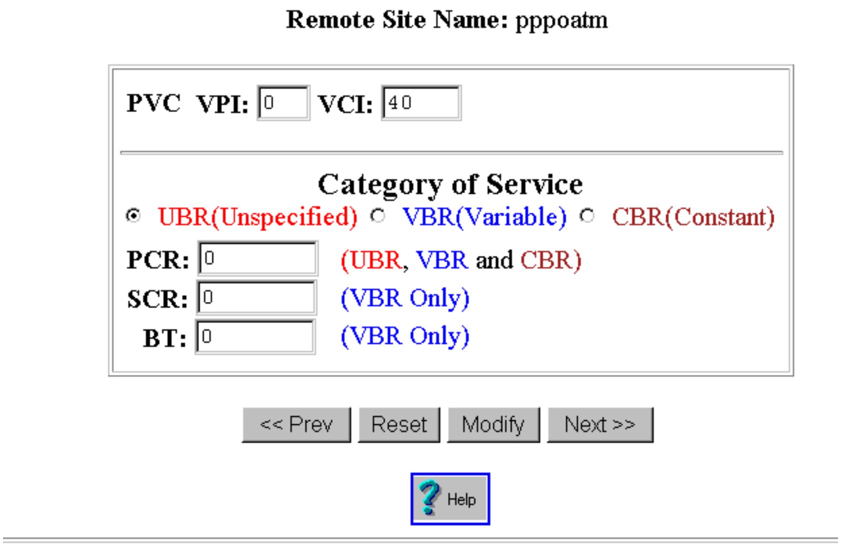
- Enter a name to identify the remote site.
- Set **Network Service** to **PPP over Frame Relay** or **RFC 1483**.
- If PPP, enter the **Authentication Name** and **Authentication Password** provided to you. You can change the header compression from the default of none to TCP/IP if you wish.
- Check **Enable Bridging** and **Enable MAC Encapsulated Routing** boxes according to your service provider’s directions.

2 Click the **Add** button. This advances you to the ATM Modify screen.

Step 2: Configuring the Remote Site ATM Parameters (ATM Only)

The ATM Modify screen is to be filled in with information from the Configuration Planning Forms in Chapter 1 of the *Installation Guide*.

The screen contains the following fields:



Remote Site Name: pppoatm

PVC VPI: 0 **VCI:** 40

Category of Service

● UBR(Unspecified) ○ VBR(Variable) ○ CBR(Constant)

PCR: 0 (UBR, VBR and CBR)

SCR: 0 (VBR Only)

BT: 0 (VBR Only)

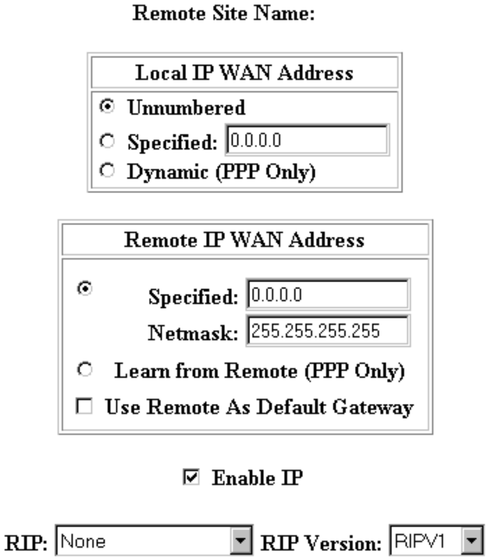
1 Enter the information in these fields as contained in the Configuration Planning Forms.

- Enter the Virtual Path Identifier (VPI) and the Virtual Channel Identifier (VCI) for the virtual channel you are configuring.
- If necessary, enter any upstream **Category of Service** parameters that may have been provided to you.
- The default value of **UBR** with a Peak Cell Rate (PCR) of 0 will attempt to use all available bandwidth when transmitting.

2 Press **Next** to continue on to the IP Modify Screen.

Step 3: Configuring the Remote Site IP Network Information

The IP Modify screen contains the following fields.



Remote Site Name:

Local IP WAN Address

● Unnumbered

○ Specified: 0.0.0.0

○ Dynamic (PPP Only)

Remote IP WAN Address

● Specified: 0.0.0.0

Netmask: 255.255.255.255

○ Learn from Remote (PPP Only)

□ Use Remote As Default Gateway

☑ Enable IP

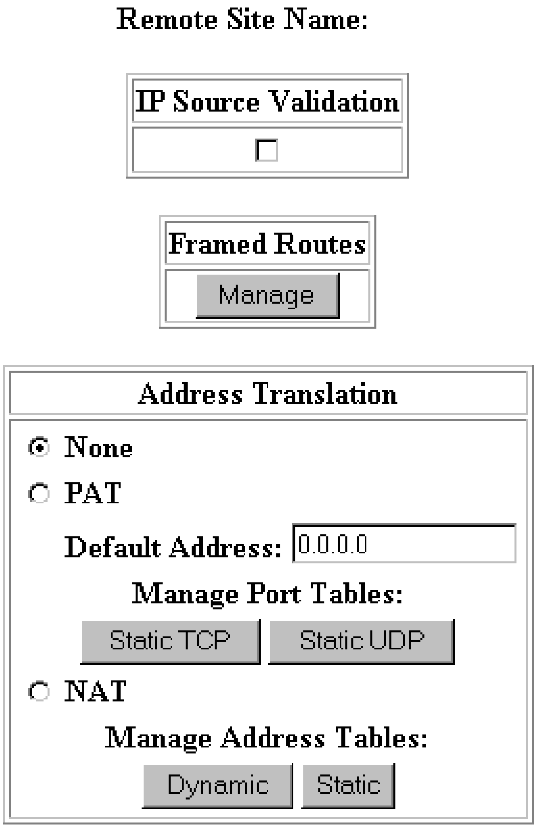
RIP: None RIP Version: RIPV1

1 Configure the Local WAN IP Address:

- If the ISP provided you with a single IP address, select **Specified** and enter that address.
- If you are using PPP to dynamically assign an address, select **Dynamic**, and the remote site on the WAN will assign a local WAN IP address to you.
- Otherwise, select **Unnumbered**, and there will be no IP address assigned to the VC connection.
- Configure the Remote WAN IP Address:
- If the ISP provided a remote IP address and netmask, select **Specified** and type in that address and netmask.
- If the OfficeConnect Remote 840 is learning the remote IP address from the remote site (PPP only), select **Learn From Remote**.
- In order to designate the remote site you are configuring as the default gateway, check the **Use Remote as Default Gateway** checkbox.(Only one remote site can be designated as the default gateway.)

- If you want to run RIP, select from the pull-down menu to have the RIP set to **Broadcast**, **Listen**, or **Broadcast & Listen**, and if one of these is chosen, set the RIP option to RIPV1 or RIPV2.
- Ensure that **Enable IP** is checked (enabled).

2 Press the **Next** button to proceed to the IP Advanced Modify screen. This screen contains the following fields:



Remote Site Name:

IP Source Validation

□

Framed Routes

Address Translation

● None

○ PAT

Default Address: 0.0.0.0

Manage Port Tables:

○ NAT

Manage Address Tables:

3 Check the **Enable PAT** button to use Port Address Translation (refer to the **Configuration Planning Table** in **Chapter 1** of the *OfficeConnect Remote 840 SDSL Router Install Guide* to determine if PAT is to be enabled).

You cannot use an unnumbered Local IP WAN Address and have PAT enabled.

4 Press the **Modify** button before leaving this screen to save the changes.

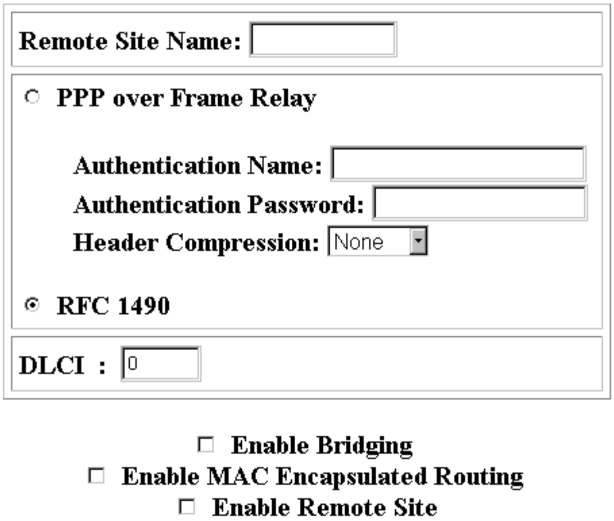
5 If you are also going to configure the router for Telecommuting / Remote Office Access, continue to the next section. Otherwise, go to Using the Configuration Audit.

Instructions for Telecommuting / Remote Office Access

Before you configure your OfficeConnect Remote 840 to access a remote office, make sure you have completed the Telecommuting/Remote Access Planning Form from Chapter 1 of the Installation Guide by entering information from your remote site network administrator.

Step 1: Configuring Remote Site General Information

Add a remote site by going to the OfficeConnect Remote 840 home page.



Remote Site Name:

○ **PPP over Frame Relay**

Authentication Name:

Authentication Password:

Header Compression: None

● **RFC 1490**

DLCI : 0

□ **Enable Bridging**

□ **Enable MAC Encapsulated Routing**

□ **Enable Remote Site**

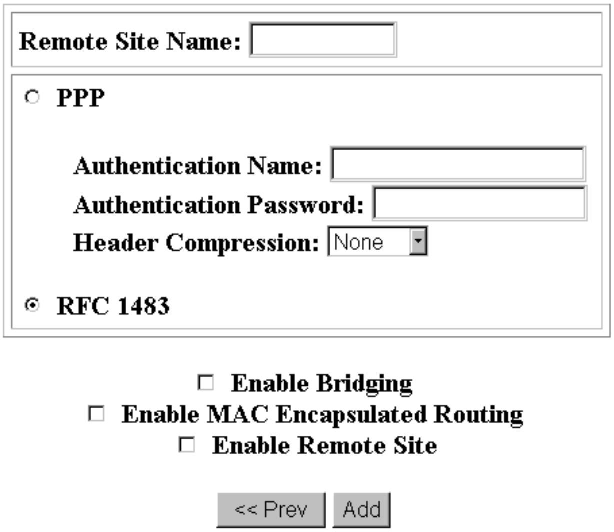
1 Add a remote site by going to the OfficeConnect Remote 840 home page. Select **Configuration > Remote Sites (WAN) > Add**.

If your unit is using Frame Relay, this will access the Remote Sites General Add screen, containing the following fields:

- Enter a name to identify the remote site.
- Set **Network Service** to **PPP over Frame Relay** or **RFC 1490**.

- Enter the **DLCI**.
- Check the **Enable Bridging** and/or **Enable MAC Encapsulated Routing** boxes as needed.

If your unit is using ATM, the Remote Sites General Add screen will contain the following fields:



Remote Site Name:

○ PPP

Authentication Name:

Authentication Password:

Header Compression: None

● RFC 1483

□ Enable Bridging

□ Enable MAC Encapsulated Routing

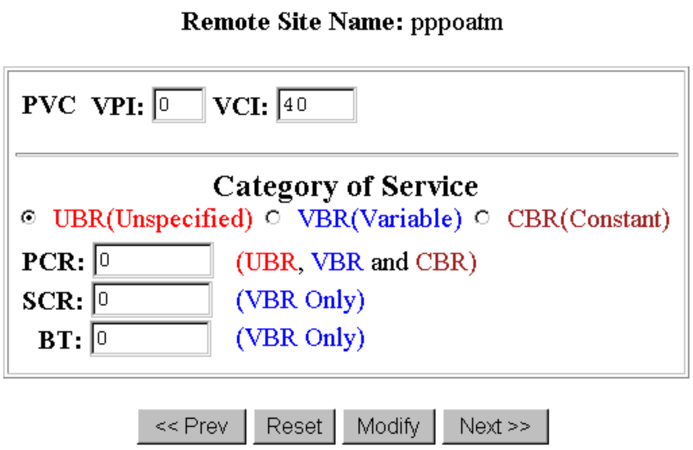
□ Enable Remote Site

- Enter a name to identify the remote site.
- Set **Network Service** to **PPP over Frame Relay** or **RFC 1483**.
- If PPP, enter the Authentication Name and Authentication Password provided to you. You can change the header compression from the default of **none** to TCP/IP if you wish.
- Check the **Enable Bridging** and/or **Enable MAC Encapsulated Routing** boxes as needed.

2 Click the **Add** button. This advances you to the ATM Modify screen.

Step 2: Configuring the Remote Site ATM Parameters

The ATM Modify screen shown below is to be filled in with information from the Configuration Planning Table you completed in Chapter 1 of the Installation Guide.



Remote Site Name: pppoatm

PVC VPI: 0 **VCI:** 40

Category of Service

● UBR(Unspecified) ○ VBR(Variable) ○ CBR(Constant)

PCR: 0 (UBR, VBR and CBR)

SCR: 0 (VBR Only)

BT: 0 (VBR Only)

1 Enter the information in these fields as contained in the Configuration Planning Table in *Chapter 1 of the OfficeConnect Remote 840 SDSL Router Install Guide*.

2 2 Enter the Virtual Path Identifier (VPI) and the Virtual Channel Identifier (VCI) for the virtual channel you are configuring.

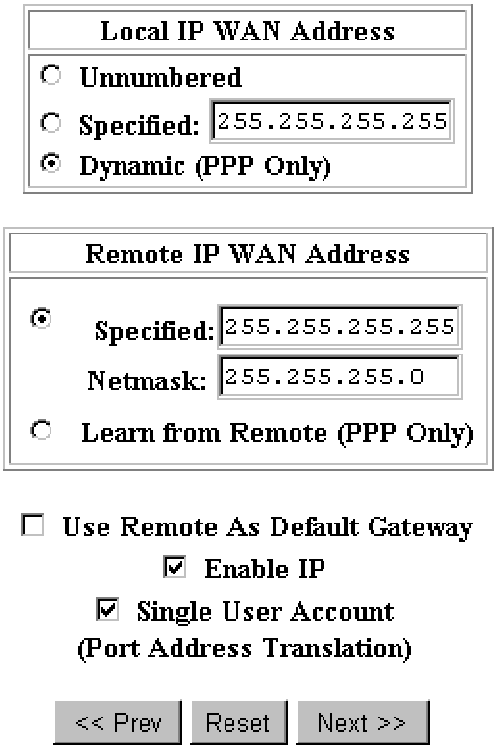
3 If necessary, enter any upstream Category of Service parameters that may have been provided to you.

The default value of UBR with a Peak Cell Rate (PCR) of 0 will attempt to use all available bandwidth when transmitting.

4 Press **Next** to continue on to the IP Modify Screen.

Step 3: Configuring the Remote Site IP Network Information

1 If you are routing with IP, complete the entries on this screen. Otherwise, press **Next**.



Local IP WAN Address

○ Unnumbered

○ Specified: 255.255.255.255

● Dynamic (PPP Only)

Remote IP WAN Address

● Specified: 255.255.255.255

Netmask: 255.255.255.0

○ Learn from Remote (PPP Only)

□ Use Remote As Default Gateway

☑ Enable IP

☑ Single User Account (Port Address Translation)

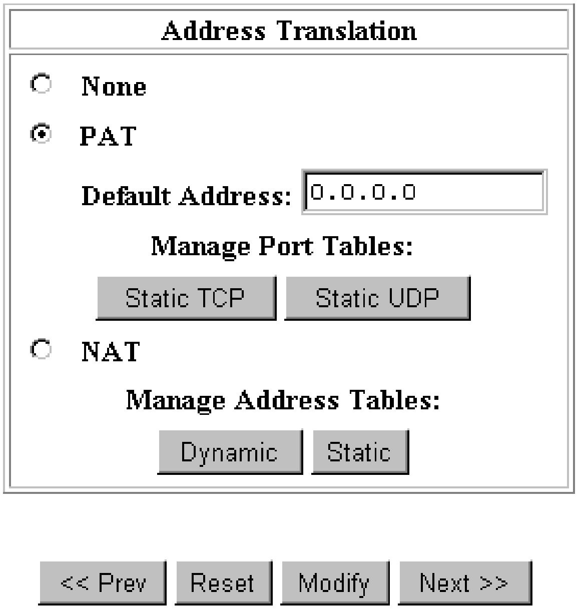
2 Local WAN IP Address:

- If the remote site administrator provided you with a single IP address, select **Specified** and enter that address.
- If you are using PPP to assign a single IP address dynamically, select **Dynamic**, and the remote site on the WAN will assign a local WAN IP address to you.
- Otherwise, select **Unnumbered**, and there will be no IP address assigned to the VC connection.

3 Remote WAN IP Address:

- If the remote site administrator provided a remote IP address and netmask, select **Specified** and type in that address and netmask.
- If the OfficeConnect Remote 840 is learning the remote IP address from the remote site (PPP only), select **Learn From Remote**.
- In order to have the remote site you are configuring act as the default gateway, check the **Use Remote as Default Gateway** checkbox. (Only one remote site can be designated as the default gateway.)
- If you want to run RIP, select from the pull-down menu to have the RIP set to **Broadcast**, **Listen**, or **Broadcast & Listen**, and if one of these is chosen, set the RIP option to RIPV1 or RIPV2.
- Ensure that Enable IP is checked (enabled).

4 Press the **Next** button to proceed to the IP Advanced Modify screen (shown below).



Address Translation

○ None

● PAT

Default Address: 0.0.0.0

Manage Port Tables:

○ NAT

Manage Address Tables:

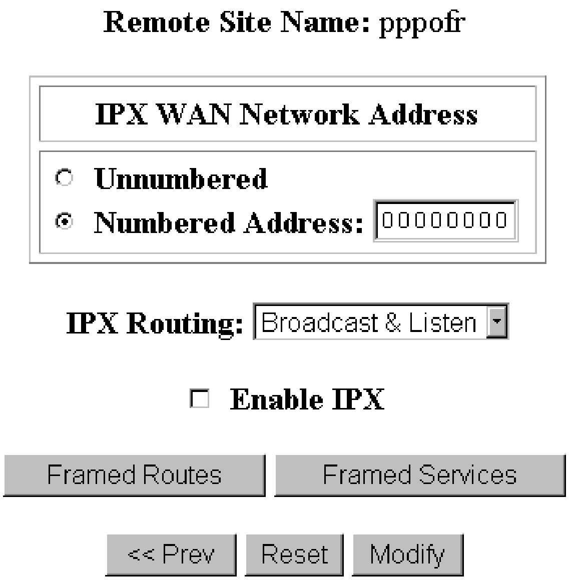
5 Check the **Enable PAT** button to use Port Address Translation. (See the Configuration Planning Table in Chapter 1 of the Installation Guide to determine if PAT is to be enabled.) If Network Address translation is required, select NAT.

You cannot use an unnumbered Local IP WAN Address and have PAT enabled.

6 If you are routing IPX, press the **Next** button to proceed to the IPX Modify screen. If you are not routing IPX, press **Modify** to complete the remote site configuration.

Step 4: Configuring the Remote Site IPX Network Information

1 If you are routing IPX, complete the entries in this page. Otherwise, press the **Modify** button to complete your remote site configuration, and then press the **Save Configuration** button.



Remote Site Name: pppofr

IPX WAN Network Address

○ Unnumbered

● Numbered Address: 00000000

IPX Routing: Broadcast & Listen

□ Enable IPX

2 Select the option in the IPX WAN Network Address box.

- Select Unnumbered or, if the remote site administrator provided an IPX address for the WAN connection, select **Numbered** and then enter the address.
- To automatically learn IPX RIPs and SAPs, set the **IPX Routing** option to **Both**.

3 Check the **Enable IPX** checkbox.

4 Press the **Modify** button to finish the configuration of the remote site.

5 5 Press the **Save Configuration** button on the sidebar to save the settings you just entered.

Step 5: Configuring a Local IPX Network

If you are setting up the OfficeConnect Remote 840 to route IPX, follow these steps.

1 From the OfficeConnect Remote 840 home page, select **Configuration > Local Site (LAN) > IPX > Add**.

2 Enter a name for the network, the IPX address of the network, and the frame type of the network running on the LAN.

3 Check the **Enable IPX** box.

4 Click the **Add** button to add this defined IPX network.

5 Press the **Save Configuration** button on the sidebar to save the settings you just entered.

Step 6: Configuring a Local Bridge Network

If you are setting up the OfficeConnect Remote 840 to bridge traffic, follow these steps:

1 From the OfficeConnect Remote 840 home page, select **Configuration > Local Site (LAN) > Bridge > Add**.

2 Enter a name for the network and check the **Enable Bridging** box.

3 Click **Add** to add this defined bridge network.

If you plan to bridge IP packets instead of routing them, you need to disable IP Forwarding. To do this:

1 From the OfficeConnect Remote 840 Manager home page, select **Global > IP > IP Settings**.

2 Uncheck the **IP Forwarding** checkbox, and press the **Submit** button. At this point, you will momentarily lose connectivity.

3 To re-establish the connection, press the Stop button on the Web browser, and then press the Reload button.

Using the Configuration Audit

When you have finished the basic configuration, run the Configuration Audit by visiting the OfficeConnect Remote 840 home page. Select **Tools > Configuration Audit**.

Read the explanation of the audit topics and categories to help you interpret the results of the audit by selecting the audit topics at the bottom of the page. Notice that a link is provided at the bottom of each audit topic's configuration page if changes are needed.

Saving the Configuration

Pressing the **Save Configuration** on the sidebar (also within the Tools menu) causes the current configuration of the unit to be saved to FLASH memory. This means that this configuration will be reinstated after power cycle or reboot.

Unless saved to FLASH, configuration changes remain in effect only until the next reboot or power cycle.

Testing the Configuration

After you finish your configuration, you will need to test the configuration. See the chapter on Testing the Configuration in the Installation Guide.

F TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the very latest, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site

World Wide Web Site

Access the latest networking information on the 3Com Corporation World Wide Web site by entering the URL into your Internet browser:

`http://www.3com.com/`

This service provides access to online support information such as technical documentation and software library, as well as support options ranging from technical education to maintenance and professional services.

A user name and password are not needed with Web browser software such as Netscape Navigator and Internet Explorer.

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number

- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, please call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain a Return Materials Authorization (RMA) number. Products sent to 3Com without RMA numbers will be returned to the sender unopened, at the sender’s expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266)	1 408 326 7120

3Com Corporation LIMITED WARRANTY

This warranty applies to customers located in the United States, Australia, Canada (except Quebec), Ireland, New Zealand, U.K., and other English language countries, and countries for which a translation into the local language is not provided.

OFFICECONNECT Remote 840 SDSL Router

HARDWARE

3Com warrants this hardware product to be free from defects in workmanship and materials, under normal use and service, for the following length of time from the date of purchase from 3Com or its authorized reseller:

Five (5) years

3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, 3Com may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. 3Com warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

SOFTWARE

3Com warrants that each software program licensed from it will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with 3Com's published specifications or user manual.

THIS 3COM PRODUCT MAY INCLUDE OR BE BUNDLED WITH THIRD PARTY SOFTWARE, THE USE OF WHICH IS GOVERNEND BY A SEPARATE END USER LICENSE AGREEMENT. THIS 3COM WARRANTY DOES NOT APPLY TO SUCH THIRD PARTY SOFTWARE. FOR THE APPLICABLE WARRANTY, PLEASE REFER TO THE END USER LICENSE AGREEMENT GOVERNING THE USE OF SUCH SOFTWARE.

YEAR 2000 WARRANTY

In addition to the Hardware Warranty and Software Warranty stated above, 3Com warrants that each product sold or licensed to Customer on and after January 1, 1998 that is date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com product, including hardware, software, and firmware, accurately exchange date data with the 3Com product, with the exception of those products identified at 3Com's Web site, http://www.3com.com/products/yr2000.html, as not meeting this standard. If it appears that any product that is stated to meet this standard does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com before the later of April 1, 2000, or ninety (90) days after purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days after purchase or until April 1, 2000, whichever is later.

OBTAINING WARRANTY SERVICE

Customer must contact a 3Com Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from 3Com or its authorized reseller may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after 3Com receives the defective product.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

Dead- or Defective-on-Arrival. In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement. The replacement product will normally be shipped not later than three (3) business days after 3Com's verification of the DOA product, but may be delayed due to export or import procedures. When an advance replacement is provided and Customer fails to return the original product to 3Com within fifteen (15) days after shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

Telephone Support. This OfficeConnect® or SuperStack® product comes with telephone technical support for ninety (90) days. The ninety (90) day period begins on the date of Customer's product purchase.

The telephone technical support is available from 9 a.m. to 5 p.m., local time, Monday through Friday, excluding local holidays. Telephone technical support is limited to the 3Com products designated above, and may include assistance with installation, product specific configuration, and identification of equipment problems. Please refer to the Technical Support appendix in the User's Guide for telephone numbers.

Response to requests for telephone technical support will be in the form of a return call from a 3Com representative by close of business the following business day.

To qualify for this ninety (90) days of telephone technical support, Customer must register on the 3Com Web site at http://support.3com.com/index/htm, and provide the date of purchase, product number, and serial number. 3Com reserves the right to modify or cancel this telephone support and software update offering at any time, without advance notice. This offering is not available where prohibited or restricted by law.

Warranties Exclusive

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

Limitation of Liability

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Disclaimer

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

Governing Law

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

3Com Corporation
5400 Bayfront Plaza
Santa Clara, CA 95054
(408) 326-5000

FCC Class B Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

WARNING: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, "Digital Apparatus," ICES-003. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

The user may find the following booklet prepared by the Federal Communications Commission helpful:

The Interference Handbook

This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402. Stock No. 004-000-00345-4.

NOTE: In order to maintain compliance with the limits of a Class B digital device, 3Com requires that you use quality interface cables when connecting to this device. Changes or modifications not expressly approved by 3Com could void the user's authority to operate this equipment. Refer to the manual for specifications on cabling types.

FCC Declaration of Conformity

We declare under our sole responsibility that the

Model:	**Description:**
3C840	OfficeConnect Remote 840

to which this declaration relates, is in conformity with the following standards or other normative documents:

- ANSI C63.4-1992 Methods of Measurement
- Federal Communications Commission 47 CFR Part 15, subpart B
  5.107 (e) Class B conducted limits

  5.109 (g) Class B Radiated Emissions Limits

3Com Corporation, 5400 Bayfront Plaza, P.O. Box 58145, Santa Clara, CA 95052-8145