

**NetComm™**

NB3

# My ADSL Modem

Ethernet/USB ADSL Modem Router

*User Guide*

Introduction .....	5
Package Contents .....	5
Features .....	6
System Requirements .....	6
Using this Document .....	6
Getting to Know the My ADSL Modem .....	8
Front Panel .....	8
Rear Panel .....	9
Do I need a Micro filter? .....	10
Quick Start .....	11
USB Configuration .....	12
Step 1 - Hardware Installation - USB .....	12
Step 2 - Computer Configuration - USB .....	13
Step 3 - Modem Configuration - USB .....	22
Ethernet Configuration .....	23
Step 1 - Hardware Installation - Ethernet .....	23
Step 2 - Computer Configuration - Ethernet .....	24
Step 3 - Modem Configuration - Ethernet .....	38
LAN Configuration .....	39
Step 1 - Hardware Installation - LAN .....	39
Step 2 - Computer Configuration - LAN .....	40
Step 3 - Modem Configuration - LAN .....	54
Assigning static Internet Information to your PCs .....	55
The My ADSL Modem Quick Configuration Page .....	56
Default My ADSL Modem Settings .....	59
Getting Started with the Configuration Manager .....	60
Accessing the Configuration Manager .....	60
Functional Layout .....	61
Configuring the LAN Ports .....	67
Connecting via Ethernet .....	67
Configuring the LAN Port IP Address .....	67
Viewing the My ADSL Modem's IP Addresses .....	70
Viewing IP Performance Statistics .....	71
Configuring Dynamic Host Configuration Protocol .....	72
Overview of DHCP .....	72
My ADSL Modem DHCP modes .....	72
Configuring DHCP Server .....	73
Viewing, modifying, and deleting address pools .....	76

Configuring Network Address Translation .....	80
Overview of NAT .....	80
Viewing NAT Global Settings and Statistics .....	81
Viewing NAT Rules and Rule Statistics .....	83
Viewing Current NAT Translations .....	84
Configuring DNS Server Addresses .....	98
About DNS .....	98
Assigning DNS Addresses .....	98
Configuring DNS Relay .....	98
Configuring IP Routes .....	101
Overview of IP Routes .....	101
Adding IP Routes .....	104
Configuring Routing Information Protocol .....	105
RIP Overview .....	105
When should you configure RIP? .....	105
Viewing RIP Statistics .....	107
Configuring the ATM Virtual Circuit .....	109
Viewing Your ATM VC .....	109
Adding ATM VCs .....	110
Modifying ATM VCs .....	111
Configuring PPP Interfaces .....	112
Viewing Your Current PPP Configuration .....	112
Modifying and Deleting PPP Interfaces .....	117
Configuring Ethernet-over-ATM .....	118
Overview of EOA .....	118
Viewing Your EOA Setup .....	118
Adding EOA Interfaces .....	120
Configuring Internet Protocol-over-ATM .....	122
Viewing Your IPoA Interface Setup .....	122
Config IP Address and Netmask .....	123
Gateway Address .....	123
Adding IPoA Interfaces .....	124
Configuring Bridging .....	126
Overview of Bridges .....	126
When to Use the Bridging Feature .....	127
Defining Bridge Interfaces .....	127
Deleting a Bridge Interface .....	129
Configuring Global Firewall Settings .....	129
Managing the Black List .....	131

Configuring IP Filters & Blocked Protocols .....	133
Configuring IP Filters .....	133
Viewing Your IP Filter Configuration .....	133
Configuring IP Filter Global Settings .....	134
Creating IP Filter Rules .....	136
IP filter rule examples – Example 1 .....	141
IP filter rule examples – Example 2 .....	142
Viewing IP Filter Statistics .....	143
Managing Current IP Filter Sessions .....	143
Blocked Protocols .....	145
Viewing a DSL Line Information .....	147
Administrative Tasks .....	150
Configuring User Names and Passwords .....	150
Creating and Deleting Logins .....	150
Changing Login Passwords .....	152
Viewing System Alarms .....	152
Viewing the Alarm Table .....	153
Upgrading the Software .....	153
Local Image Upgrade .....	153
Remote Image Upgrade .....	155
Using Diagnostics .....	156
Modifying Port Settings .....	157
Appendix A: IP Addresses, Network Maskes, and Subnets .....	159
Network classes .....	160
Subnet masks .....	160
Binary Numbers .....	161
Bits and bytes .....	162
Appendix B: Troubleshooting .....	163
LEDs .....	163
Internet Access .....	163
Configuration Manager Program .....	164
Diagnosing Problem using IP Utilities .....	165
Glossary .....	167
Registering your NetComm Product .....	176
Contact Information .....	176
Legal & Regulatory Information .....	177
Product Warranty .....	178



## Introduction

Congratulations on becoming the owner of the My ADSL Modem. Your LAN (local area network) will now be able to access the Internet using your high-speed ADSL connection. This User Guide will show you how to set up the My ADSL Modem, and how to customize its configuration to get the most out of your new product.

## Package Contents

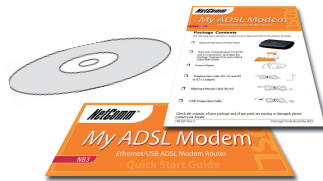
The following items should be contained in your My ADSL Modem Package:



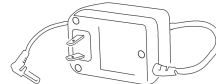
My ADSL Modem (NB3)



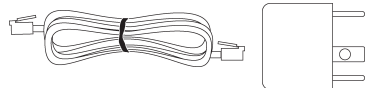
NetComm Communications CD-ROM and Documentation (including a Package Contents Note and a folded Quick Start Guide)



Power Adaptor



Telephone line cable (RJ-11) and 605 to RJ-11 Adaptor



Ethernet Network Cable (RJ-45)



USB Connection Cable



Check the contents of your package and, if any parts are missing or damaged, please contact your Dealer.

## Features

- External ADSL modem for high-speed Internet access
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- Optional USB port for connecting a USB-enabled PC
- Network address translation (NAT), Firewall, and IP filtering functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Relay
- Services including IP route and DNS configuration, RIP, and IP and DSL performance monitoring
- Configuration program you access via an HTML browser

## System Requirements

In order to use the My ADSL Modem, you must have the following:

- ADSL service up and running on your telephone line, with at least one public Internet address for your LAN
- One or more computers each containing an Ethernet 10/100 Base-T network interface card (NIC) and/or a single computer with a USB port.
- An Ethernet hub/switch, if you are connecting the device to more than one computer on an Ethernet network.
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer V5.0 or later, or Netscape V6.1 or later

## Using this Document

### Notational conventions

Acronyms are defined the first time they appear in text and in the Glossary.

For brevity, the My ADSL Modem is referred to as the device.

The terms LAN and network are used interchangeably to refer to a group of Ethernet-connected computers at one site.

### Typographical conventions

*Italics* are used to identify terms that are defined in the Glossary.

**Bold text** is used for items you select from menus and drop-down lists, and text strings you type when prompted by the program.

---

## Special messages

This document uses the following statement to call your attention to specific instructions or explanations.

**Note :**                *Provides clarifying or non-essential information on the current topic.*

**Definition :**       *Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.*

**Warning :**          ***Provides messages of high importance, including messages relating to personal safety or system integrity.***

<p><b>NOTE:</b>                <i>NetComm Technical Support for this product only covers the basic installation and features outlined in Option 1 and Option 2 of the Quick Start Guide.</i></p>
--

## Getting to Know the My ADSL Modem

### Front Panel

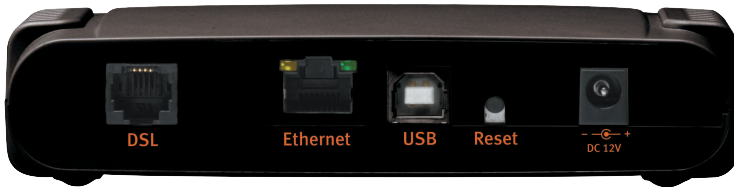
The front panel contains lights called LEDs that indicate the status of the unit.



LED	COLOR	FUNCTION
PW (Power)	Green	On: Unit is powered on Off: Unit is powered off
LK (Link)	Green	Flashes when ADSL data activity occurs. May appear solid when data traffic is heavy.

## Rear Panel

The rear panel contains the ports for the unit's data and power connections.



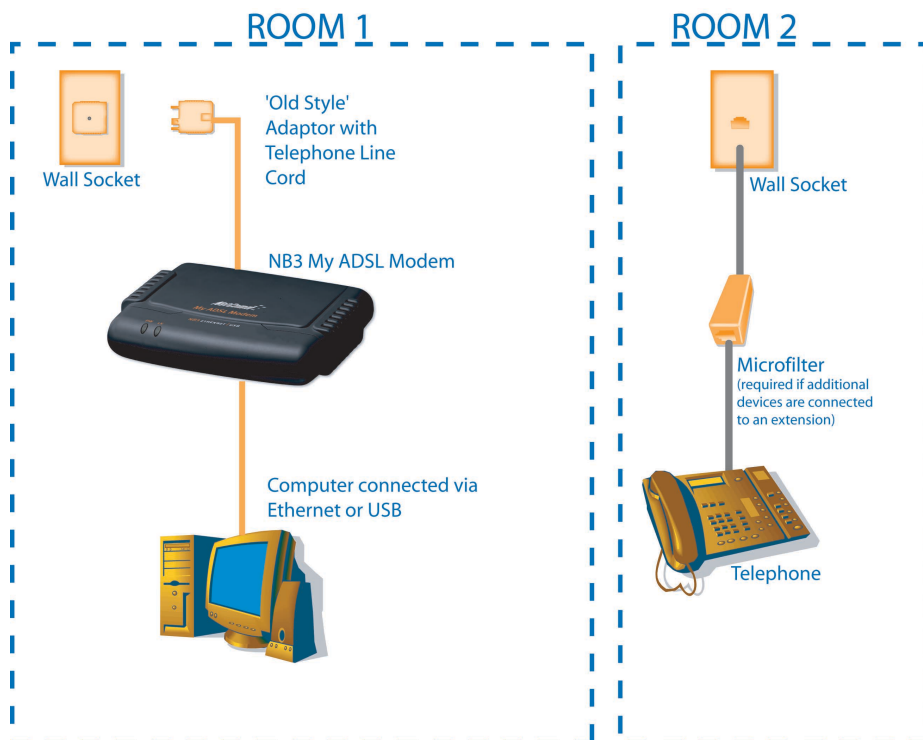
<b>LABEL</b>	<b>FUNCTION</b>
DSL	Connects the device to a telephone jack for DSL communication
Ethernet	Connects the device to your PC's Ethernet port, or to the uplink port on your LAN's hub, using the cable provided  Yellow LED: On: 10M LAN link established and active Off: No 10M LAN link  Green LED: On: 100M LAN link established and active Off: No 100M LAN link
USB	Connects to the USB port on your PC
Reset	Resets the device to the factory default configuration
Power	Connects to the supplied power converter cable

## Do I need a Micro filter?

Micro filters are used to prevent common telephone equipment, such as phones, answering machines and fax machines, from interfering with your ADSL service. If your ADSL enabled phone line is being used with any other equipment other than your ADSL Modem then you will need to use one Micro filter for each phone device.

Splitters may be installed when your ADSL line is installed or when your current phone line is upgraded to ADSL. If your telephone line is already split you will not need to use a Microfilter - check with your ADSL service provider if you are unsure.

Each micro filter is connected in-line with your telephone or fax machine so that all signals pass through it. Telephones and/or facsimiles in other rooms that are using the same extension will also require Microfilters. The following diagram gives an example of connecting your ADSL Modem/Router using a Microfilter.



## Quick Start

---

This Quick Start provides basic instructions for connecting the My ADSL Modem to a computer and to the Internet.

- **Step 1** - describes setting up the hardware.
- **Step 2** - describes how to configure Internet properties on your computer(s).
- **Step 3** - shows you how to configure basic settings on the My ADSL Modem to get your LAN connected to the Internet.

This Quick Start assumes that you have already established an ADSL service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters in this User Guide for advanced configuration instructions.

**NOTE:** *NetComm Technical Support for this product only covers the basic installation and features outlined in Option 1 and Option 2 of the Quick Start Guide.*

The NetComm NB3 My ADSL Modem can be connected directly to your computer via a USB or Ethernet interface.

### How do I choose the connection type?

**Option 1: PREFERRED**

If your computer has a network card (NIC) but isn't connected to a network hub or switch, or another computer, then connect the NB3 to your network port of your PC. This is the preferred connection method. **Follow the step-by-step instructions in the ETHERNET INSTALLATION section.**

**Option2:**

If your computer doesn't have a network card, then connect the NB3 to a USB port (Windows® 98/Me/2000/XP only). **Follow the step-by-step instructions in the USB INSTALLATION section.**

**Option 3:**

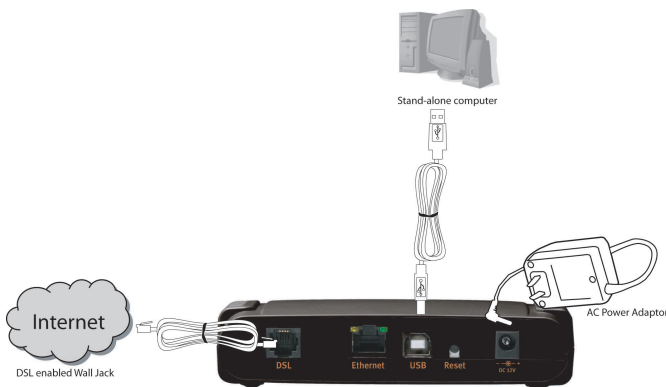
If your computer has a network card (NIC) and is connected to a network hub or switch, then connect the NB3 to your network port of your hub or switch. **Follow the step-by-step instructions in the LAN INSTALLATION section.**

**Warning:** *Before you begin, turn the power off for all devices. These include your computer(s) and the My ADSL Modem.*

## USB Configuration

### Step 1 - Hardware Installation - USB

When connecting your My ADSL Modem using a USB cable, please refer to the appropriate USB diagram and follow the complete driver installation instructions for your operating in Step 2 - Computer Configuration - USB.



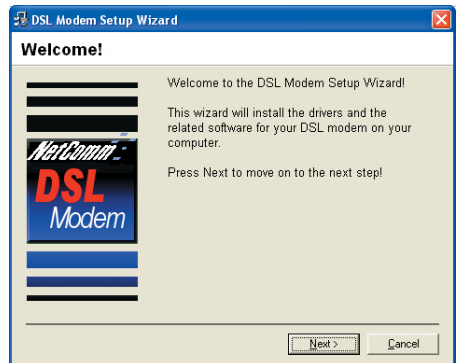
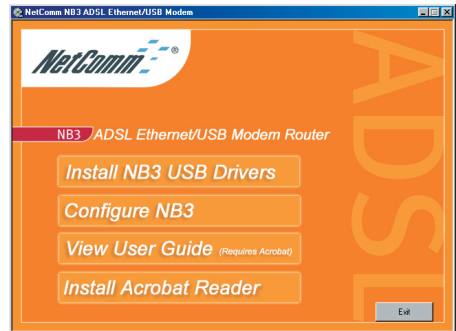
**Note:** *When connecting your My ADSL Modem with a USB cable, the USB cable should not be connected until the driver installation requests it. Refer to the appropriate operating system instructions for USB Configuration.*



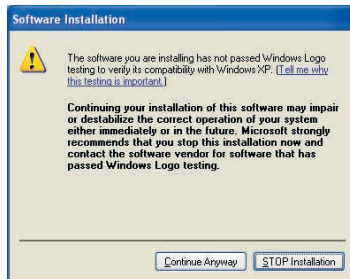
## Step 2 - Computer Configuration - USB

### Windows XP - USB

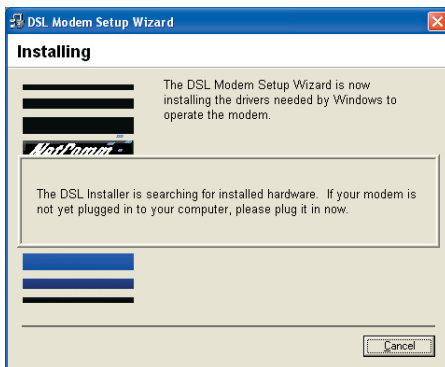
1. Plug in the supplied plug pack and turn power point on.
2. Connect USB Cable to a USB port on your PC but do not connect it to the modem yet.
3. Start PC and log in if not already started.
4. Insert the NetComm NB 3 CD into your CD drive.
5. The NB3 ADSL Ethernet/USB Modem autorun screen will appear. Click on **Install NB3 USB Drivers**.
6. The DSL Modem Setup Wizard will then start. Click on **Next>** to continue .
7. Click on **Accept** to agree to the License Agreement and continue the installation.
8. When prompted by the Found New Hardware Wizard click on **Next>**. Windows will locate the USB device driver and copy the required files to your PC.



9. Click on **Continue Anyway**.



10. Connect the USB cable to the modem.



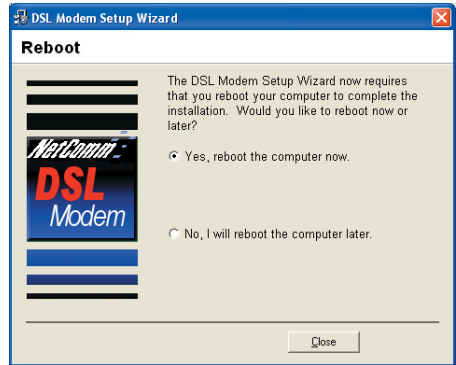
11. When prompted by the Found New Hardware Wizard confirm that “**Install the software automatically (Recommended)**” is selected and click on **Next>**.



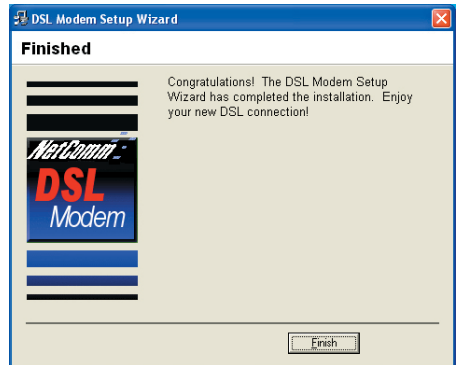
12. Click on **Continue Anyway**. Windows will locate the NetComm USB IAD LAN Modem driver and copy the required files to your PC.



13. When prompted, select **Yes**, reboot the computer now and click on **Close**.

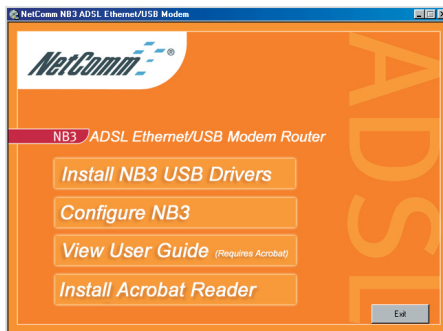


14. After rebooting the DSL Modem Setup Wizard will complete the installation. Click on **Finish**.

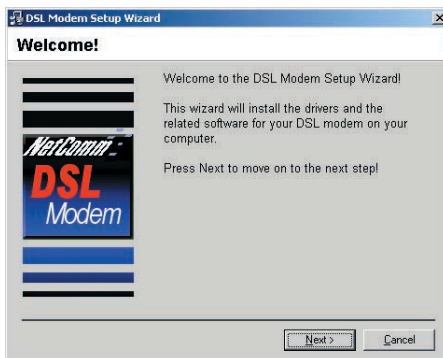


## Windows 2000 - USB

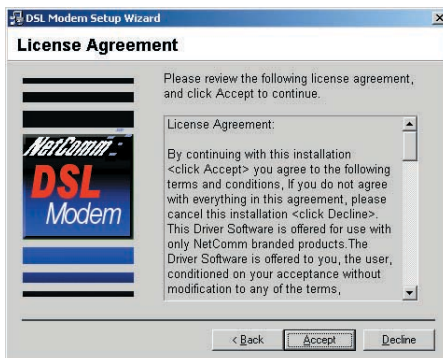
1. Plug in the supplied plug pack and turn power point on.
2. Connect USB Cable to a USB port on your PC, but do not connect it to the modem yet.
3. Start PC and log in if not already started.
4. Insert the NetComm NB 3 CD into your CD drive.
5. The NB3 ADSL Ethernet/USB Modem autorun screen will appear. Click on **“Install NB3 USB Drivers”**.



6. The DSL Modem Setup Wizard will then start. Click on **Next>** to continue.



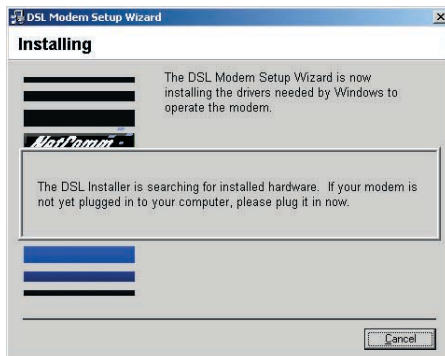
7. Click on **Accept** to agree to the License Agreement and continue the installation.



8. Click **Yes** to continue.



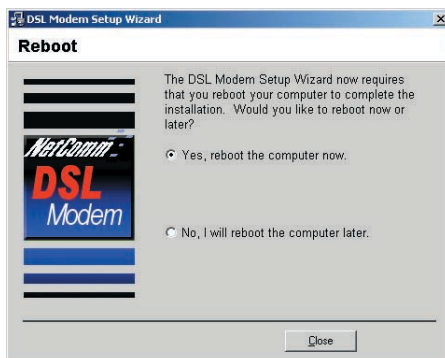
9. Connect the USB cable to the modem.  
The driver files required to operate the ADSL modem will be copied to your system.



10. Click **Yes** to continue.

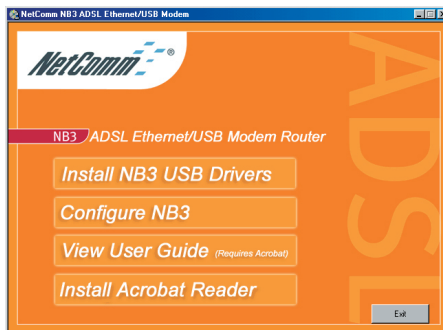


11. When prompted select **Yes**, reboot the computer now and click on **Close**.
12. After rebooting the DSL Modem Setup Wizard will complete the installation. Click on **Finish**.

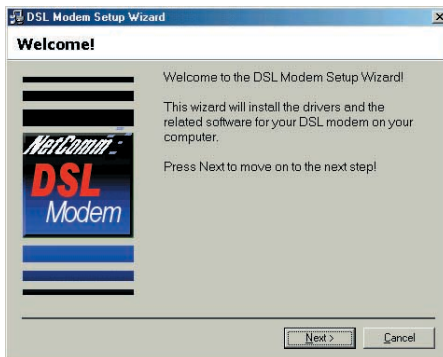


## Windows Me - USB

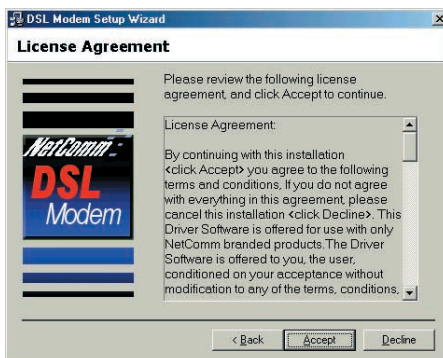
1. Plug in the supplied plug pack and turn power point on.
2. Connect USB Cable to a USB port on your PC, but do not connect it to the Modem yet.
3. Start PC and log in if not already started.
4. Insert the NetComm NB 3 CD into your CD drive.
5. The NB3 ADSL Ethernet/USB Modem autorun screen will appear. Click on “**Install NB3 USB Drivers**”.



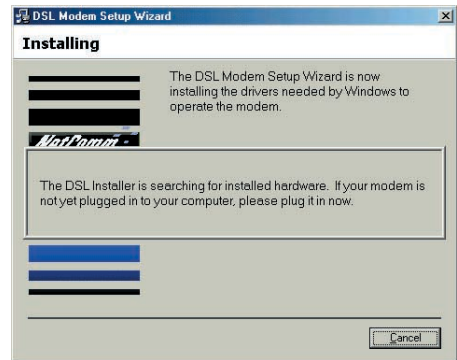
6. The DSL Modem Setup Wizard will then start. Click on **Next>** to continue.



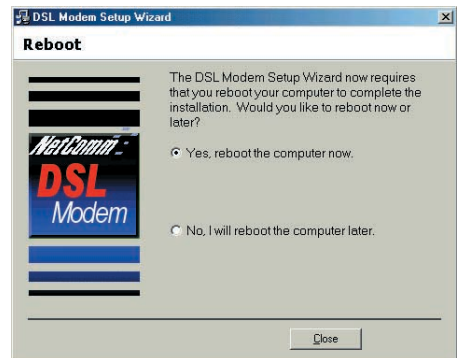
7. Click on **Accept** to agree to the License Agreement and continue the installation.



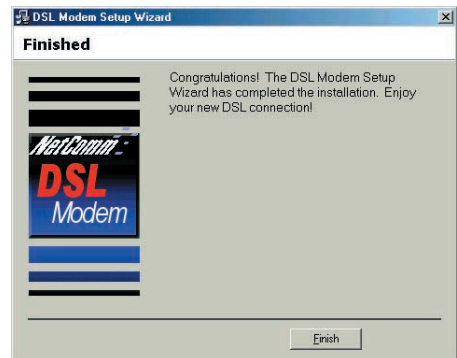
8. Connect the USB cable to the modem.  
The driver files required to operate the ADSL modem will be copied to your system.



9. When prompted select **Yes**, reboot the computer now and click on **Close**.

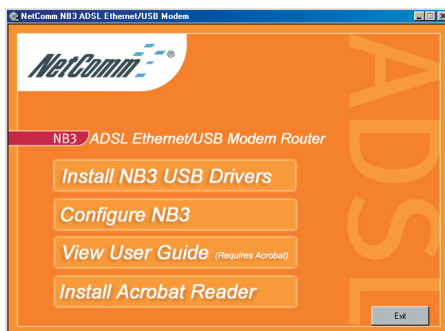


10. After rebooting the DSL Modem Setup Wizard will complete the installation. Click on **Finish**.

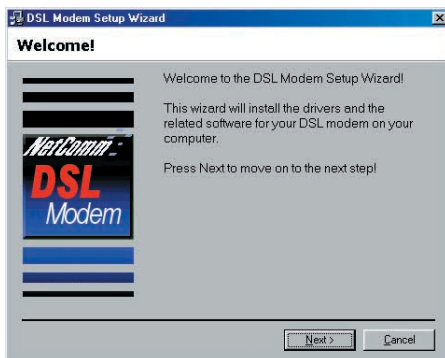


## Windows 98 - USB

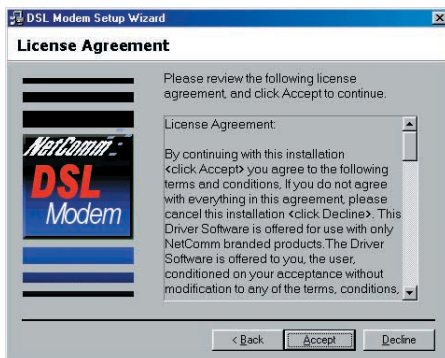
1. Plug in the supplied plug pack and turn power point on.
2. Connect USB Cable to a USB port on your PC, but do not connect it to the Modem yet.
3. Start PC and log in if not already started.
4. Insert the NetComm NB 3 CD into your CD drive.
5. The NB3 ADSL Ethernet/USB Modem autorun screen will appear. Click on “**Install NB3 USB Drivers**”.



6. The DSL Modem Setup Wizard will then start. Click on **Next>** to continue.

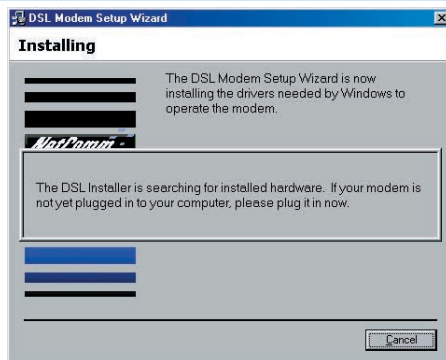


7. Click on **Accept** to agree to the License Agreement and continue the installation.

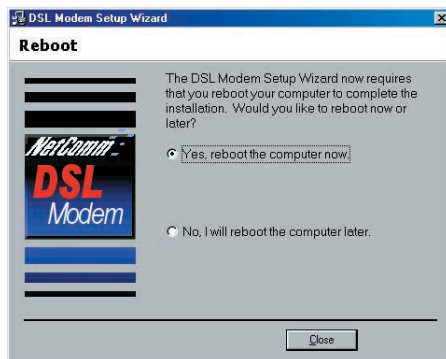




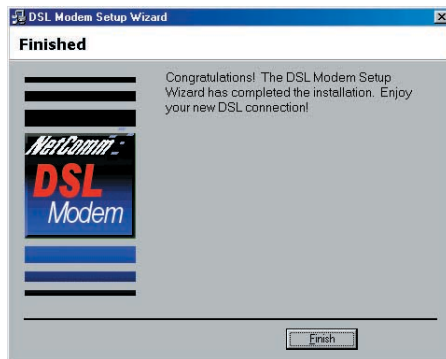
8. Connect the USB cable to the modem.  
The driver files required to operate the ADSL modem will be copied to your system.



9. When prompted select **Yes**, reboot the computer now and click on **Close**.



10. After rebooting the DSL Modem Setup Wizard will complete the installation. Click on **Finish**.



*Note:* USB configuration is not available for Macintosh systems.

## Step 3 - Modem Configuration - USB

In Step 3, you log directly into My ADSL Modem and configure basic settings for your Internet connection. Your ISP should provide you with the necessary information to complete this step.

The settings that you most likely need to change before using the device are grouped onto a single Quick Configuration page.

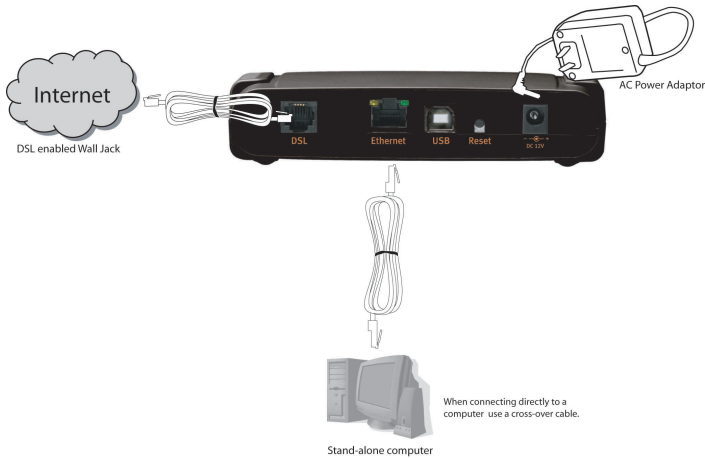
### Logging in to your My ADSL Modem Quick Configuration Page

1. Insert the NetComm NB 3 CD into your CD drive. The NB3 My ADSL Modem autorun screen will appear. Click on **Configure NB3**.
2. The login page will be displayed. Enter the username and password.  
The default username is **root**  
The default password is **root**.  
Click on OK
3. The configuration page will be displayed.
4. Under the PPP heading, enter the username and password that your ISP has provided, scroll to the bottom of the screen and click on **Submit**.
5. To save these settings you now need to click on the Admin tab & select **Commit & Reboot**.
6. Click on **Commit** to save the settings.
7. You should now be able to access the Internet with a web browser, email client or other Internet application.

## Ethernet Configuration

### Step 1 - Hardware Installation - Ethernet

If you are connecting your modem using the ethernet cable, follow the step by step instruction.



#### 1. Connecting the ADSL cable.

Connect one end of the provided phone cable to the port labeled ADSL on the Rear Panel of the device. Connect the other end to your wall phone jack.

#### 2. Connecting the Ethernet cable.

Connect one end of the ethernet cable to the network port on your PC and the other end of the cable to the ethernet port of the My ADSL Modem.

#### 3. Attach the power connector.

Connect the AC power adapter to the Power connector on the back of the device and plug in the adapter to a wall outlet or power strip.

#### 4. Power up your systems.

Turn on and boot up your computer.

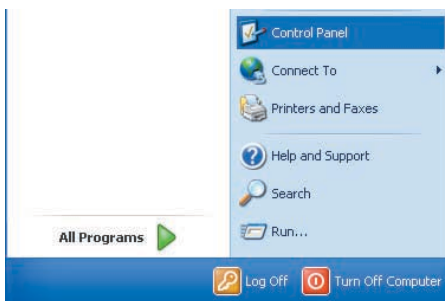
After completing the above, refer to the appropriate operating system section to configure your computer.

## Step 2 - Computer Configuration - Ethernet

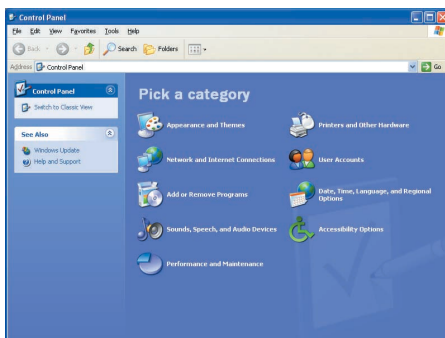
Step 2 of the Quick Start provides instructions for configuring the Internet settings on your computer to work with the My ADSL Modem.

### Windows® XP PCs

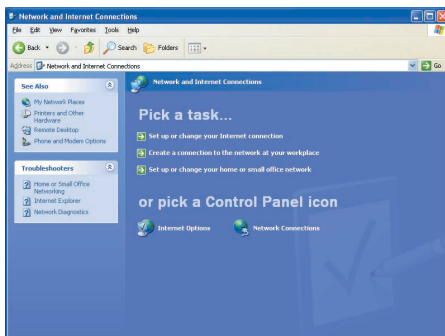
1. In the Windows task bar, click the **Start** button, and then click **Control Panel**.



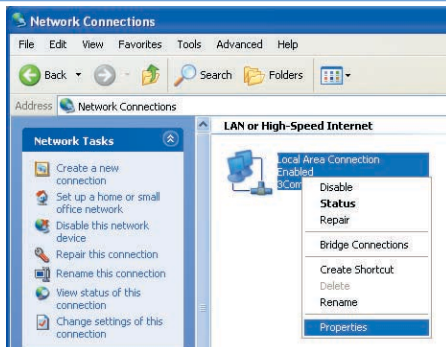
2. Click on **Network & Internet Connections** icon. (Category mode only).



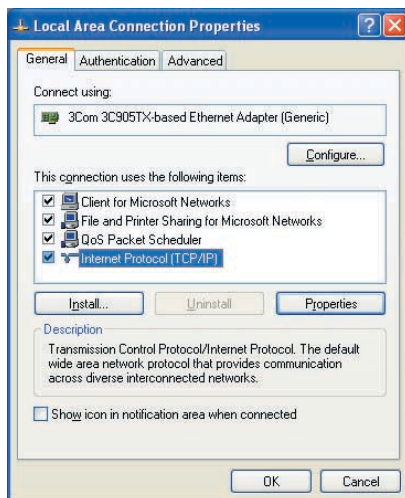
3. Click the **Network Connections** icon.



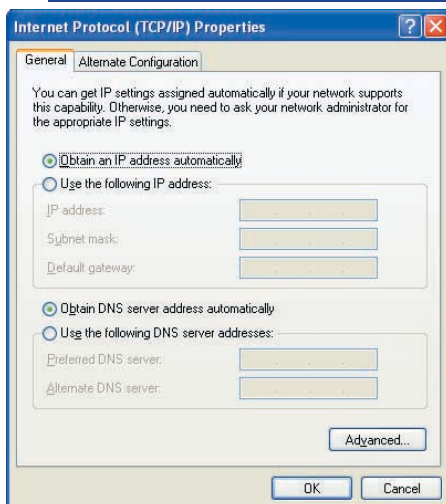
- In the LAN or High-Speed Internet window, right-click on the icon corresponding to your network interface card (NIC) and select **Properties**. (Often, this icon is labeled **Local Area Connection**).



- The Local Area Connection dialog box displays with a list of currently installed network items. Ensure that the check box to the left of the item labeled **Internet Protocol (TCP/IP)** is checked. Select **Internet Protocol TCP/IP** and click on **Properties**.



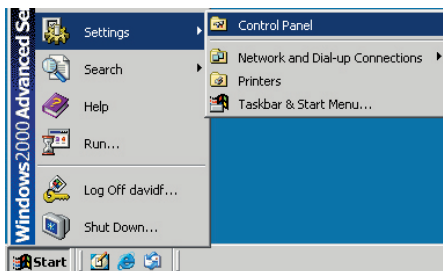
- In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
- Click **OK** twice to confirm your changes, and close the **Control Panel**.



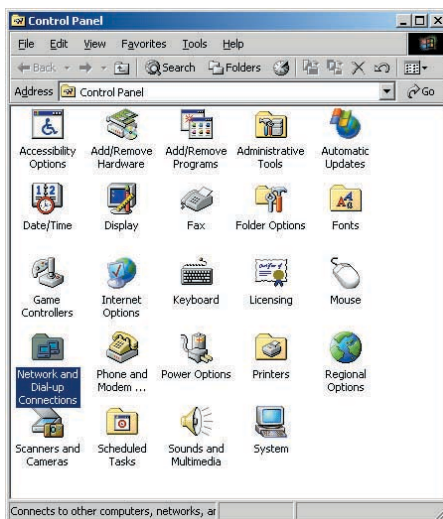
## Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

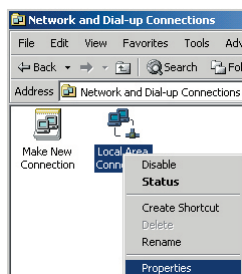
1. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.



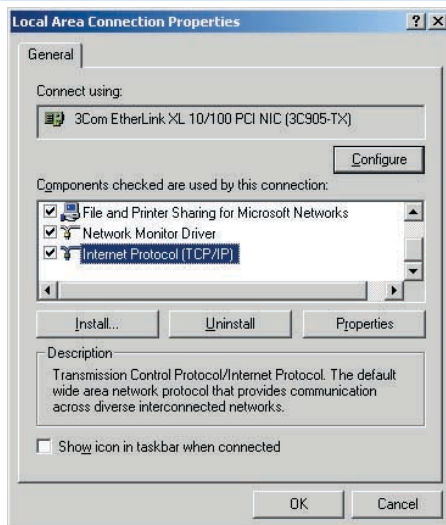
2. Double-click the **Network and Dial-up Connections** icon.



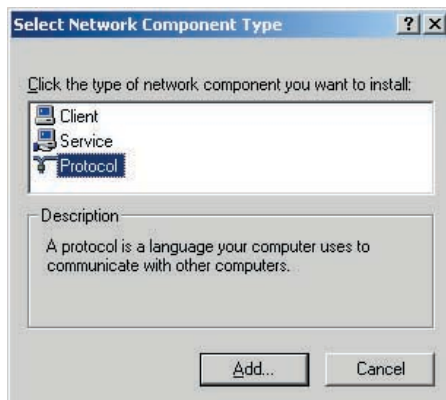
3. In the **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.



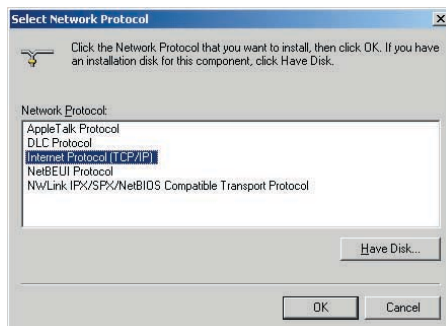
4. The **Local Area Connection Properties** dialog box displays with a list of currently installed network components. If the list includes **Internet Protocol (TCP/IP)**, then the *protocol* has already been enabled. Skip to step 11.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Install**.



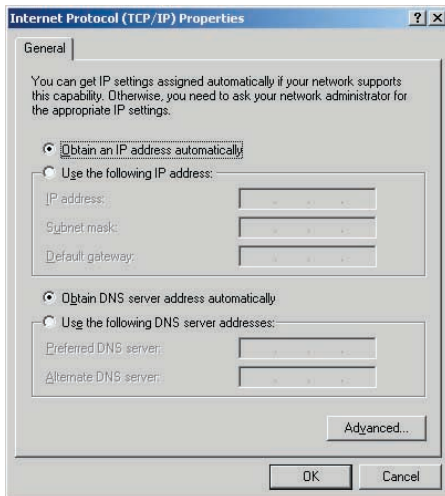
6. In the **Select Network Component Type** dialog box, select Protocol, and then click **Add...**



7. Select Internet Protocol (TCP/IP) in the **Network Protocols** list, and then click **OK**. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
8. If prompted, click **OK** to restart your computer with the new settings.



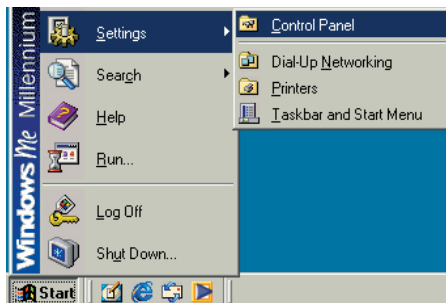
9. Next, configure the PCs to accept IP information assigned by the My ADSL Modem:
10. Follow steps 1 – 3 above.
11. In the **Local Area Connection Properties** dialog box, select Internet Protocol (TCP/IP), and then click Properties
12. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the radio button labeled Obtain an IP address automatically. Also click the radio button labeled Obtain DNS server address automatically.
13. Click **OK** twice to confirm and save your changes, and then close the **Control Panel**.



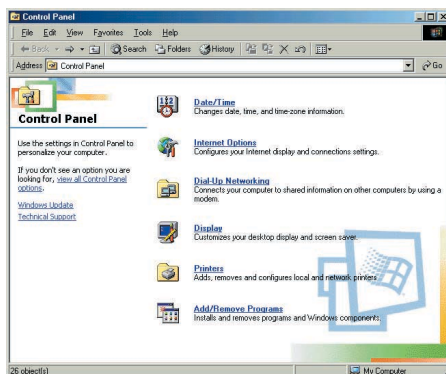


## Windows ME PCs

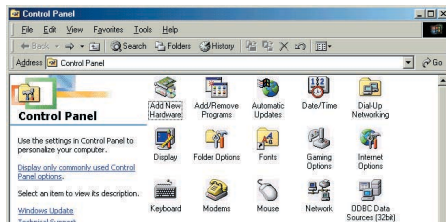
1. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.



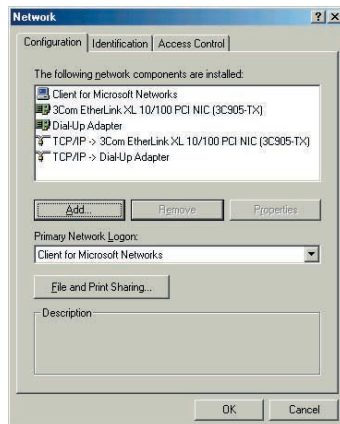
2. Click on **View All Control Panel Options**.



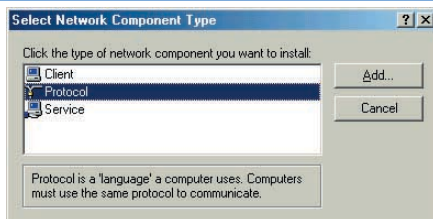
3. Double-click the **Network** icon.



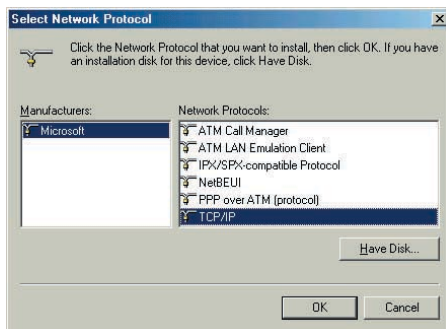
4. The **Network Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add...**



6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add...**

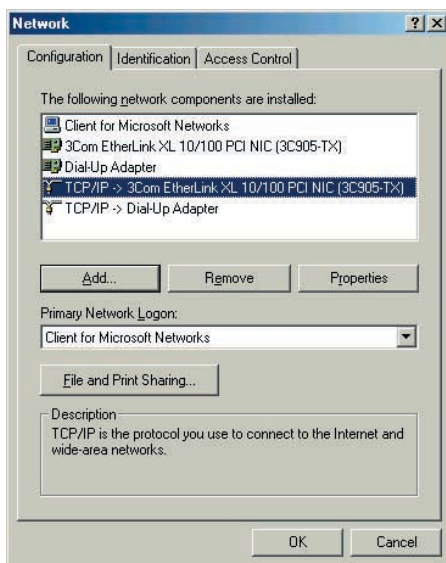


7. Select Microsoft in the **Manufacturers** box.
8. Select Internet Protocol (TCP/IP) in the **Network Protocols** list, and then click **OK**. You may be prompted to install files from your Windows ME installation CD or other media. Follow the instructions to install the files. If prompted, click **OK** to restart your computer with the new settings.

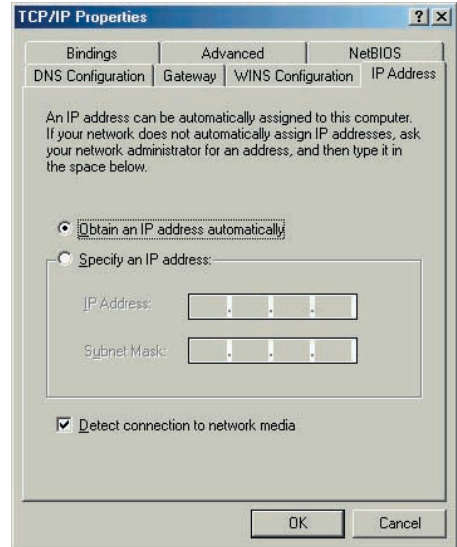


Next, configure the PC to accept IP information assigned by the My ADSL Modem:

9. Follow steps 1 – 4 above..
10. In the **Network Properties** dialog box, select TCP/IP, and then click Properties. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.



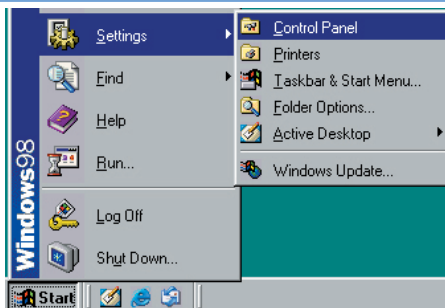
11. In the **TCP/IP Settings** dialog box, click the radio button labeled **Obtain an IP address automatically**.
12. Click **OK** twice to confirm and save your changes, and then close the **Control Panel**.



## Windows 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

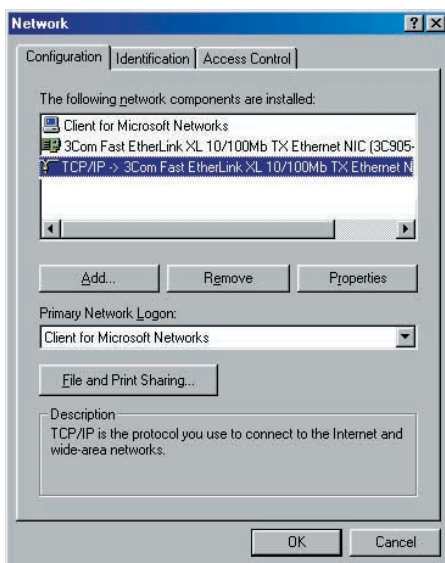
1. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.



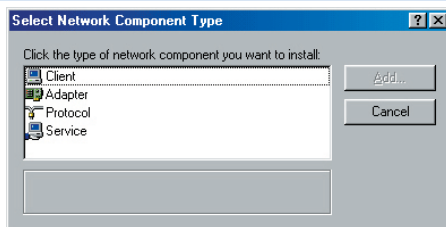
2. Double-click the **Network** icon.



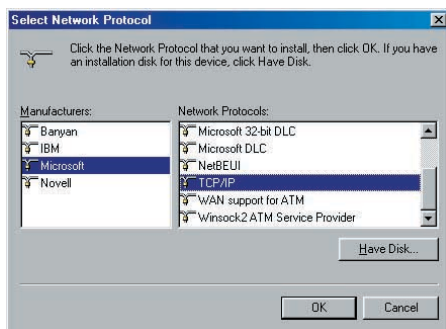
3. The **Network** dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.
4. If TCP/IP does not display as an installed component, click Add... The **Select Network Component Type** dialog box displays.



5. Select Protocol, and then click Add... The **Select Network Protocol** dialog box displays.

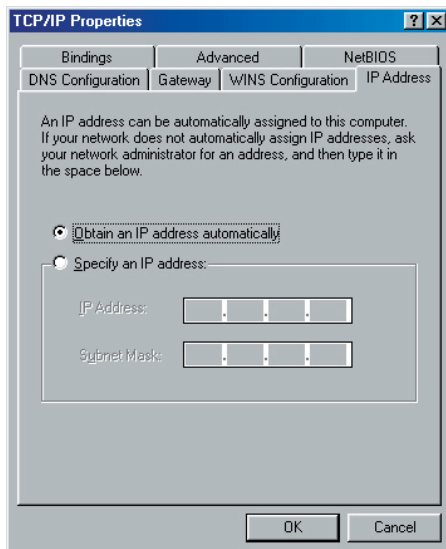


6. Click on Microsoft in the **Manufacturers** list box, and then click TCP/IP in the **Network Protocols** list box.
7. Click **OK** to return to the **Network** dialog box, and then click **OK** again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
8. Click **OK** to restart the PC and complete the TCP/IP installation.



Next, configure the PCs to accept IP information assigned by the My ADSL Modem:

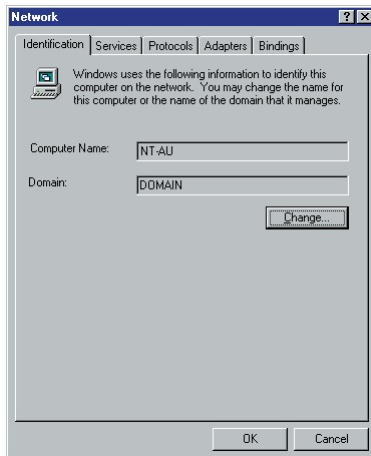
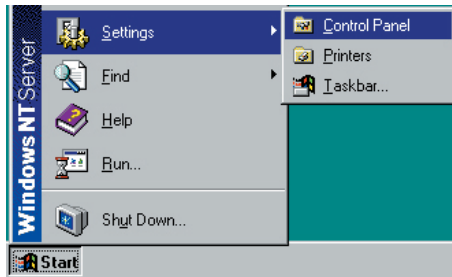
9. Follow steps 1 – 3 above.
10. Select the network component labeled **TCP/IP**, and then click **Properties**. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
11. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.
12. Click the radio button labeled **Obtain an IP address automatically**.
13. Click **OK** twice to confirm and save your changes. You will be prompted to restart Windows.
14. Click **Yes**.



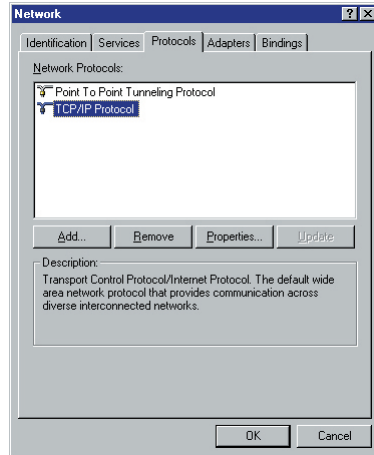
## Windows NT 4.0 workstations

First, check for the IP protocol and, if necessary, install it:

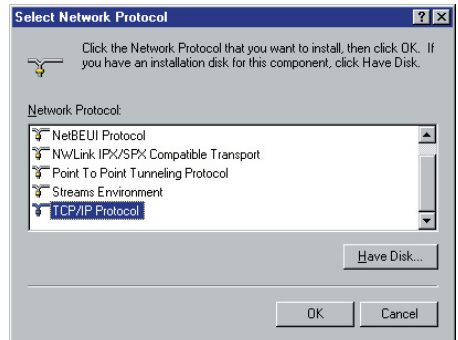
1. In the Windows NT task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. In the **Control Panel** window, double click the **Network** icon.
3. In the **Network** dialog box, click the **Protocols** tab.



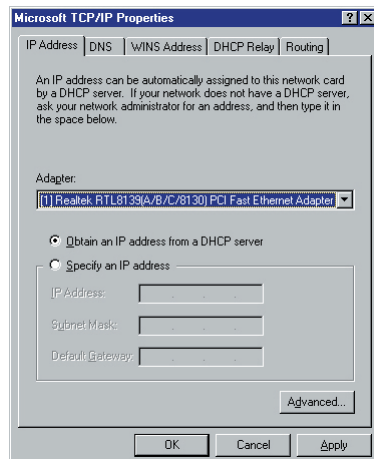
4. The **Protocols** tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 8.
5. If TCP/IP does not display as an installed component, click **Add...**



6. In the **Select Network Protocol** dialog box, select **TCP/IP**, and then click **OK**.
7. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.  
After all files are installed, a window displays to inform you that a TCP/IP service called *DHCP* can be set up to dynamically assign IP information.
8. Click **Yes** to continue, and then click **OK** if prompted to restart your computer. Next, configure the PCs to accept IP information assigned by the My ADSL Modem:

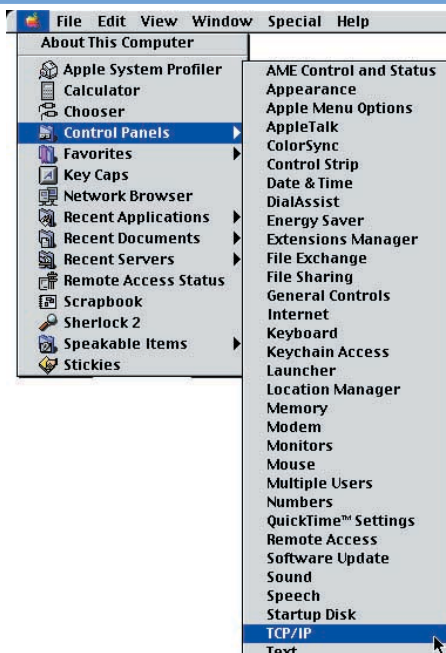


9. Follow steps 1 – 3 above.
10. In the **Protocols** tab, select **TCP/IP**, and then click **Properties**.
11. In the **Microsoft TCP/IP Properties** dialog box, click the radio button labeled **Obtain an IP address from a DHCP server**.
12. Click **OK** twice to confirm and save your changes, and then close the **Control Panel**.

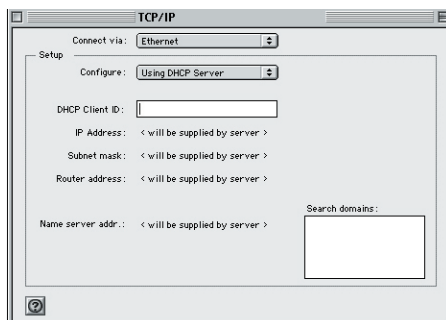


## Mac OS 9.x

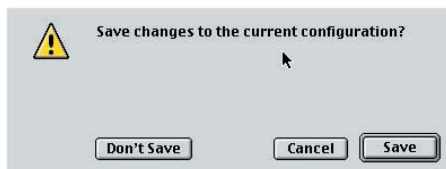
1. Click on the Apple in the toolbar, select **Control Panels**, and then click on **TCP/IP**.



2. Choose **Connect: via Ethernet** and **Configure: Using DHCP Server**.



3. Close the TCP/IP configuration box and save the changes.





## Mac OS X

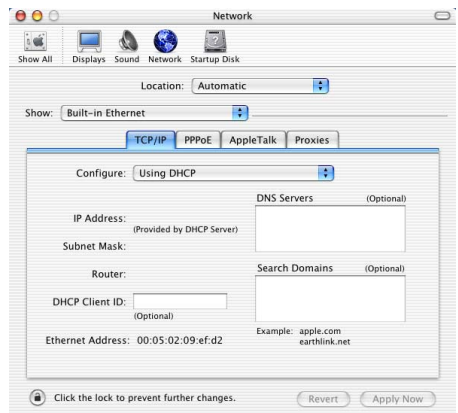
1. On the Dock, click on **System Preferences**.



2. Click on **Network**.



3. Confirm that **Built in Ethernet** is selected. From the TCP/IP tab select **Configure: Using DHCP**. Click on **Apply Now** to save any changes and exit from the System Preferences.



## Step 3 - Modem Configuration - Ethernet

In Step 3, you log into the program on the My ADSL Modem and configure basic settings for your Internet connection. Your ISP should provide you with the necessary information to complete this step.

The My ADSL Modem provides a preinstalled software program called Configuration Manager which enables you to configure the operation of the device via your Web browser. The settings that you most likely need to change before using the device are grouped onto a single Quick Configuration page.

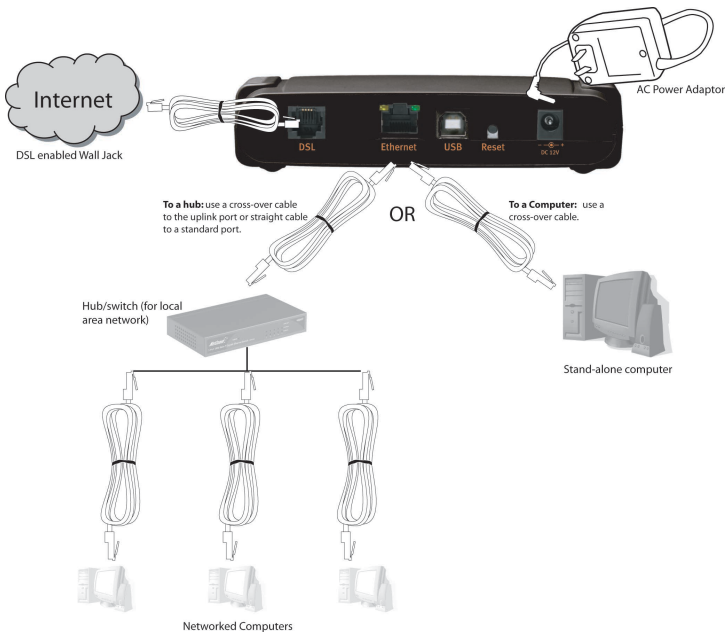
### Logging in to your My ADSL Modem Quick Configuration Page

1. Insert the NetComm NB 3 CD into your CD drive. The NB3 My ADSL Modem autorun screen will appear. Click on **Configure NB3**.
2. The logon page will be displayed. Enter the username and password.  
The default username is **root**  
The default password is **root**.  
Click on OK
3. The configuration page will be displayed.
4. Under the PPP heading, enter the username and password that your ISP has provided, scroll to the bottom of the screen and click on **Submit**.
5. To save these settings you now need to click on the Admin tab & select **Commit & Reboot**.
6. Click on **Commit** to save the settings.
7. You should now be able to access the Internet with a web browser, email client or other Internet application.

# LAN Configuration

## Step 1 - Hardware Installation - LAN

If you are connecting your modem using the ethernet cable, follow the step by step instruction.



### 1. Connecting the ADSL cable.

Connect one end of the provided phone cable to the port labeled ADSL on the Rear Panel of the device. Connect the other end to your wall phone jack.

### 2. Connecting the Ethernet cable.

Connect one end of the ethernet cable to the ethernet port of the My ADSL Modem and the other end to the network port of a Switch or Hub. Connect the required spare ports of your Switch or Hub to computers with network cards via ethernet cable.

### 3. Attach the power connector.

Connect the AC power adapter to the Power connector on the back of the device and plug in the adapter to a wall outlet or power strip.

### 4. Power up your systems.

Turn on and boot up your computer.

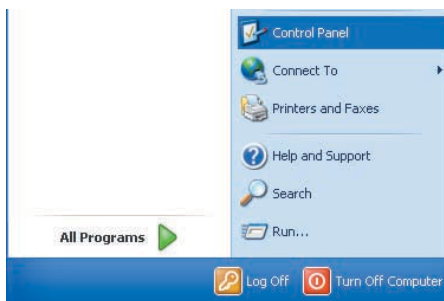
After completing the above, refer to the appropriate operating system section to configure your computer.

## Step 2 - Computer Configuration - LAN

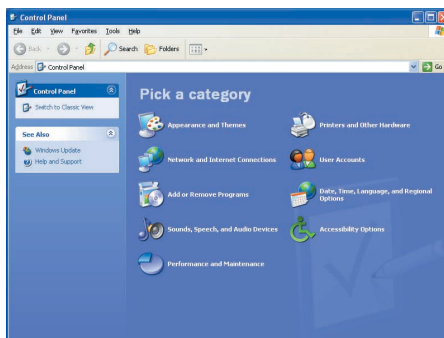
Step 2 of the Quick Start provides instructions for configuring the Internet settings on your computer to work with the My ADSL Modem.

### Windows® XP PCs

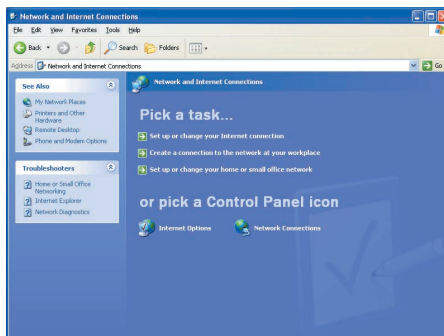
1. In the Windows task bar, click the **Start** button, and then click **Control Panel**.



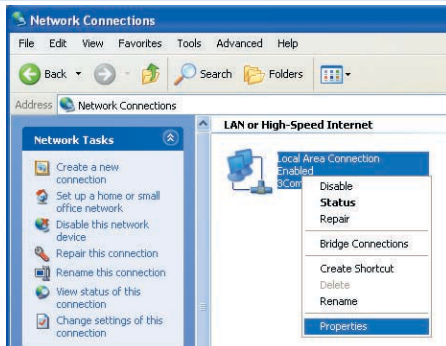
2. Click on **Network & Internet Connections** icon. (Category mode only).



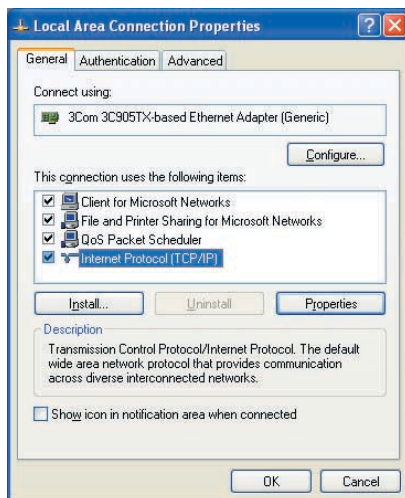
3. Click the **Network Connections** icon.



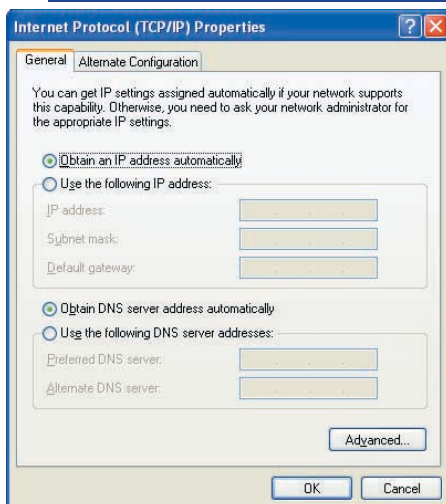
- In the LAN or High-Speed Internet window, right-click on the icon corresponding to your network interface card (NIC) and select **Properties**. (Often, this icon is labeled **Local Area Connection**).



- The Local Area Connection dialog box displays with a list of currently installed network items. Ensure that the check box to the left of the item labeled **Internet Protocol (TCP/IP)** is checked. Select **Internet Protocol TCP/IP** and click on **Properties**.



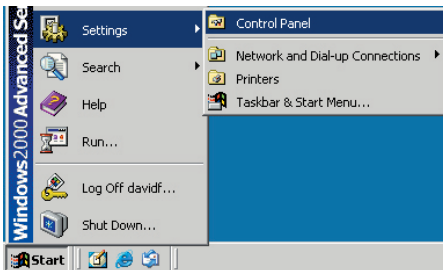
- In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
- Click **OK** twice to confirm your changes, and close the **Control Panel**.



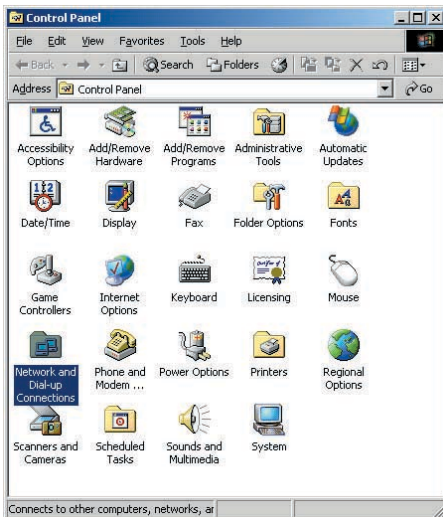
## Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

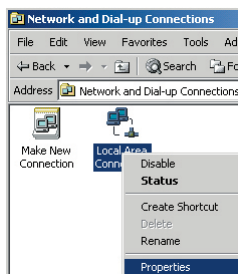
1. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.



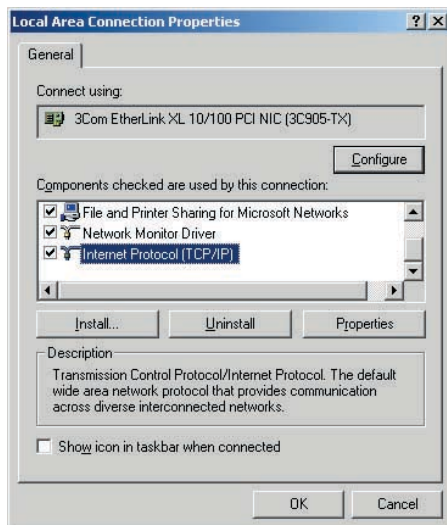
2. Double-click the **Network and Dial-up Connections** icon.



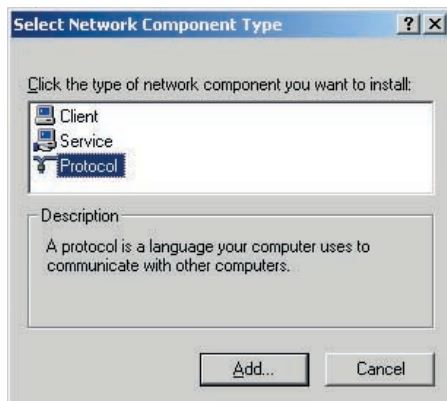
3. In the **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.



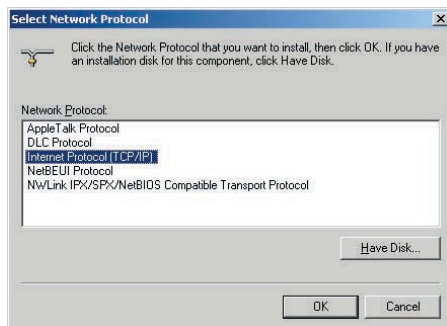
4. The **Local Area Connection Properties** dialog box displays with a list of currently installed network components. If the list includes **Internet Protocol (TCP/IP)**, then the *protocol* has already been enabled. Skip to step 11.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Install**.



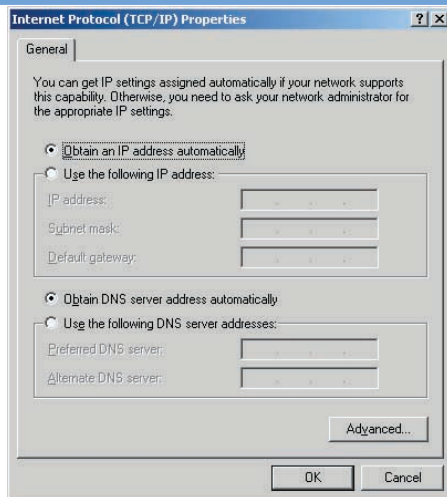
6. In the **Select Network Component Type** dialog box, select Protocol, and then click **Add...**



7. Select Internet Protocol (TCP/IP) in the **Network Protocols** list, and then click **OK**. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
8. If prompted, click **OK** to restart your computer with the new settings.



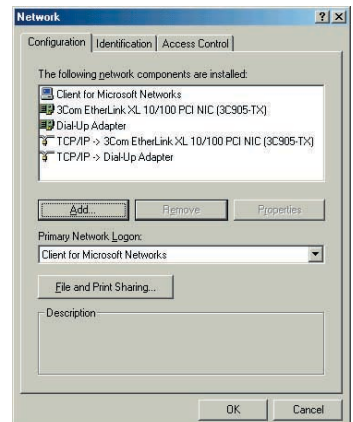
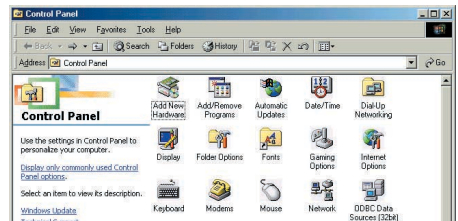
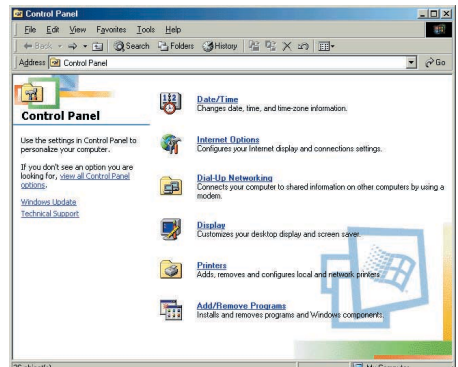
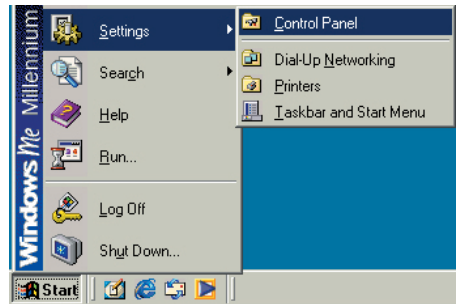
9. Next, configure the PCs to accept IP information assigned by the My ADSL Modem:
10. Follow steps 1 – 3 above.
11. In the **Local Area Connection Properties** dialog box, select Internet Protocol (TCP/IP), and then click Properties
12. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the radio button labeled Obtain an IP address automatically. Also click the radio button labeled Obtain DNS server address automatically.
13. Click **OK** twice to confirm and save your changes, and then close the **Control Panel**.



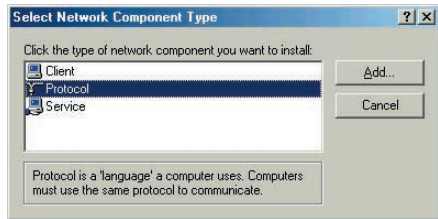


## Windows ME PCs

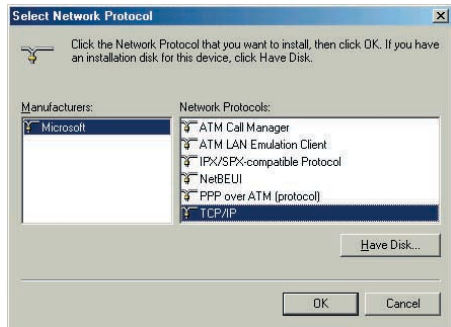
1. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Click on **View All Control Panel Options**.
3. Double-click the **Network** icon.
4. The **Network Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add...**



6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add...**

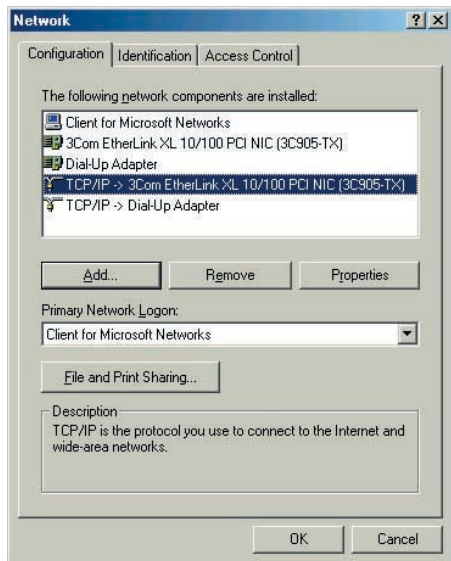


7. Select Microsoft in the **Manufacturers** box.

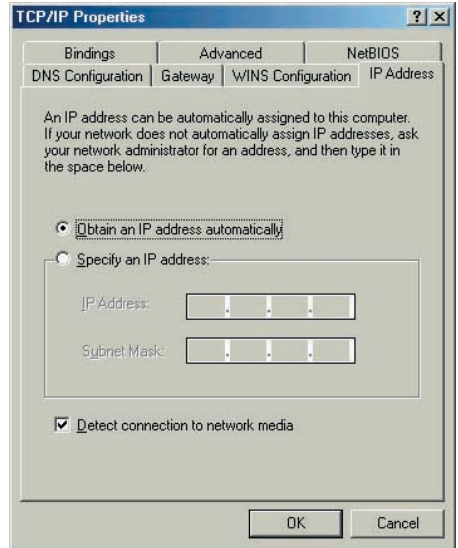


8. Select Internet Protocol (TCP/IP) in the **Network Protocols** list, and then click **OK**. You may be prompted to install files from your Windows ME installation CD or other media. Follow the instructions to install the files. If prompted, click **OK** to restart your computer with the new settings.

Next, configure the PC to accept IP information assigned by the My ADSL Modem:



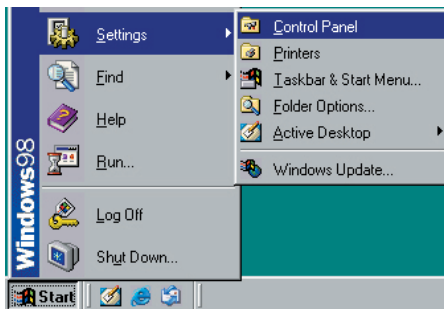
9. Follow steps 1 – 4 above..
10. In the **Network Properties** dialog box, select TCP/IP, and then click Properties. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
11. In the **TCP/IP Settings** dialog box, click the radio button labeled **Obtain an IP address automatically**.
12. Click **OK** twice to confirm and save your changes, and then close the **Control Panel**.



## Windows 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

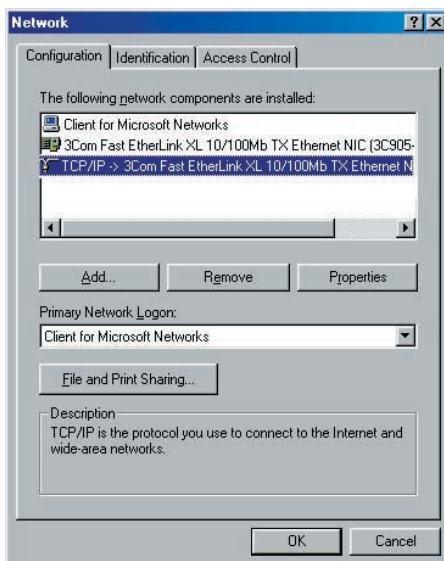
1. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.



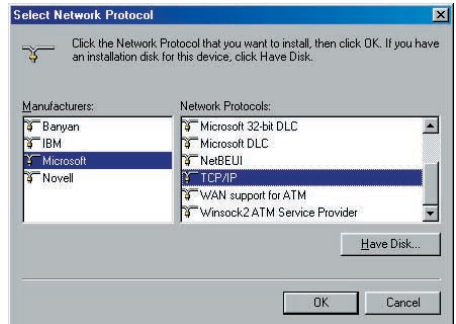
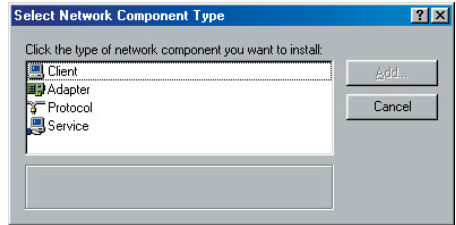
2. Double-click the **Network** icon.



3. The **Network** dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.
4. If TCP/IP does not display as an installed component, click **Add...** The **Select Network Component Type** dialog box displays.

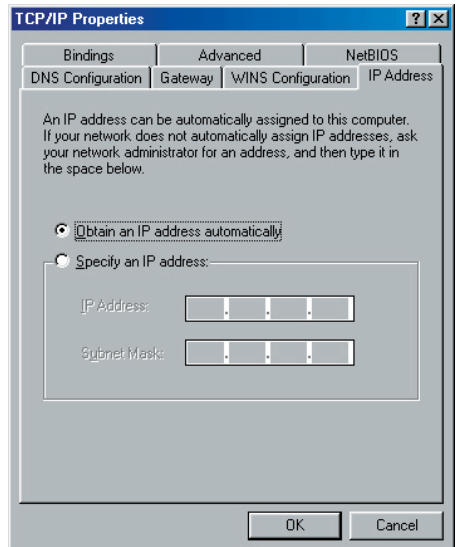


5. Select **Protocol**, and then click **Add...** The **Select Network Protocol** dialog box displays.
6. Click on **Microsoft** in the **Manufacturers** list box, and then click **TCP/IP** in the **Network Protocols** list box.
7. Click **OK** to return to the **Network** dialog box, and then click **OK** again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
8. Click **OK** to restart the PC and complete the TCP/IP installation.



Next, configure the PCs to accept IP information assigned by the My ADSL Modem:

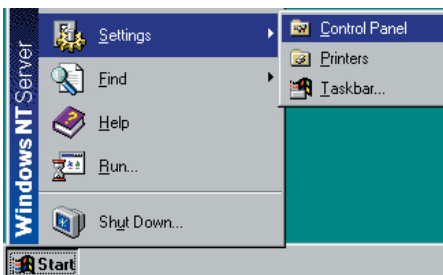
9. Follow steps 1 – 3 above.
10. Select the network component labeled **TCP/IP**, and then click **Properties**. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
11. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.
11. Click the radio button labeled **Obtain an IP address automatically**.
13. Click **OK** twice to confirm and save your changes. You will be prompted to restart Windows.
14. Click **Yes**.



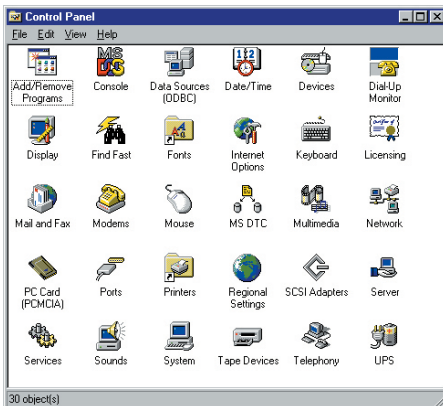
## Windows NT 4.0 workstations

First, check for the IP protocol and, if necessary, install it:

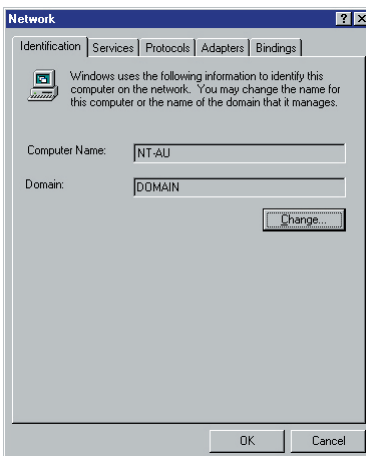
1. In the Windows NT task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.



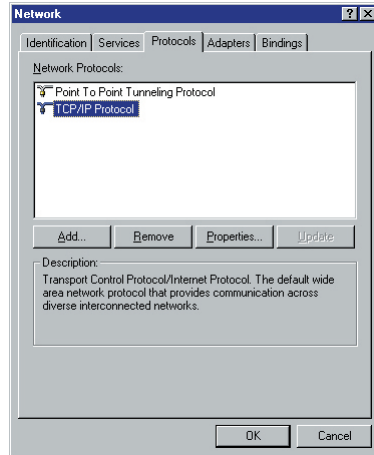
2. In the **Control Panel** window, double click the **Network** icon.



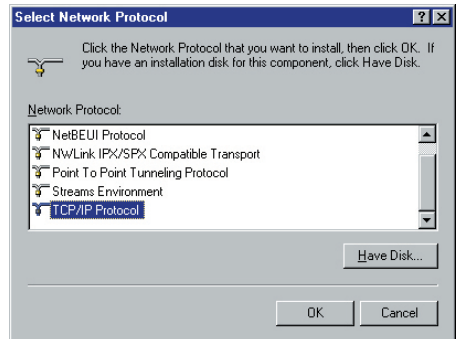
3. In the **Network** dialog box, click the **Protocols** tab.



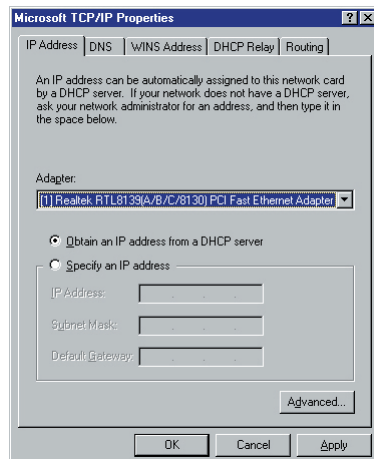
4. The **Protocols** tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 8.
5. If TCP/IP does not display as an installed component, click **Add...**



6. In the **Select Network Protocol** dialog box, select **TCP/IP**, and then click **OK**.
7. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.  
After all files are installed, a window displays to inform you that a TCP/IP service called *DHCP* can be set up to dynamically assign IP information.
8. Click **Yes** to continue, and then click **OK** if prompted to restart your computer. Next, configure the PCs to accept IP information assigned by the My ADSL Modem:

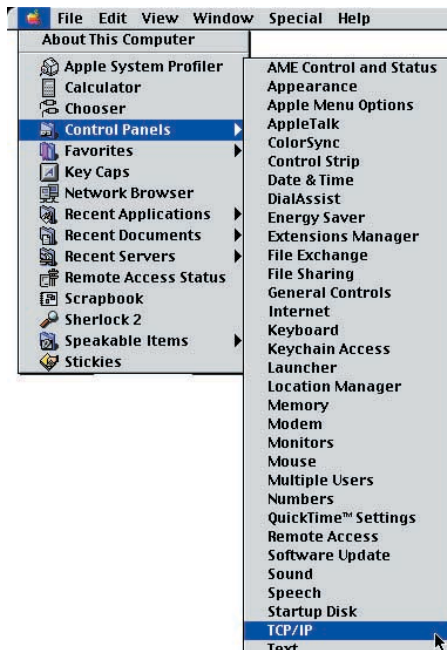


9. Follow steps 1 – 3 above.
10. In the **Protocols** tab, select **TCP/IP**, and then click **Properties**.
11. In the **Microsoft TCP/IP Properties** dialog box, click the radio button labeled **Obtain an IP address from a DHCP server**.
12. Click **OK** twice to confirm and save your changes, and then close the **Control Panel**.

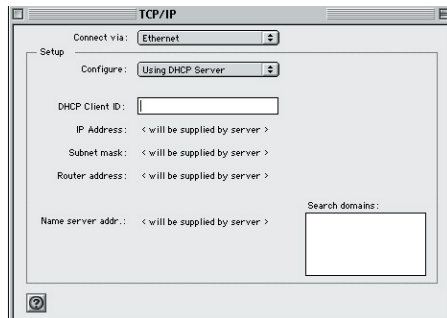


## Mac OS 9.x

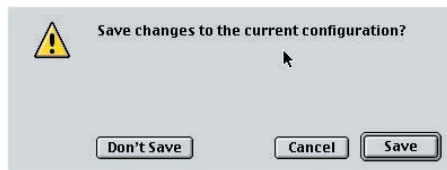
1. Click on the Apple in the toolbar, select **Control Panels**, and then click on **TCP/IP**.



2. Choose **Connect: via Ethernet** and **Configure: Using DHCP Server**.



3. Close the TCP/IP configuration box and save the changes.





## Mac OS X

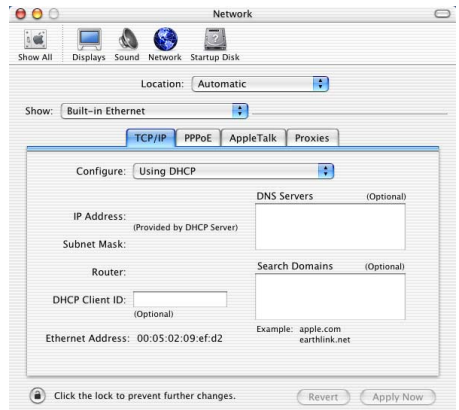
1. On the Dock, click on **System Preferences**.



2. Click on **Network**.



3. Confirm that **Built in Ethernet** is selected. From the TCP/IP tab select **Configure: Using DHCP**. Click on **Apply Now** to save any changes and exit from the System Preferences.



## Step 3 - Modem Configuration - LAN

In Step 3, you log into the program on the My ADSL Modem and configure basic settings for your Internet connection. Your ISP should provide you with the necessary information to complete this step.

The My ADSL Modem provides a preinstalled software program called Configuration Manager which enables you to configure the operation of the device via your Web browser. The settings that you most likely need to change before using the device are grouped onto a single Quick Configuration page.

### Logging in to your My ADSL Modem Quick Configuration Page

1. Insert the NetComm NB 3 CD into your CD drive. The NB3 My ADSL Modem autorun screen will appear. Click on **Configure NB3**.
2. The logon page will be displayed. Enter the username and password.  
The default username is **root**  
The default password is **root**.  
Click on OK
3. The configuration page will be displayed.
4. Under the PPP heading, enter the username and password that your ISP has provided, scroll to the bottom of the screen and click on **Submit**.
5. To save these settings you now need to click on the Admin tab & select **Commit & Reboot**.
6. Click on **Commit** to save the settings.
7. You should now be able to access the Internet with a web browser, email client or other Internet application.

## Assigning static Internet Information to your PCs

In some cases, you may want to assign Internet information to some or all of your PCs directly (often called statically), rather than allowing the My ADSL Modem to assign it. This option may be desirable (but not required) if:

- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- You maintain different subnets on your LAN (subnets are described in IP Addresses, Network Masks, and Subnets).

Before you begin, be sure to have the following information on hand, or contact your ISP if you do not know it:

- The IP address and subnet mask to be assigned to each PC to which you will be assigning static IP information.
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the My ADSL Modem. By default, the LAN port is assigned this IP address: 192.168.1.1. (You can change this number, or another number can be assigned by your ISP. See Configuring the LAN Ports for more information.
- The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the Ethernet Configuration instructions relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server, and default gateway, click the radio buttons that enable you to enter the information manually.

*Note :*                *Your PCs must have IP addresses that place them in the same subnet as the My ADSL Modem's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in Configuring the LAN Ports to change the LAN port IP address accordingly.*

## The My ADSL Modem Quick Configuration Page

You log into the program on the My ADSL Modem and configure basic settings for your Internet connection. Your ISP should provide you with the necessary information to complete this step.

The My ADSL Modem provides a preinstalled software program called Configuration Manager which enables you to configure the operation of the device via your Web browser. The settings that you most likely need to change before using the device are grouped onto a single Quick Configuration page.

1. Insert the NetComm NB 3 CD into your CD drive. The NB3 My ADSL Modem autorun screen will appear. Click on **Configure NB3**.
2. The logon page will be displayed. Enter the username and password.  
The default username is **root**  
The default password is **root**.  
Click on OK
3. The configuration page will be displayed.

**Figure 2. Quick Configuration Page in Configuration Manager**

4. Under the PPP heading, enter the username and password that your ISP has provided, scroll to the bottom of the screen and click on **Submit**.
5. To save these settings you now need to click on the Admin tab & select **Commit & Reboot**.
6. Click on **Commit** to save the settings.
7. You should now be able to access the Internet with a web browser, email client or other Internet application.

The fields are described in the following table. Work with your ISP to determine which settings you need to change.

<b>FIELD</b>	<b>DESCRIPTION</b>
<b>General Settings</b>	
ATM Interface	Select the ATM interface you want to use (usually atm-0). Your system may be configured with more than one ATM interface if you are using different types of services with your ISP.
Operation Mode	This setting enables or disables the My ADSL Modem. When set to Disabled, the device cannot be used to provide Internet connectivity for your network. Set it to Enabled now, if necessary.
Encapsulation	This setting determines the type of data link your ISP uses to communicate with your My ADSL Modem. Contact them to determine the appropriate setting.
VCI and VPI	These values are provided by your ISP and determine the unique path your connection uses to communicate with your ISP.
Bridge	This setting Enabled or Disabled bridging between the My ADSL Modem and your ISP. Your ISPs may also refer to this as RFC 1483 or Ethernet over ATM.
IGMP	This setting Enabled or Disabled the Internet Group Management Protocol, which some ISPs use to perform remote configuration of your device.
IP Address and Subnet Mask	If your ISP has assigned a public IP address to your LAN, enter the address and the associated subnet mask in the boxes provided. (Note: in some configurations, the public IP address should be entered on your PC rather than on the My ADSL Modem; check with your ISP.)
Use DHCP	To enable or disable DHCP server function.
Default Route	When enabled, this setting specifies that the IP address specified above will be used as the default route for your LAN. Whenever, one of your LAN computers attempts to access the Internet, the data will be sent via the WAN interface.
Gateway IP Address	Specify the IP address that identifies the ISP server through which your Internet connection will be routed.

## PPP

Username and Password

Enter the Username and Password you use to log in to your ISP. (Note: this is not the same as the user name and password you used to log in to Configuration Manager.)

Use DNS

Enable this feature if the DNS server addresses that your LAN will use should be supplied dynamically each time you connect to the ISP. If you click Disable, you must configure DNS addresses manually on each PC or on the fields below.

## DNS

Primary DNS Server  
and Secondary DNS Server

Enter the Primary and Secondary Domain Name System (DNS) server addresses provided by your ISP.

3. When finished customizing these settings, click **Submit**. The settings are now in effect; however, if you reboot or if the power is disconnected, your settings will be lost. In step 4, you save the changes to permanent memory.
4. Click the **Admin** tab that displays in the upper right of the page, and then click **Commit & Reboot** in the task bar.
5. Click **Commit**.

A page will display briefly to confirm your changes, and then you will be returned to the Commit & Reboot page.

You can click **Delete** to remove all existing Quick Configuration settings and return to the default values.

You are now finished customizing basic settings. Read the following section to determine if you need to change additional settings.

## Default My ADSL Modem Settings

In addition to handling the DSL connection to your ISP, the My ADSL Modem can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

Below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review the settings below to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

Before you modifying any settings, review Getting Started with the Configuration Manager using the Configuration Manager program. We strongly recommend that you contact your ISP prior to changing the default configuration.

### **DHCP**

**Default :** DHCP server enabled with the following pool of addresses: 192.168.1.3 through 192.168.1.34

The My ADSL Modem maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in Quick Start. See Configuring Dynamic Host Configuration Protocol for an explanation of the DHCP service.

### **NAT**

**Default :** NAT rule enabled

Your computers' private IP addresses (see DHCP above) will be translated to your public IP address whenever they access the Internet. See Configuring the LAN Ports for a description of the NAT service.

### **LAN Port IP Address**

**Default :** Assigned static IP address: 192.168.1.1  
Subnet mask: 255.255.255.0

This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See Configuring the LAN Ports for instructions.

### **USB Port IP Address**

**Default :** Assigned static IP address: 192.168.1.2  
Subnet mask: 255.255.255.0

This is the IP address assigned to the USB port on the device (if used). Typically, you will not need to change this address. See USB Functionality for instructions.

The My ADSL Modem includes a preinstalled program called the Configuration Manager, which provides an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You access it through your web browser from any PC connected to the My ADSL Modem via the LAN or USB ports.

## Getting Started with the Configuration Manager

This chapter describes how to use the Configuration Manager.

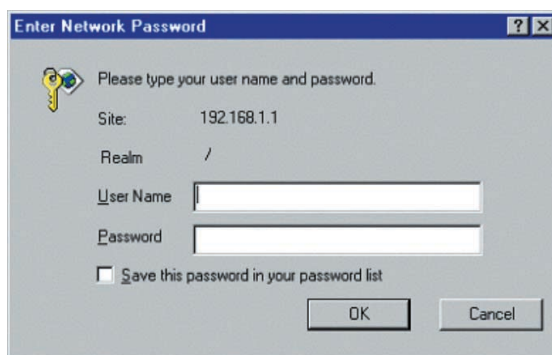
### Accessing the Configuration Manager

The Configuration Manager program is preinstalled into memory on the My ADSL Modem. To access the program, you need the following:

- A PC or laptop connected to the LAN port on the device as described in the Quick Start chapter.
- A web browser installed on the PC. The program is designed to work best with Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 6.1, or later versions.

You can access the program from any computer connected to the My ADSL Modem via the LAN or USB ports.

1. From a LAN computer, open your web browser, type the following URL in the web address (or location) box, and press Enter: `http://192.168.1.1` Or, from the USB computer, type: `http://192.168.1.2` These are the predefined IP addresses for the LAN and USB ports on the My ADSL Modem. A login screen displays, as shown in Figure 3.



**Figure 3. Login Screen**

2. Enter your User Name and Password, and then click OK. The first time you log into the program, use these defaults:

Default User Name : root

Default Password : root

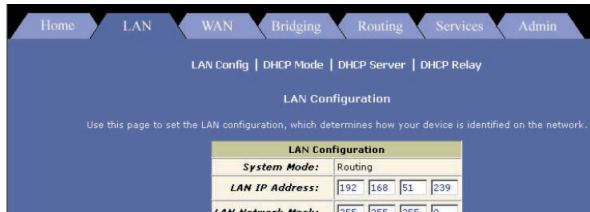
**Note :** *You can change the password at any time (See Configuring User Names and Passwords for instructions).*

The System View page on the Home tab displays each time you log into the program (shown in Figure 4.)



## Functional Layout

Configuration Manager tasks are grouped into categories, which you can access by clicking the tabs at the top of each page. Each tab displays the available tasks in a horizontal menu at the top of the page. You can click on these menu items to display the specific configuration options.



A separate page displays for each task in the task bar. The left-most task displays by default when you click on a new tab. The same task may appear in more than one tab, when appropriate. For example, the Lan Config task displays in both the LAN tab and the Routing tab.

## Commonly used buttons

The following buttons are used throughout the application.

Button	Function
Submit	Stores in temporary system memory any changes you have made on the current page.
Cancel	On pages that display accumulated statistics, this button resets the statistics to their initial values.
Refresh	Redisplays the current page with updated statistics or settings.
Help	Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.

The Home Page and System View Table

The Home page displays when you first access the program. This page is one of two options available in the Home tab (the other is the Quick Configuration page).

System View

Use this page to get the summary on the existing configuration of your device.

Device		DSL					
Model:	Titanium	Operational Status:		Startup Handshake			
H/W Version:	810012	Last State:		0x0			
S/W Version:	VIK-1.37.020618b/T93.3.13.	DSL Version:		T93.3.13			
Serial Number:	123456789abcdx	Standard:		Multimode			
Mode:	Routing And Bridging	Up		Down			
Up Time:	0:2:35	Speed	Latency	Speed	Latency		
Time:	Thu Jan 01 00:02:35 1970	0 Kbps	-	0 Kbps	-		
Time Zone:	GMT						
Daylight Saving Time:	OFF						
Name:	-						
Domain Name:	-						
WAN Interfaces							
Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoE	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	0/35	
LAN Interface							
Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	192.168.51.239	255.255.255.0	-	Auto	Auto	
usb-0	-	9.25.67.1	255.255.255.0	-	-	-	
Services Summary							
Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	inside						
ppp-0	outside						
usb-0	inside						

Figure 4. System View Table

The System View table provides a snapshot of your system configuration.

Note that some of the settings are links to the software pages that enable you to configure those settings. The following table describes each section of the System View table.

Table Heading	Description
Device	Displays basic information about the My ADSL Modem hardware and software versions, the system uptime (since the last reboot), and the preconfigured operating mode.
DSL	Displays the operational status, version, and performance statistics for the DSL line. You can check DSL in the table or display the WAN tab to view additional DSL settings, which are described in Configuring EOA Interfaces.

## WAN Interfaces

Displays the software name(s) and various settings for the device interface(s) that communicates with your ISP via DSL. Although you only have one physical DSL port, multiple software-defined interfaces can be configured to use it. See the ATM VC, PPP, EOA, and IPoA chapters for more information about the WAN interfaces defined on your system.

For each interface, a Lower Interface name, such as aal5-0, should display. You can click on the Lower Interface name to view or change the ATM VC settings that this interface uses.

## LAN Interface

Displays the software names and various settings for the device interfaces that communicate directly with your network. These typically include an Ethernet Interface named eth-0, and may include a USB Interface named usb-0. For information on modifying properties of these interfaces, see Configuring the LAN Ports and USB Functionality.

## Services Summary

Displays the status of various services that the My ADSL Modem performs to help you manage your network. A green check mark indicates the service is active and a red X indicates that it is inactive:

NAT:	Translating private IP addresses to your public IP address (Configuring Network Address Translation)
IP Filter:	Setting up filtering rules that accept or deny incoming or outgoing data (Configuring IP Filters and Blocking Protocols)
RIP:	Enabling router-to-router communication (Configuring the Routing Information Protocol)
DHCP Relay:	Enabling dynamic assignment of IP information from your ISP to your computers (Configuring Dynamic Host Configuration Protocol)
DHCP Client:	Enabling dynamic assignment of IP information from your ISP or another computer on your network to the device's LAN port (Configuring the LAN Ports)

DHCP Server:	Enabling dynamic assignment of IP information from the device's built-in DHCP server to your LAN computers (Configuring Dynamic Host Configuration)
IGMP:	Enabling message forwarding from external sources such as your ISP, based on Internet Group Management Protocol (not configurable).

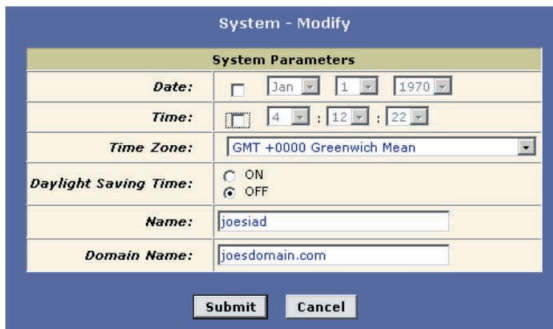
## Modifying Basic System Information

You can modify basic system information, which includes the system date and time and the names assigned to the My ADSL Modem and the network domain in which it exists.

*Note :*        *Changing the My ADSL Modem date and time does not affect the date and time on your PCs.*

Follow these instructions to change basic system information:

1. At the bottom of the Home page, click Modify. The System - Modify page displays in a separate browser window:



**Figure 5. System-Modify Page**

2. Modify the fields on this page as required. The following table describes each field:

Option	Description
Date and Time	These fields initially appear dimmed. To modify the date and time, click the respective check boxes and select the appropriate values from the drop-down lists. The time displays in military format.

**Time Zone****Daylight Savings Time**

You can select your time zone from the drop-down list, and then click the appropriate radio button to indicate whether Daylight Savings Time is currently in effect.

After you initially set the time, turning DST On or Off will adjust the current displayed time by one hour in the appropriate direction.

You must remember to change the DST option each spring and fall — it will not change automatically.

**Host Name**

You can use this field to specify an easy-to-remember name for the My ADSL Modem. The next time you want to access Configuration Manager, you can type this name in the location box in your Web browser, instead of typing the numeric IP address. For example, if you entered myrouter in this field (and left the Domain Name field blank), then you could type the following in your Web browser to access Configuration Manager: `http://myrouter`

*Note: This will only work if you are using the My ADSL Modem's DNS relay feature. This feature is automatically enabled when the DNS server address configured on your PCs is also the address assigned to the LAN port on the My ADSL Modem. See Configuring DNS Server Addresses for more information.*

**Domain Name**

You can use this field to specify an Internet domain name for the My ADSL Modem. The next time you access Configuration Manager, you can type the domain name and the device name (see the Name field above) in your Web browser. For example, if you entered myrouter in the Name field and mydomain.com in the Domain Name field, then you would type the following in your Web browser to access Configuration Manager: `http://myrouter.mydomain.com`

3. When you are finished modifying the settings, click Submit. and then click Close to return to the System View page.
4. To save your changes to permanent memory, click the Admin tab, and then click Commit & Reboot in the task bar.
5. Click Commit.

## Committing Changes and Rebooting

### Committing your changes

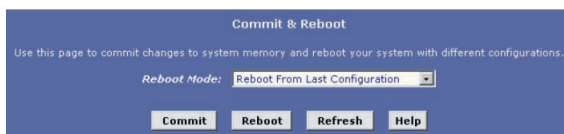
Whenever you use the Configuration Manager to change system settings, the changes are initially placed in temporary storage called random access memory or RAM. Your changes are made effective when you submit them, but will be lost if the device is reset or turned off.

You can commit changes to save them permanently to flash memory.

**Note :** *Submitting changes activates them immediately, but saves them only until the device is reset or powered down. Committing changes saves them permanently.*

Follow these steps to commit changes.

1. Click the Admin tab, and then click Commit & Reboot in the task bar. The Commit & Reboot page displays.



**Figure 6. Commit & Reboot Page**

2. Click Commit. (Disregard the selection in the Reboot Mode drop-down list; it does not affect the commit process.) These changes are saved to permanent storage.

The previous settings are copied to backup storage so that they can be recalled if your new settings do not work properly (see the rebooting instructions).

### Rebooting the device using Configuration Manager

To reboot the device, display the Commit & Reboot page, select the appropriate reboot mode from the drop-down menu, and then click Reboot.

You can select from the following three options when rebooting:

Option	Description
Reboot from Last Configuration	Reboot the device using the current settings in permanent memory, including any changes you just committed.
Reboot from Backup Configuration	Reboot the device using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.
Reboot from Default Configuration	Reboot the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.

**Warning :** *Do not reboot the device using the Reset button on the back Panel of the My ADSL Modem to activate new changes. This button resets the device settings to the factory default values. Any custom settings will be lost.*

---

## Configuring the LAN Ports

---

This chapter describes how to configure IP properties for the interfaces on the My ADSL Modem that communicate with your LAN computers.

### Connecting via Ethernet

If you are using the My ADSL Modem with multiple PCs on your LAN, you must connect the LAN via an Ethernet hub to the device's LAN port, called eth-0.

If you are using a single PC with the My ADSL Modem, You can connect the PC directly to the LAN port using a Ethernet cable.

You must assign a unique IP address to each device port that you use.

### Configuring the LAN Port IP Address

The LAN IP address identifies the LAN port (eth-0) as a node on your network; that is, its IP address must be in the same subnet as the PCs on your LAN.

**Definition:**     *A network node can be thought of as any interface where a device connects to the network, such as the My ADSL Modem's LAN port and the network interface cards on your PCs. See IP Addresses, Network Masks, and Subnets for an explanation of subnets.*

You can change the default to reflect the set of IP addresses that you want to use with your network.

If your network uses a DHCP server (other than the My ADSL Modem) to assign IP addresses, you can configure the device to accept and use a LAN IP address assigned by that server. Similarly, if your ISP performs DHCP serving for your network, you can configure the device to accept an IP address assigned from the ISP's server. In this mode, the My ADSL Modem is considered a DHCP client of your (or your ISP's) DHCP server.

**Note :**           *The My ADSL Modem itself can function as a DHCP server for your LAN computers, as described in Configuring Dynamic Host Configuration Protocol, but not for its own LAN port.*

Follow these steps to change the default LAN IP address or to configure the LAN port as a DHCP client:

1. Log into Configuration Manager, and then click the LAN tab. The LAN Configuration page displays.

LAN Configuration

Use this page to set the LAN configuration, which determines how your device is identified on the network.

LAN Configuration

System Mode:

Routing And Bridging

Get LAN Address:

☒ Manual

☐ External DHCP Server

☐ Internal DHCP Server

LAN IP Address:

19216811

LAN Network Mask:

2552552550

Speed:

100BT

Duplex:

Full

IGMP:

☐ Enable

☒ Disable

USB Configuration

USB IP Address:

19216812

USB Network Mask:

2552552550

IGMP:

☐ Enable

☒ Disable

Submit

Cancel

Refresh

Help

Figure 7. LAN Configuration Page

The LAN Configuration table displays the following settings:

Setting

Description

System Mode

The preconfigured mode for your device, such as Routing mode, Bridging mode, or both modes simultaneously. This setting is not user -configurable.

Get LAN Address

Provides options for how the device’s LAN port is assigned an IP address:

Manual indicates that you will be assigning a static IP address, which you can enter in the fields below.

External DHCP Server indicates that your ISP will be assigning an IP address from their own DHCP server to the port, dynamically each time you log on.

Internal DHCP Server indicates that you have a DHCP server device on your network that will assign an address to the port. If you choose either the internal or external server option, the LAN port is called a DHCP client of the server.

Note that the public IP address assigned to you by your ISP is not your LAN IP address. The public IP address identifies the WAN (ADSL) port on your My ADSL Modem to the Internet.

LAN IP Address and  
LAN Network Mask

The IP address and network mask for the port. See IP Addresses, Network Masks, and Subnets for and overview of IP addresses and masks.



---

Speed	Ethernet speed
Duplex	Duplex method
IGMP	To Enable or Disable IGMP

2. Enter an IP address and mask in the fields provided and choose Disabled in the Use DHCP field, or enable either a remote or local DHCP server. Keep these points in mind:

**Manually specifying an address:** If you are using routing services on your LAN such as DHCP and NAT, you will want to assign a fixed LAN IP address and mask. This ensures that your LAN computers have a fixed address that they use to communicate with the device.

The IP address you assign must be in the same subnet as your LAN computers that connect to this port (that is, the network ID portion of their IP addresses and their subnet masks must be the same). See IP Addresses, Network Masks, and Subnets for an explanation of IP addresses and network masks.

If you change the LAN IP address, you may need to update the DHCP configuration so that the addresses that the DHCP server dynamically assigns to your computers are on the same subnet as the new LAN IP address. See Configuring Dynamic Host Configuration Protocol for instructions on changing the pool of dynamically assigned addresses.

**Enabling DHCP:** If you choose to have the LAN port be a DHCP client of an internal or external server, the LAN Network Mask field will be dimmed and made unavailable for entry. The LAN IP Address field will remain editable, however. The address that you specify here will be used as a request to the DHCP server. This is referred to as a Configured IP Address in the program. If the configured IP address is not available from the DHCP server, then system will accept another assigned address. Even after another number is assigned, the same configured IP address will continue to display in this field.

3. Click Submit.

If you changed the LAN IP address while working from a PC that is connected to the device via Ethernet, then your connection will be terminated.

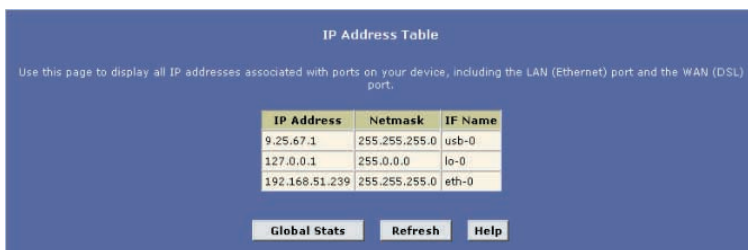
If you enabled the DHCP service, the My ADSL Modem will initiate a request for an IP address from your LAN's DHCP server. If a different IP address is assigned than was previously configured, your current connection will be terminated.

4. Reconfigure your PCs, if necessary, so that their IP addresses place them in the same subnet as the new IP address of the LAN port. See the Quick Start Configuring Your Computers for instructions.
5. Log into Configuration Manager by typing the new IP address in your Web browser's address/location box.
6. If the new settings work properly, click the Admin tab, and then click Commit & Reboot in the task bar.
7. Click Commit to save your changes to permanent memory.

The interfaces on the My ADSL Modem that communicate with other network and Internet devices are identified by unique Internet protocol (IP) addresses. You can use the Configuration Manager to view the list of IP addresses that your device uses, and to view other system and network performance data. See IP Addresses, Network Masks, and Subnets for a description of IP addresses and masks.

## Viewing the My ADSL Modem's IP Addresses

To view the My ADSL Modem's IP addresses, click the Routing tab, and then click IP Address in the task bar. The IP Address Table page displays:



IP Address	Netmask	IF Name
9.25.67.1	255.255.255.0	usb-0
127.0.0.1	255.0.0.0	lo-0
192.168.51.239	255.255.255.0	eth-0

Global Stats Refresh Help

**Figure 8. IP Address Table Page**

The table lists the IP address, network masks (Netmask), and interface names (IF Name) for each of its IP-enabled interfaces. The listed IP addresses may include:

- The IP address of the device's LAN (Ethernet) port, called eth-0. See Configuring the LAN Ports for instructions on configuring this address.
- The IP address of the WAN (ADSL line) interface, which your ISP and other external devices use to identify your network. It may be identified in the Configuration Manager by the names ppp-0, eoa-0, or ipoa-0, depending on the protocol your device uses to communicate with your ISP. Your ISP may assign the same address each time, or it may change each time you reconnect.
- The loopback IP address, named lo-0, of 127.0.0.1. This special address enables the device to keep any data addressed directly to it, rather than route the data through the WAN or LAN ports.

If your device has additional IP-enabled interfaces, the IP addresses of these will also display.

## Viewing IP Performance Statistics

You can view statistics on the processing of Internet protocol packets (a packet is a collection of data that has been bundled for transmission). You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.

To view global IP statistics, click Global Stats on the IP Address Table page. Below shows the IP Global Statistics page:

IP Global Statistics	
IP Datagrams Statistic	Values
<b>IP Received:</b>	607 Packets
<b>IP Received w/ Header Error:</b>	0 Packets
<b>IP Received w/ Wrong Address:</b>	0 Packets
<b>IP Received w/ Unknown Protocol:</b>	0 Packets
<b>IP Routing Discarded:</b>	0 Packets
IP Datagrams Forwarded	
<b>Forwarded Datagrams:</b>	106 Packets
Input IP Datagrams	
<b>Input IP Discarded:</b>	0 Packets
<b>Input IP Delivered To User-Protocol:</b>	237 Packets
Output IP Datagrams	
<b>IP Requests For Transmission w/ User-Protocol:</b>	132 Packets
<b>Output IP Discarded:</b>	0 Packets
<b>Output IP Discarded w/ No Route:</b>	106 Packets
IP Datagrams / Reassemble	
<b>Maximum # of Seconds IP Waits For Reassemble:</b>	60 Second(s)
<b>IP Received Which Needed To Be Reassembled:</b>	0 Packets
<b>IP Successfully Re-assembled:</b>	0 Packets
<b>IP Fails To Re-Assemble:</b>	0 Packets
IP Datagrams / Fragment	
<b>IP Successfully Fragmented:</b>	0 Packets
<b>IP Fails To Fragment:</b>	0 Packets
<b>IP Fragments Created:</b>	0 Packets
<input type="button" value="Close"/> <input type="button" value="Refresh"/> <input type="button" value="Help"/>	

**Figure 9. IP Global Statistics Page**

To display updated statistics showing any new data since you opened the page, click Refresh.

---

## Configuring Dynamic Host Configuration Protocol

---

You can configure your network and My ADSL Modem to use the Dynamic Host Configuration Protocol (DHCP). This chapter provides an overview of DHCP and instructions for implementing it on your network.

### Overview of DHCP

#### What is DHCP?

DHCP is a protocol that enables network administrators to centrally manage the assignment and distribution of IP information to computers on a network.

When you enable DHCP on a network, you allow a device — such as the My ADSL Modem or a router located with your ISP — to assign temporary IP addresses to your computers whenever they connect to your network. The assigning device is called a DHCP server, and the receiving device is a DHCP client.

*Note :*      *If you used the Quick Start instructions, you configured each LAN PC with an IP address, or you specified that it will receive IP information dynamically (automatically). If you chose to have the information assigned dynamically, then you configured your PCs as DHCP clients that will accept IP addresses assigned from a DHCP server such as the*

#### My ADSL Modem.

The DHCP server draws from a defined pool of IP addresses and leases them for a specified amount of time to your computers when they request an Internet session. It monitors, collects, and redistributes the addresses as needed.

On a DHCP-enabled network, the IP information is assigned dynamically rather than statically. A DHCP client can be assigned a different address from the pool each time it reconnects to the network.

#### Why use DHCP?

DHCP allows you to manage and distribute IP addresses throughout your network from a central computer. Without DHCP, you would have to configure each computer separately with IP addresses and related information. DHCP is commonly used with large networks and those that are frequently expanded or otherwise updated.

#### My ADSL Modem DHCP modes

The device can be configured as a DHCP server, relay agent or client.

If you configure the device as a DHCP server, it will maintain the pool of addresses and distribute them to your LAN computers. If the pool of addresses includes private IP addresses, you must also configure the Network Address Translation service, so that the private addresses can be translated to your public IP address on the Internet.

If your ISP performs the DHCP server function for your network, then you can configure the device as a DHCP relay agent. When the My ADSL Modem receives a request for Internet



With this configuration, you could create the following two pools:

- Pool 0: 192.168.1.2 through 192.168.1.11
- Pool 1: 192.168.2.2 through 192.168.2.2

The DHCP server would automatically distribute the Pool 0 addresses only to computers connected to the interface in the same subnet as these addresses—the LAN interface, eth-0. Likewise, the address in Pool 1 would be distributed to the USB-connected computer.

Adding DHCP Server Address Pools

Follow these instructions to create an IP address pool:

- 1. Log into Configuration Manager, click the LAN tab, and then click DHCP Server in the task bar.

The Dynamic Host Configuration Protocol (DHCP) Server Configuration page displays.



Figure 10. DHCP Server Configuration Page

Depending on your preconfigured settings, the table may display one or more address pools, each in a row, or may be empty

- 2. Click Add. The DHCP Server Pool – Add page displays, as shown in Figure 11

The screenshot shows the 'DHCP Server Pool – Add' page. It has a title bar and a section titled 'DHCP Pool Information'. Below this are several fields for configuration: Start IP Address, End IP Address, Mac Address, Netmask, Domain Name, Gateway Address, DNS Address, SDNS Address, SMTP Address, POP3 Address, NNTP Address, WWW Address, IRC Address, WINS Address, and SWINS Address. Each field is represented by a set of input boxes or a dropdown menu. At the bottom of the page are buttons for 'Submit', 'Cancel', and 'Help'.

Figure 11. DHCP Server Pool – Add Page

3. Enter values for the Start IP Address, End IP Address, and Netmask fields, which are required, and any others as needed:

Field	Description
Start IP Address	
End IP Address	Specifies the lowest and highest addresses in the pool, up to a maximum range of 254 addresses. For example, if the LAN port is assigned IP address 192.168.1.1, then you could create a pool with address range 192.168.1.2 – 192.168.1.254 for distribution to your LAN computers.
Mac Address	A MAC address is a manufacturer-assigned hardware ID that is unique for each device on a network. Use this field only if you want to assign a specific IP address to the computer that uses this MAC address. If you type a MAC address here, you must have specified the same IP address in both the Start IP Address and End IP Address fields.
Netmask	Specifies which portion of each IP address in this range refers to the network and which portion refers to the host (computer). For a description of network masks and LAN network masks, see IP Addresses, Network Masks, and Subnets. You can use the network mask to distinguish which pool of addresses should be distributed to a particular subnet.
Domain Name	A user-friendly name that refers to the subnet that includes the addresses in this pool. This is used for reference only.
Gateway Address	The address of the default gateway for computers that receive IP addresses from this pool. If no value is specified, then the appropriate LAN (eth-0) or USB (usb-0) port address on the device will be distributed to each PC as its gateway address, depending on how each is connected. See Hops and Gateways for an explanation of gateway addresses.
DNS Address SDNS Address	The IP address of the Domain Name System server and Secondary Domain Name System server to be used by computers that receive IP addresses from this pool. These DNS servers translate common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, these servers are located with your ISP.

SMTP Address, POP3 Address, NNTP Address, WWW Address, IRC Address, WINS Address, SWINS Address, (optional)

The IP addresses of devices that perform various services for computers that receive IP addresses from this pool (such as the SMTP, or Simple Mail Transfer Protocol, server which handles e-mail traffic). Contact your ISP for these addresses.

4. When you are done defining the pool, click Submit.

A confirmation page displays briefly to indicate that the pool has been added successfully. After a few seconds, the DHCP Server Pool – Add page displays with the newly added pool.

5. Follow the instructions in the section on Setting the DHCP Mode to enable the DHCP Server.

## Viewing, modifying, and deleting address pools

To view, modify, or delete an existing address pool, display the DHCP Server Configuration page, and click the icons in the corresponding row in the address pool table.

To delete an IP address pool, click , then Submit and Commit your changes.

To view details on an IP address pool, click . A page displays with the same information that you entered when you added the pool.

To modify the pool, click . The DHCP Server Pool - Modify page displays, as shown in Figure 12.

DHCP Pool Information							
Start IP Address:	192.168.1.3						
End IP Address:	192.168.1.34						
Netmask:	255.255.255.0						
Domain Name:							
Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable						
Excluded IP:	<table border="1"> <thead> <tr> <th>Excluded IP Address</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>No Excluded IP!</td> <td></td> </tr> <tr> <td>192 168 1 3</td> <td>Add</td> </tr> </tbody> </table>	Excluded IP Address	Action	No Excluded IP!		192 168 1 3	Add
Excluded IP Address	Action						
No Excluded IP!							
192 168 1 3	Add						

Submit Cancel Help

**Figure 12. DHCP Server Pool-Modify Page**

You can change the Domain Name associated with an IP address pool or enable/disable the pool. By default, a pool is enabled when you create it.

When you are done making modifications, click Submit. Use the Commit function to save your changes to permanent memory.



## Excluding IP addresses from a pool

If you have IP addresses that are designated for fixed use with specific devices, or for some other reason you do not want to make them available to your network, you can exclude them from the pool. Display the DHCP Server Pool – Modify page, as shown in Figure 12. Type each address to be excluded in the Excluded IP field, and click Add. When you are done specifying excluded addresses, click Submit, and then use the Commit function to save your changes to permanent memory

## Viewing current DHCP address assignments

When the My ADSL Modem functions as a DHCP server for your LAN, it keeps a record of any addresses currently leased to your computers. To view a table of all current IP address assignments, display the DHCP Server Address Table page, and then click Address Table.

DHCP Server Address Table					
IP Address	Netmask	Mac Address	Pool Start	Address Type	Time Remaining
192.168.51.158	255.255.255.0	00:50:DA:57:F4:F6	0.0.0.0	Static	0 Second(s)

Close Refresh Help

**Figure 13. DHCP Server Address Table Page**

The DHCP Server Address Table lists any IP addresses that are currently leased to LAN devices. For each leased address, the table lists the following information:

Field	Description
IP Address	The address that has been leased from the pool.
Netmask	The network mask associated with the leased address. This identifies the network ID and host ID portions of the address (see IP Addresses, Network Masks, and Subnets for an explanation of these terms).
Mac Address	The unique hardware ID of the computer to which the IP address has been assigned.
Pool Start	The lower boundary of the address pool (shown here to identify the pool from which the leased address was assigned).
Address Type	Can be Static or Dynamic. Static indicates that the IP number has been assigned permanently to the specific hardware device. Dynamic indicates that the number has been leased temporarily for a specified length of time.

## Time Remaining

The amount of time left for the device to use the assigned address. The default lease time is 30 days (31536000 seconds).

## Configuring DHCP Relay

Some ISPs perform the DHCP server function for their customers' home/small office networks. In this case, you can configure the device as a DHCP relay agent. When a computer on your network requests Internet access, the My ADSL Modem contacts your ISP to obtain an IP address (and other information), and then forwards that information to the computer. Follow these instructions to configure DHCP relay:

First, you must configure your PCs to accept DHCP information assigned by a DHCP server:

1. Open the Windows Control Panel and display the computer's Networking properties. Configure the TCP/IP properties to Obtain an IP address automatically (the actual text may vary depending on your operating system). For detailed instructions, see the Quick Start Part2-Configuring Your Computers.

Next, you specify the IP address of the DHCP server and select the interfaces on your network that will be using the relay service.

2. Log into the Configuration Manager, click the LAN tab, and then click DHCP Relay in the task bar. The Dynamic HOST Configuration Protocol (DHCP) Relay Configuration page displays:

**Dynamic Host Configuration Protocol (DHCP) Relay Configuration**

As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.

DHCP Server Address:

Interfaces Running DHCP Relay	Action
ppp-0	
eth-0	

**Figure 14. DHCP Relay Configuration Page**

3. In the DHCP Server Address fields, type the IP address of your ISP's DHCP server.

If you do not have this number, it is not essential to enter it here. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

4. Select your WAN interface from the drop-down list and click Add. Your WAN interface may be named ppp-0, coa-0, or ipoa-0. Contact your ISP if you are unsure which type of WAN interface you use.

**Note:** You can also delete an interface from the table by clicking in the right column.

5. Click Submit.

A page displays to confirm your changes, and then the program returns to the Dynamic Host Configuration Protocol (DHCP) Relay Configuration page.

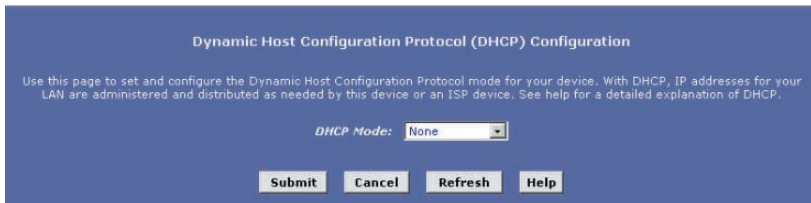
6. Follow the instructions in Setting the DHCP Mode to set the DHCP mode to DHCP Relay.

## Setting the DHCP Mode

You must enable the appropriate DHCP mode to activate your DHCP relay or DHCP server settings.

Follow these instructions to set the DHCP mode:

1. Click the LAN tab, and then click DHCP Mode in the task bar. The Dynamic Host Configuration Protocol (DHCP) Configuration page displays.



Dynamic Host Configuration Protocol (DHCP) Configuration

Use this page to set and configure the Dynamic Host Configuration Protocol mode for your device. With DHCP, IP addresses for your LAN are administered and distributed as needed by this device or an ISP device. See help for a detailed explanation of DHCP.

DHCP Mode:

**Figure 15. DHCP Configuration Page**

2. From the DHCP Mode drop-down list, choose DHCP Server, DHCP Relay, or None. If you choose None, your LAN computers must be configured with static IP addresses.
3. Click Submit.
4. Click the Admin tab, and then click Commit & Reboot in the task bar.
5. Click Commit to save your changes to permanent memory.

---

## Configuring Network Address Translation

---

This chapter provides an overview of Network Address Translation (NAT) and instructions for modifying the default configuration on your device.

### Overview of NAT

Network Address Translation is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses.

*Definitions :* A private IP address is created by a network administrator for use only on a LAN, whereas a public IP address is purchased from the Internet Corporation for Assigned Names and Numbers (ICANN) for use on the Internet. Typically, your ISP provides a public IP address for your entire LAN, and you define the private addresses for computers on your LAN.

In a typical NAT setup, your ISP provides you with a single public IP address to use for your entire network. Then, you assign each computer on your LAN a unique private IP address. (Or, you define a pool of private IP addresses for dynamic assignment to your computers, as described in Configuring Dynamic Host Configuration Protocol). On the My ADSL Modem, you set up a NAT rule to specify that whenever one of your computers communicates with the Internet, (that is, it sends and receives IP data packets) its private IP address—which is referenced in each packet—will be replaced by the LAN's public IP address.

*Definitions :* An IP data packet contains bits of data bundled together in a specific format for efficient transmission over the Internet. Such packets are the building blocks of all Internet communication. Each packet contains header information that identifies the IP address of the computer that initiates the communication (the source IP address), the port number that the router associates with that computer (the source port number), the IP address of the targeted Internet computer (the destination IP address), and other information.

When this type of NAT rule is applied, because the source IP address is swapped out, it appears to other Internet computers as if the data packets are actually originating from the computer assigned your public IP address (in this case, the My ADSL Modem).

The NAT rule could further be defined to disguise the source port in the data packet (i.e., change it to another number), so that outside computers will not be able to determine the actual port from which the packet originated. Data packets that arrive in response contain the public IP address as the destination IP address and the disguised source port number. The My ADSL Modem changes the IP address and source port number back to the original values (having kept track of the changes it made earlier), and then routes the packet to the originating computer.

NAT rules such as these provide several benefits:

- They eliminate the need for purchasing multiple public IP addresses for computers on your LAN. You can make up your own private IP addresses at no cost, and then have them translated to the public IP address when your computers access the Internet.

- They provide a measure of security for you LAN by enabling you to assign private IP addresses and then have these and the source port numbers swapped out before your computers access the Internet.
- The type of NAT function described above is called network address port translation (NAPT). You can use other types, called flavors, of NAT for other purposes; for example, providing outside access to your LAN or translating multiple private addresses to multiple public addresses.

## Viewing NAT Global Settings and Statistics

To view your NAT settings, log into Configuration Manager, click the Services tab. The NAT Configuration page displays by default.

NAT Global Information	
TCP Idle Timeout(sec):	86400
TCP Close Wait(sec):	60
TCP Def Timeout(sec):	60
UDP Timeout(sec):	300
ICMP Timeout(sec):	5
GRE Timeout(sec):	300
ESP Timeout(sec):	300
Default Nat Age(sec):	240
NAPT Port Start:	50000
NAPT Port End:	51023

**Figure 16. NAT Configuration Page**

The NAT Configuration page contains the following elements:

- The NAT Options drop-down list, which provides access to the NAT Configuration page and NAT Global Information table (shown by default and in Figure 16), the NAT Rule Configuration page (see Figure 18), and the NAT Translations page (see Figure 20).
- Enable/Disable radio buttons, which allow you to turn on or off the NAT feature.
- The NAT Global Information table, which displays the following settings that apply to all NAT rule translations:

## Field

## Description

TCP Idle Timeout (sec)

TCP Close Wait (sec)

TCP Def Timeout (sec)

When two computers communicate via the Internet, a TCP-based communication session is created between them to control the exchange of data packets. The TCP session can be viewed as being in one of three states, depending on the types of packets being transferred: the establishing state, where the connection is being set up, the active state, where the connection is being used to transfer data, and the closing state, in which the connection is being shut down. When a NAT rule is in effect on a TCP session in the active state, the session will timeout if no packets are received for the time specified in TCP Idle Timeout.

When in the closing state, the session will timeout if no packets are received for the time specified in TCP Close Wait.

When in the establishing state, the session will timeout if no packets are received for the time specified in TCP Def Timeout.

UDP Timeout (sec)

Same as TCP Idle Timeout, but for UDP-based communication sessions.

ICMP Timeout (sec)

Same as TCP Idle Timeout, but for ICMP-based communication sessions.

GRE Timeout (sec)

Same as TCP Idle Timeout, but for GRE-based communication sessions.

ESP Timeout (sec)

Same as TCP Idle Timeout, but for ESP-based communication sessions.

Default Nat Age (sec)

For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid if no packets are received.

NAPT Port Start,  
NAPT Port End

When an NAPT rule is defined, the source ports will be translated to sequential numbers in this range.

If you change any values, click Submit, and then click the Admin tab and Commit your changes to permanent system memory.

You can click Global Stats to view accumulated data on how many NAT rules have been invoked and how much data has been translated.



NAT Rule Global Statistics	
<b>Total NAT Sessions</b>	
<i>Total Translation Sessions:</i>	0 Sessions
<i>Sessions For FTP ALG:</i>	0 Sessions
<i>Sessions For SNMP ALG:</i>	0 Sessions
<i>Sessions For Real Audio ALG:</i>	0 Sessions
<i>Sessions For Remote-Command-Session:</i>	0 Sessions
<i>Number Of L2TP Alg Sessions:</i>	0 Sessions
<i>Number Of MIRC Alg Sessions:</i>	0 Sessions
<i>Number Of ICQ Alg Sessions:</i>	0 Sessions
<i>Number Of CUCME Alg Sessions:</i>	0 Sessions
<i>Number Of H323 Q931 Alg Sessions:</i>	0 Sessions
<i>Number Of H323 RAS Alg Sessions:</i>	0 Sessions
<i>Number Of H323 H245 Alg Sessions:</i>	0 Sessions
<i>Number Of H323 RTP Alg Sessions:</i>	0 Sessions
<i>Number Of ICQ TCP Alg Sessions:</i>	0 Sessions
<i>Number Of CUSEEME UDP Alg Sessions:</i>	0 Sessions
<i>Number Of PPTP Alg Sessions:</i>	0 Sessions
<i>Number Of RTSP Alg Sessions:</i>	0 Sessions
<i>Number Of Timbuktu Alg Sessions:</i>	0 Sessions
<b>Translation Statistic</b>	
<i>Packets w/o Matching Translation Rules:</i>	0 Packets
<i>Number Of In-Packets Translated:</i>	0 Packets
<i>Number Of Out-Packets Translated:</i>	0 Packets

**Figure 17. NAT Rule Global Statistics Page**

The table provides basic information for each NAT rule you have set up. You can click Clear to restart the accumulation of the statistics at their initial values.



## Viewing NAT Rules and Rule Statistics

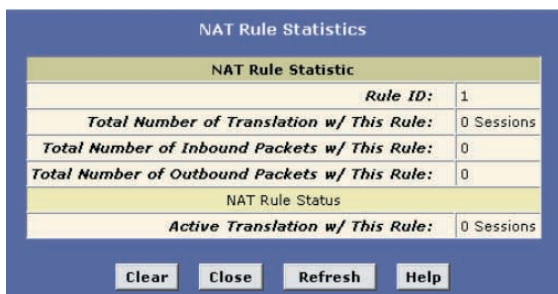
To view the NAT rules currently defined on your system, select NAT Rule Entry in the NAT Options drop-down list. The Network Address Translation (NAT) Rule Configuration page displays, as shown in Figure 18

Network Address Translation (NAT) Rule Configuration						
Each row in the table lists a rule for translating addresses. See Help for instructions on creating NAT rules.						
NAT Options: NAT Rule Entry						
Rule ID	IF Name	Rule Flavor	Protocol	Local IP From	Local IP To	Action
1	ALL	NAPT	ANY	0.0.0.0	255.255.255.255	  <b>Stats</b>
<div>Add</div> <div>Refresh</div> <div>Help</div>						

**Figure 18. NAT Rule Configuration Page**

The Network Address Translation (NAT) Rule Configuration table displays a row containing basic information for each rule. For a description of these fields, refer to the instructions for adding rules.

From the Network Address Translation (NAT) Rule Configuration page, you can click Add to add a new rule, or use the icons in the right column to delete  or view details on  a rule. To view data on how often a specific NAT rule has been used, click Stats in the Action column. A page displays similar to the one shown in Figure 19:

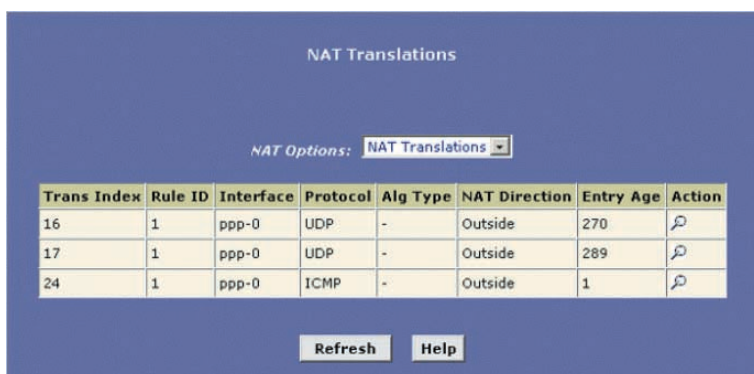


**Figure 19. NAT Rule Statistics Page**

The statistics show how many times this rule has been invoked and how many currently active sessions are using this rule. You can click Clear to reset the statistics to zeros and Refresh to display newly accumulated data.

## Viewing Current NAT Translations

To view a list of NAT Translations that have recently been performed and which remain in effect (for any of the defined rules), select NAT Translations from the NAT Options drop-down list.



**Figure 20. NAT Translations Page**

For each current NAT Translation session, the table contains the following fields:



Field	Description
Trans Index	The sequential number assigned to the IP session used by this NAT translation session.
Rule ID	The ID of the NAT rule invoked.
Interface	The device interface on which the NAT rule was invoked (from the rule definition).
Protocol	The IP protocol used by the data packets that are undergoing translations (from the rule definition) Example: TCP, UDP, ICMP.
Alg Type	The Application Level Gateway (ALG), if any, that was used to enable this NAT translation (ALGs are special settings that certain applications require in order to work while NAT is enabled).
NAT Direction	The direction (Inside or Outside) of the translation. A NAT direction is assigned to each port; the Ethernet and USB ports are defined as inside ports, and the WAN ports are defined as outside ports. The NAT direction is determined by the interface on which the rule is invoked.
Entry Age	The elapsed time, in seconds, of the NAT translation session.

You can click in the Action column to view additional details about a NAT translation session.

NAT TRANSLATION - Details	
Translation Information	
<b>Translation Index:</b>	16
<b>Rule ID:</b>	1
<b>IF Name:</b>	ppp-0
<b>Protocol:</b>	UDP
<b>ALG Type:</b>	-
<b>Translation Direction:</b>	Outside
<b>NAT Age:</b>	209
<b>Translated InAddress:</b>	10.0.20.102
<b>In Address:</b>	192.168.1.4
<b>Out Address:</b>	192.168.1.255
<b>In Packets:</b>	0
<b>Out Packets :</b>	39
<b>In Ports:</b>	137
<b>Out Ports:</b>	137
<b>Translated In Ports:</b>	50000
<div>Close Refresh Help</div>	

**Figure 21. NAT TRANSLATION – Detail Page**

In addition to the information displayed in the NAT Translations- Detail table, this table displays the following for the selected current translation sessions:

Field	Description
Translated InAddress	The public IP address to which the private IP address was translated.
In Address	The private IP address that was translated.
Out Address	The IP address of the outside destination (web, ftp site, etc.)
In Packets, Out Packets	The number of incoming and outgoing IP packets that have been translated in this translation session.
In Ports	The actual port number corresponding to the LAN computer.
Out Ports	The port number associated with the destination address.
Translated In Ports	The port number to which the LAN computer's actual port number was translated.
Adding NAT Rules	This section explains how to create rules for each NAT flavor.

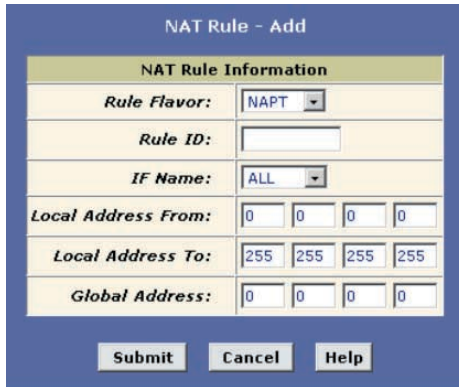
*Note :*      *You cannot edit existing NAT rules. To change a rule setup, delete it and add a new rule with the modified settings.*

## The NATP rule: Translating between private and public IP addresses

Follow these instructions to create a rule for translating the private IP addresses on your LAN to your public IP addresses. This type of rule uses the NAT flavor NATP, which was used in your default configuration. The NATP flavor translates private source IP addresses to a single public IP addresses. The NATP rule also translates the source port numbers to port numbers that are defined on the NAT Global Configuration page.

1. Click the NAT tab, and then select NAT Rule Entry from the NAT Options drop-down list. The NAT Rule entry page displays a row for each currently configured NAT rule.
2. Click Add to display the NAT Rule – Add page.
3. From the Rule Flavor drop-down list, select NATP.

The page redisplay with only those fields that are appropriate for the NATP rule flavor, as shown in Figure 22



NAT Rule Information				
Rule Flavor:	NAPT			
Rule ID:				
IF Name:	ALL			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address:	0	0	0	0

Submit Cancel Help

**Figure 22. NAT Rule-Add Page (NAPT Flavor)**

4. Enter a Rule ID. The Rule ID determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). If you define two or more rules that act on the same set of IP addresses, be sure to assign the Rule ID so that the higher priority rules are invoked first. It is recommended that you specify rule IDs as multiples of 5 or 10 so that, in the future, you can insert a rule between two existing rules.

Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

5. From the IF Name drop-down list, select the interface on the device to which this rule applies.

Typically, NAT rules are used for communication between your LAN and the Internet. Because the device uses the WAN interface (which may be named ppp-0, eoa-0, or ipoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

6. In the Local Address From field and Local Address To fields, type the starting and ending IP addresses, respectively, of the range of private address you use on your network that you want to be translated.

You can specify that data from all LAN addresses should be translated by typing 0 (zero) in each From field and 255 in each To field. Or, type the same address in both fields if the rule only applies to one LAN computer.

7. In the Global Address field, type the public IP address assigned to you by your ISP.
8. Click Submit.
9. When a page displays to confirm your change, click Close to return to the NAT Configuration page. The new rule should display in the NAT Rule Configuration table.
10. Ensure that the Enable radio button is selected, and then click Submit. A page displays to confirm your changes.
11. Click the Admin tab, and then click Commit and Reboot in the task bar.
12. Click Commit to save your changes to permanent memory.

## The RDR rule: Allowing external access to a LAN computer

You can create an RDR rule to make a computer on your LAN, such as a Web or FTP server, available to Internet users without requiring you to obtain a public IP address for that computer. The computer's private IP address is translated to your public IP address in all incoming and outgoing data packets.

**Note :** *Without an RDR rule (or the Bimap rule), the Ethernet / USB ADSL Modem blocks attempts by external computers to access your LAN computers.*

The following example illustrates using the RDR rule to provide external access to your web server:

Your My ADSL Modem receives a packet containing a request for access to your Web server. The packet header contains the public address for your LAN as the destination IP address, and a destination port number of 80. Because you have set up an RDR rule for incoming packets with destination port 80, the device recognizes the data as a request for Web server access. The device changes the packet's destination address to the private IP address of your Web server and forwards the data packet to it.

Your Web server sends data packets in response. Before the My ADSL Modem forwards them on to the Internet, it changes the source IP address in the data packets from the Web server's private address to your LAN's public address. To an external Internet user then, it appears as if your Web server uses your public IP address.

The screenshot shows a 'NAT Rule - Add' dialog box with a 'NAT Rule Information' section. The 'Rule Flavor' is set to 'RDR'. The 'Rule ID' is empty. The 'IF Name' is set to 'ALL' and the 'Protocol' is set to 'ANY'. The 'Local Address From' and 'Local Address To' fields are empty. The 'Global Address From' and 'Global Address To' fields are both set to '0.0.0.0'. The 'Destination Port From' is set to 'Any other port' and '0'. The 'Destination Port To' is set to 'Any other port' and '65535'. The 'Local Port' is set to 'Any other port' and '0'. At the bottom are 'Submit', 'Cancel', and 'Help' buttons.

NAT Rule Information	
Rule Flavor:	RDR
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	
Local Address To:	
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535
Local Port:	Any other port 0

Submit Cancel Help

**Figure 23. NAT Rule-Add Page (RDR Flavor)**

Follow these instructions to add an RDR rule (see steps 1-4 under The NAPT Rule for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select RDR as the Rule Flavor, if necessary, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. Select a Protocol to which this rule applies, or choose ANY .

This selection specifies which type of Internet communication will be subject to this translation rule. You can select ANY if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the Internet Assigned Numbers Authority (IANA)-specified protocol number.

4. In the Local Address From and Local Address To fields, type the same private IP address, or the lowest and highest addresses in a range:

If you type the same IP address in both fields, incoming traffic that matches the criteria you specify in steps 5 and 6 will be redirected to that IP address.

If you type a range of addresses, incoming traffic will be redirected to any available computer in that range. This option would typically be used for load balancing, whereby traffic is distributed among several redundant servers to help ensure efficient network performance.

These addresses should correspond to private addresses already in use on your network (either assigned statically to your PCs or assigned dynamically using DHCP, as discussed in the Quick Start, Part 2).

5. In the Global Address From and Global Address To fields, type the public IP address assigned to you by your ISP. “If you have multiple WAN (PPP) interfaces, this rule will not be enforced for data that arrives on other PPP interfaces. This rule will not be enforced for data that arrives on WAN interfaces not specified here.” If you have multiple WAN interfaces and want the rule to be enforced on more than one of them (or all), type the starting and ending IP addresses of the range.
6. In the Destination Port From and Destination Port To fields, type the port ID numbers of the computer you are making publicly available.

You can specify a range using the From/To fields if you want the rule to apply to a range of port types, or enter the same port number in both fields.

A port ID identifies the specific function of the computer connected to it, and therefore can limit the types of data that pass to and from the computer.

For example, Web (HTTP) servers are usually identified by port number 80; packets containing traffic destined for a Web server will contain this port ID. The Internet Assigned Numbers Authority (IANA) assigns port numbers for common types of servers and functions.

7. If the LAN computer that you are making publicly available is configured to use a non-standard port number for the type of traffic it receives, type the non-standard port number in the Local Port field.

This option translates the standard port number in packets destined for your LAN computer

to the non-standard number you specify. For example, if your Web server uses (non-standard) port 2000, but you expect incoming data packets to refer to (standard) port 80, you would enter 2000 here (and select HTTP or type 80 in the Destination Port fields). The headers of incoming packets destined for port 80 will be modified to refer to port 2000. The packet will then be routed appropriately to the web server.

8. Follow steps 8-12 under The NAT Rule to submit your changes.

## The Basic rule: Performing 1:1 translations

The Basic flavor translates the private (LAN-side) IP address to a public (WAN-side) address, like NATP rules. However, unlike NATP rules, Basic rules do not also translate the port numbers in the packet header; they are passed through untranslated. Therefore, the Basic rule does not provide the same level of security as the NATP rule.

The screenshot shows a 'NAT Rule - Add' dialog box with a 'NAT Rule Information' section. The 'Rule Flavor' is set to 'BASIC'. The 'Rule ID' field is empty. The 'IF Name' is set to 'ALL'. The 'Protocol' is set to 'ANY'. The 'Local Address From' and 'Local Address To' fields are both set to '0.0.0.0' to '255.255.255.255'. The 'Global Address From' and 'Global Address To' fields are both set to '0.0.0.0' to '0.0.0.0'. At the bottom are 'Submit', 'Cancel', and 'Help' buttons.

NAT Rule Information			
Rule Flavor:	BASIC		
Rule ID:			
IF Name:	ALL		
Protocol:	ANY		
Local Address From:	0	0	0
Local Address To:	255	255	255
Global Address From:	0	0	0
Global Address To:	0	0	0

Submit Cancel Help

**Figure 24. NAT Rule-Add Page (Basic Flavor)**

Follow these instructions to add an BASIC rule (see steps 1-4 under The NATP Rule for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select BASIC as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. Select a Protocol to which this rule applies, or choose ANY.

This selection specifies which type of Internet communication will be subject to this translation rule. You can select ANY if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the Internet Assigned Numbers Authority (IANA)-specified protocol number.

4. In the Local Address From and Local Address To fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

If you specify a range, each address will be translated in sequence to a corresponding address in a range of Global Addresses (which you specify in step 5).



You can create a BASIC rule for each specific address translation to occur. The range of addresses should correspond to private addresses already in use on your network, whether assigned statically to your PCs, or assigned dynamically using DHCP.

5. In the Global Address From and Global Address To fields, type the starting and ending address that identify the pool of public IP addresses that the private addresses should be translated to. Or, type the same address in both fields (if you also specified a single address in step 4).
6. Follow steps 8-12 under The NAT Rule to submit your changes.

## The Filter rule: Configuring a BASIC rule with additional criteria

Like the BASIC flavor, the Filter flavor translates public and private IP addresses on a one-to-one basis. The Filter flavor extends the capability of the BASIC rule. Refer to The BASIC Rule for a general description.

You can use the Filter rule if you want an address translation to occur only when your LAN computers initiate access to specific destinations. The destinations can be identified by their IP addresses, port type (which identifies it as a FTP or Web server, for example), or both.

The screenshot shows the 'NAT Rule - Add' window with the 'Filter' flavor selected. The form contains the following fields and values:

NAT Rule Information				
Rule Flavor:	FILTER			
Rule ID:				
IF Name:	ALL			
Protocol:	ANY			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address From:	0	0	0	0
Global Address To:	0	0	0	0
Destination Address From:	0	0	0	0
Destination Address To:	255	255	255	255
Destination Port From:	Any other port		0	
Destination Port To:	Any other port		65535	

Buttons at the bottom: Submit, Cancel, Help.

**Figure 25. NAT Rule-Add Page (Filter Flavor)**

Follow these instructions to add a Filter rule (see steps 1-4 under The NAPT Rule for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select FILTER as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. Select a Protocol to which this rule applies, or choose ANY.

This selection specifies which type of Internet communication will be subject to this translation rule. You can select ANY if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the Internet Assigned Numbers Authority (IANA)-specified protocol number.

4. In the Local Address From and Local Address To fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

If you specify a range, each address will be translated in sequence to a corresponding address in a range of Global Addresses (which you specify in step 5).

The address (or range of addresses) should correspond to a private addresses (or addresses) already in use on your network. These may be assigned statically to your PCs or assigned dynamically using DHCP, as discussed in the Quick Start.

5. In the Global Address From and Global Address To fields, type the starting and ending address that identify the range of public IP addresses to translate your private addresses to. Or, type the same address in both fields (if you also specified a single address in step 4).
6. In the Destination Address From, Destination Address To fields, specify a destination address (or range) if you want this rule to apply only to outbound traffic to the address (or range). If you enter only the network ID portion of the destination address, then the rule will apply to outbound traffic to all computers on network.
7. In the Destination Port From field, type a port ID number if you want the rule to apply only to outbound traffic to servers of this type.
8. You can specify a range using the From/To fields if you want the rule to apply to a range of port types, or enter the same port number in both fields. See step 6 for creating an RDR Rule for an explanation of port IDs.
9. Follow steps 8-12 under The NAT Rule to submit your changes.

## The Bimap rule: Performing two-way translations

Unlike the other NAT flavors, the Bimap flavor performs address translations in both the outgoing and incoming directions.

In the incoming direction, when the specified My ADSL Modem interface receives a packet with your public IP address as the destination address, this address is translated to the private IP address of a computer on your LAN. To the external computer, it appears as if the access is being made to the public IP address, when, in fact, it is communicating with a LAN computer.

In the outgoing direction, the private source IP address in a data packet is translated to the LAN's public IP address. To the rest of the Internet, it appears as if the data packet originated from the public IP address.

Bimap rules can be used to provide external access to a LAN device. They do not provide the same level of security as RDR rules, because RDR rules also reroute incoming packets based on the port ID. Bimap rules do not account for the port number, and therefore allow external access regardless of the destination port type specified in the incoming packet.

The screenshot shows a window titled "NAT Rule - Add" with a blue border. Inside, there's a section titled "NAT Rule Information" with a yellow background. Below this, there are several fields: "Rule Flavor:" with a dropdown menu set to "BIMAP"; "Rule ID:" with an empty text box; "IF Name:" with a dropdown menu set to "ALL"; "Local Address:" with four empty text boxes for IP address entry; and "Global Address:" with four text boxes, each containing a "0". At the bottom of the window are three buttons: "Submit", "Cancel", and "Help".

**Figure 26. NAT Rule-Add Page (Bimap Flavor)**

Follow these instructions to add a Bimap rule (see steps 1-4 under The NAPT Rule for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select BIMAP as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. In the Local Address field, type the private IP address of the computer to which you are granting external access.
4. In the Global Address field, type the address that you want to serve as the publicly known address for the LAN computer.
5. Follow steps 8-12 under The NAPT Rule to submit your changes.

## The Pass rule: Allowing specific addresses to pass through untranslated

You can create a Pass rule to allow a range of IP addresses to remain untranslated when another rule would otherwise do so.

The screenshot shows a window titled "NAT Rule - Add". Inside, there is a section titled "NAT Rule Information" with the following fields:

- Rule Flavor:** A dropdown menu set to "PASS".
- Rule ID:** An empty text input field.
- IF Name:** A dropdown menu set to "ALL".
- Local Address From:** Four input boxes containing "0", "0", "0", and "0".
- Local Address To:** Four input boxes containing "255", "255", "255", and "255".

At the bottom of the window are three buttons: "Submit", "Cancel", and "Help".

**Figure 27. NAT Rule-Add Page (Pass Flavor)**

The Pass rule must be assigned a rule ID that is a lower number than the ID assigned to the rule it is intended to pass. If you want a specific IP address or range of addresses to not be subject to an existing rule, say rule ID #5, then you can create a Pass rule with ID #1 through #4.

Follow these instructions to add a Pass rule (see steps 1-4 under The NAPT Rule for detailed instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select PASS as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. In the Local Address From and Local Address To fields, type the lowest and highest IP addresses that define the range of private address you want to be passed without translation.

If you want the Pass rule to act on only one address, type that address in both fields.

4. Follow steps 7-12 under The NAPT Rule to submit your changes.

---

## Configuring DNS Server Addresses

---

### About DNS

Domain Name System (DNS) servers map the user-friendly domain names that users type into their Web browsers (e.g., "yahoo.com") to the equivalent numerical IP addresses that are used for Internet routing.

When a PC user types a domain name into a browser, the PC must first send a request to a DNS server to obtain the equivalent IP addresses. The DNS server will attempt to look up the domain name in its own database, and will communicate with higher-level DNS servers when the name cannot be found locally. When the address is found, it is sent back to the requesting PC and is referenced in IP packets for the remainder of the communication.

### Assigning DNS Addresses

Multiple DNS addresses are useful to provide alternatives when one of the servers is down or is encountering heavy traffic. ISPs typically provide primary and secondary DNS addresses, and may provide additional addresses. Your LAN PCs learn these DNS addresses in one of the following ways:

**Statically :** If your ISP provides you with their DNS server addresses, you can assign them to each PC by modifying the PCs' IP properties.

**Dynamically from a DHCP pool:** You can configure the DHCP Server feature on the My ADSL Modem and create an address pool that specifies the DNS addresses to be distributed to the PCs. Refer to Configuring Dynamic Host Configuration Protocol for instructions on creating DHCP address pools.

In either case, you can specify the actual addresses of the ISP's DNS servers (on the PC or in the DHCP pool), or you can specify the address of the LAN port on the My ADSL Modem (e.g., 192.168.1.1). When you specify the LAN port IP addresses, the device performs DNS relay, as described in the following section.

**Note :** If you specify the actual DNS addresses on the PCs or in the DHCP pool, the DNS relay feature is not used.

### Configuring DNS Relay

When you specify the My ADSL Modem's LAN port IP addresses as the DNS addresses, then the device automatically performs DNS relay; i.e., because the device itself is not a DNS server, it forwards domain name lookup requests it receives from the LAN PCs to a DNS server at the ISP. It then relays the DNS server's response to the PC.

When performing DNS relay, the My ADSL Modem must maintain the IP addresses of the DNS servers it contacts. It can learn these addresses in either or both of the following ways:

**Learned through PPP:** If the device uses a PPP connection to the ISP, the primary and secondary DNS addresses can be learned via the PPP protocol. To use this method, the Use DNS checkbox must be selected in the PPP Interface Properties. (See Configuring PPP Interfaces for

instructions on configuring your PPP interface. Note that you cannot change this property by modifying an existing PPP interface; you must delete the interface and recreate it with the new setting.)

Using this option provides the advantage that you will not need to reconfigure the PCs or the My ADSL Modem if the ISP changes their DNS addresses.

**Configured on the My ADSL Modem:** You can use the device's DNS feature to specify the ISP's DNS addresses. If the device also uses a PPP interface with the Use DNS property enabled, then these configured addresses will be used in addition to the two addresses learned through PPP. If Use DNS is not enabled, or if a protocol other than PPP is used (such as EoA), then these configured addresses will be used as the primary and secondary DNS addresses.

Follow these steps to configure DNS relay:

1. Configure the LAN PCs to use the My ADSL Modem's LAN IP addresses as their DNS server addresses—by assigning the LAN IP address statically to each PC, or by inputting the LAN IP address or the address 0.0.0.0 as the DNS address in the DHCP server pool used by the PCs.
2. If using a PPP connection to the ISP, click the Use DNS check box so that the DNS server addresses it learns are used for DNS relay.

Or, ...

If not using a PPP connection (or if you want to specify DNS addresses in addition to those learned through PPP), configure the DNS addresses on the My ADSL Modem as follows:

- a. Click the Services tab, and then click DNS in the task bar. The Domain Name Service (DNS) Configuration page displays.

**Figure 28. DNS Configuration Page**

- b. Type the IP address of the DNS server in an empty row and click Add. You can enter only two addresses.
- c. Click the Enable radio button, and then click Submit.
3. Click the Admin tab, and then click Commit & Reboot in the task bar.
4. Click Commit to save your changes to permanent memory.

*Note : DNS addresses that are assigned to LAN PCs prior to enabling DNS relay will remain in effect until the PC is rebooted. DNS relay will only take effect when a PC's DNS address is the LAN IP address.*

Similarly, if after enabling DNS relay, you specify a DNS address (other than the LAN IP address) in a DHCP pool or statically on a PC, then that address will be used instead of the DNS relay address.



---

## Configuring IP Routes

---

You can use Configuration Manager to define specific routes for your Internet and network data. This chapter describes basic routing concepts and provides instructions for creating routes.

Note that most users do not need to define IP routes.

### Overview of IP Routes

The essential challenge of a router is: when it receives data intended for a particular destination, which next device should it send that data to? When you define IP routes, you provide the rules that a computer uses to make these decisions.

### IP routing versus telephone switching

IP routing decisions are similar to those made by switchboards that handle telephone calls.

When you dial a long distance telephone number, you are first connected to a switchboard operated by your local phone service carrier. All calls you initiate go first to this main switchboard.

If the phone number you dialed is outside your calling area, the switchboard opens a connection to a higher-level switchboard for long distance calls. That switchboard looks at the area code you dialed and connects you with another switchboard that serves that area. This new switchboard, in turn, may look at the prefix in the number you dialed (the middle set of three numbers) and connect to a more localized switchboard that handles numbers with that prefix. This final switchboard can then look at the last four digits of the phone number to open a connection with the person or company you dialed.

In comparison, when your computer initiates communication over the Internet, such as viewing a web page connecting to a web server, the data it sends out includes the IP address of the destination computer (the “phone number”). All your outgoing requests first go to the same router at your ISP (the first “switchboard”). That router looks at the network ID portion of the destination address (the “area code”) and determines which next router to send the request to. After several such passes, the request arrives at a router for the destination network, which then uses the host ID portion of the destination IP address (the local “phone number”) to route the request to the appropriate computer. (The network ID and host ID portions of IP addresses are explained in IP Addresses, Network Masks, and Subnets.)

With both the telephone and the computer, all transactions are initially sent to the same switchboard or router, which serves as a gateway to other higher- or lower-level devices. No single device knows at the outset the eventual path the data will take, but each uses a specific part of the destination address/phone number to make a decision about which device to connect to next.

### Hops and gateways

Each time Internet data is passed from one Internet address to another, it is said to take a hop. A hop can be a handoff to a different port on the same device, to a different device on the same network, or to a device on an entirely different network.

When a hop passes data from one type of network to another, it uses a gateway. A gateway is an IP address that provides initial access to a network, just as a switchboard serves as a gateway to a specific set of phone numbers. For example, when a computer on your LAN requests access to a company's web site, your ISP serves as a gateway to the Internet. As your request reaches its destination, another gateway provides access to the company's web servers.

## Using IP routes to define default gateways

IP routes are defined on computers, routers, and other IP-enabled devices to instruct them which hop to take, or which gateway to use, to help forward data along to its specified destination.

If no IP route is defined for a destination, then IP data is passed to a predetermined default gateway. The default gateway serves like a higher-level telephone switchboard; it may not be able to connect directly to the destination, but it will know a set of other devices that can help pass the data intelligently. If it cannot determine which of these devices provides a good next hop (because no such route has been defined), then that device will forward the data to its default gateway. Eventually, a high level device, using a predefined IP route, will be able to forward the data along a path to its destination.

## Do I need to define IP routes?

Most users do not need to define IP routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN computers and for the My ADSL Modem provide the most appropriate path for all your Internet traffic.

On your LAN computers, a default gateway directs all Internet traffic to the LAN port on the My ADSL Modem. Your LAN computers know their default gateway either because you assigned it to them when you modified their TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet. (Each of these processes is described in the Quick Start instructions, Part 2.)

On the My ADSL Modem itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection.

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

## Viewing the IP Routing Table

All IP-enabled computers and routers maintain a table of IP addresses that are commonly accessed by their users. For each of these destination IP addresses, the table lists the IP address of the first hop the data should take. This table is known as the device's routing table.

To view the My ADSL Modem's routing table, click the Routing tab. The IP Route Table page displays by default, as shown in Figure 29:

IP Route Table						
This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.						
Destination	NetMask	NextHop	IFName	Route Type	Route Origin	Action
10.0.20.0	255.255.255.0	10.0.20.90	eth-0	Direct	Dynamic	
10.0.20.90	255.255.255.255	127.0.0.1	ALL	Direct	Dynamic	
127.0.0.0	255.0.0.0	127.0.0.1	ALL	Direct	Dynamic	
<div> Add Refresh Help </div>						

**Figure 29. IP Route Table Page**

The IP Route Table displays a row for each existing route. These include routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices.

The following table defines the fields in the IP Route Table.

Field	Description
Destination	Specifies the IP address of the destination computer. The destination can be specified as the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
NetMask	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. Refer to IP Addresses, Network Masks, and Subnets, for an explanation of network masks.
NextHop	Specifies the next IP address to send data to when its final destination is that shown in the Destination column.
IFName	Displays the name of the interface on the device through which data is forwarded to the specified next hop.
Route Type	<p>Displays whether the route is Direct or Indirect.</p> <p>In a Direct route, the source and destination computers are on the same network, and the router attempts to directly deliver the data to the computer.</p> <p>In an Indirect route, the source and destination computers are on different networks, and the router forwards data to a device on another network for further handling.</p>

## Route Origin

Displays how the route was defined. Dynamic indicates that the route was created automatically or predefined by your ISP or the manufacturer. Routes you create are labeled Local. Other routes can be created automatically (using RIP, as described in Configuring the Routing Information Protocol), or defined remotely through various network management protocols (LCL or ICMP).

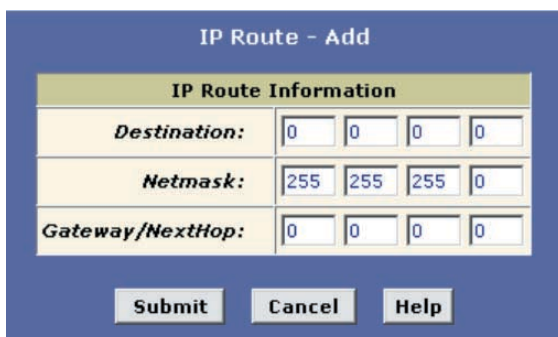
## Action

Displays an icon  you can click on to delete a route.

## Adding IP Routes

Follow these instructions to add an IP route to the routing table.

1. From the IP Route Table page, click Add. The IP Route – Add page displays, as shown in Figure 30.



**Figure 30. IP Route-Add Page**

2. Specify the Destination, Netmask, and Gateway / NextHop for this route.

To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the Destination and Netmask fields. Enter your ISP's IP address in the Gateway/NextHop field.

Note that you cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the device communicates with other routing devices. For routes you created, the routing table displays system default values in these fields.

3. Click Submit.
4. On the Confirmation page, click Close to return to the IP Route Table page.

The IP Routing Table will now display the new route.

5. Click the Admin tab, and then click Commit & Reboot in the task bar.
6. Click Commit to save your changes to permanent memory.

---

## Configuring Routing Information Protocol

---

The My ADSL Modem can be configured to communicate with other routing devices to determine the best path for sending data to its intended destination. Routing devices communicate this information using a variety of IP protocols. This chapter describes how to configure the My ADSL Modem to use one of these, called the Routing Information Protocol (RIP).

### RIP Overview

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line. Generally, RIP is used to enable communication on autonomous networks. An autonomous network is one in which all of the computers are administered by the same entity. An autonomous network may be a single network, or a grouping of several networks under the same administration. An example of an autonomous network is a corporate LAN, including devices that can access it from remote locations, such as the computers telecommuters use.

Using RIP, each device sends its routing table to its closest neighbor every 30 seconds. The neighboring device in turn passes the information on to its next neighbor and so on until all devices in the autonomous network have the same set of routes.

### When should you configure RIP?

Most small home or office networks do not need to use RIP; they have only one router, such as the My ADSL Modem, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

Your home network setup includes an additional router or RIP-enabled PC (other than the My ADSL Modem). The My ADSL Modem and the router will need to communicate via RIP to share their routing tables.

Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.

Your ISP requests that you run RIP for communication with devices on their network.

Configuring the My ADSL Modem's Interfaces with RIP The following instructions describe how to enable RIP on the My ADSL Modem

Note : In order for the My ADSL Modem to communicate with other devices using RIP, you must also enable the other devices to use the protocol. See the product documentation for those devices.

1. Log into the Configuration Manager, click the Services tab, and then click RIP in the task bar. The Routing Information Protocol (RIP) Configuration page displays, as shown in Figure 31.

**Routing Information Protocol (RIP) Configuration**

Routers on your LAN communicate with one another using the Routing Information Protocol. This table lists any interfaces on your device that use RIP (typically the LAN interface), and the version of the protocol used.

☐ Enable    ☒ Disable

Age(seconds):   
 Update Time(seconds):

IF Name	Metric	Send Mode	Receive Mode	Action
ppp-0	1	RIP1	RIP1	
<input type="text" value="eth-0"/>	<input type="text" value="1"/>	<input type="text" value="RIP1COMPAT"/>	<input type="text" value="RIP1"/>	<input type="button" value="Add"/>

**Figure 31. RIP Configuration Page**

The page contains radio buttons for Enable or Disable the RIP feature and a table listing interfaces on which the protocol is currently running. The first time you open this page, the table may be empty.

2. If necessary, change the Age(seconds) and Update Time(seconds).

These are global settings for all interfaces that use RIP.

Age is the amount of time in seconds that the device's RIP table will retain each route that it learns from adjacent computers.

Update Time specifies how frequently the My ADSL Modem will send out its routing table to its neighbors.

3. In the IF Name column, select the name of the interface on which you want to enable RIP.

For communication with RIP-enabled devices on your LAN, select eth-0 or the name of the appropriate virtual Ethernet interface.

For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.

4. Select a Metric value for the interface.

RIP uses a hop count as a way to determine the best path to a given destination in the network. The hop count is the sum of the metric values assigned to each port through which data is passed before reaching the destination. Among several alternative routes, the one with the lowest hop count is considered the fastest path.

For example, if you assign this port a metric of 1, then RIP will add 1 to the hop count when calculating a route that passes through this port. If you know that communication via this interface is slower than through other interfaces on your network, you can assign it a higher metric value than the others.

You can select any integer from 1 to 15.

5. Select a Send Mode and a Receive Mode.

The Send Mode setting indicates the RIP version this interface will use when it sends its route information to other devices.

The Receive Mode setting indicates the RIP version(s) in which information must be passed to the My ADSL Modem in order for it to be accepted into its routing table.

RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only.

RIP version 2 is the preferred selection because it supports classless IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on the autonomous network support this version of the protocol.

6. Click Add. The new RIP entry will display in the table.

7. Click the Enable radio button to enable the RIP feature.

**Note :** *If you disable the RIP feature, the interface settings you have configured will remain available for future activation.*

8. When you are finished defining RIP interfaces, click Submit. A page displays to confirm your changes.

9. Click the Admin tab, and then click Commit & Reboot in the task bar.

10. Click Commit to save your changes to permanent memory.

**Note :** *You can delete an existing RIP entry by clicking in the Action column.*

## Viewing RIP Statistics

From the RIP Configuration page, you can click Global Stats to view statistics on attempts to send and receive route table data over RIP-enabled interfaces on the My ADSL Modem.

RIP Global Statistics	
RIP Active Sessions	
<i>Request Sent:</i>	0 Packets
<i>Response Sent:</i>	0 Packets
<i>Request Received:</i>	0 Packets
RIP Packets w/ Error	
<i>Packets Received w/ Bad Version:</i>	0 Packets
<i>Packets Received w/ Bad Address Family:</i>	0 Packets
<i>Packets Received w/ Bad Request Format:</i>	0 Packets
<i>Packets Received w/ Bad Metrics:</i>	0 Packets
<i>Packets Received w/ Bad Response Format:</i>	0 Packets
<i>Packets Received w/ Invalid Port:</i>	0 Packets
<i>Packets Rejected:</i>	0 Packets
<i>Response Received:</i>	0 Packets
<i>Unknown Packets Received:</i>	0 Packets
<i>Packets Received from Non-Neighbor Router:</i>	0 Packets
<i>Packets Rejected for Authentication Failure:</i>	0 Packets
<i>Packets w/ Route Changed:</i>	0 Packets
Clear	Close
Refresh	Help

**Figure 32. RIP Global Statistics Page**

You can click Clear to reset all statistics to zero and Refresh to display any newly accumulated data.

As your LAN computers access the Internet via the My ADSL Modem, data is exchanged with your ISP through a complex network of telephone switches, Internet routers, servers, and other specialized hardware. These various devices communicate using a common language, or protocol, called Asynchronous Transfer Mode (ATM). On the Wide Area Network (WAN) that connects you to your ISP, the ATM protocol performs functions like those that the Ethernet protocol performs on your LAN.

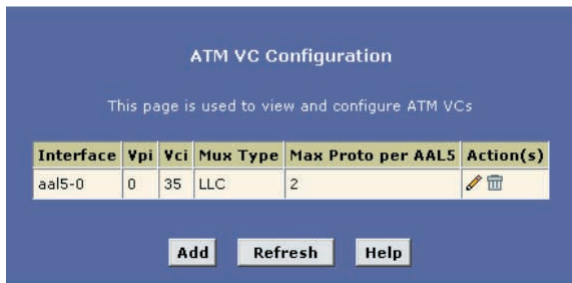


# Configuring the ATM Virtual Circuit

This chapter describes how to configure the ATM virtual circuit (VC). The VC properties define the path the My ADSL Modem uses to communicate with your ISP over the ATM network.


## Viewing Your ATM VC

To view your current configuration, log into Configuration Manager, click the WAN tab, and then click ATM VC in the task bar. The ATM VC Configuration page displays, as shown in Figure 33.



**Figure 33. ATM VC Configuration Page**

The ATM VC Configuration table displays the following fields (contact your ISP to determine these settings):

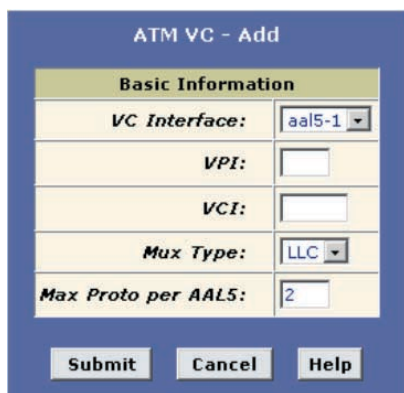
Field	Description
Interface	The name of the lower-level interface on which this VC operates. The low-level interface names are preconfigured in the software and identify the type of traffic that can be supported, such as data or voice. Internet data services typically use an aal5-type interface.
Vpi, Vci, and Mux Type	These settings identify a unique ATM data path for communication between your My ADSL Modem and your ISP.
Max Proto per AAL5	If you are using an AAL5-type of interface, this setting indicates the number of higher-level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IPoA interfaces). Contact your ISP to determine which connection protocol(s) they require.
Action (s)	Displays icons you can click on to modify and delete  the associated interface. You cannot delete an ATM interface if another protocol such as PPP, EoA, or IPoA has been defined to operate over the ATM interface. Delete the higher-level interface first, and then delete the ATM interface.

## Adding ATM VCs

You may need to create a VC if none has been predefined on your system or if you use multiple services with your ISP. Each service may require its own VC. Follow these instructions to add a VC:

1. From the ATM VC Configuration page, click Add.

The ATM VC – Add page displays, as shown in Figure 34.



**Figure 34. ATM VC-Add Page**

2. Select an interface name from the VC Interface drop-down list.
3. Enter the VPI and VCI values assigned by your ISP, and select the Mux Type from the drop-down list.
4. In the Max Proto per AAL5 text box, enter the number of protocols that the ISP indicated that you will need to configure (usually only one).
5. Click Submit.
6. When the Confirmation page displays, click Close to return to the ATM VC Configuration page.

The new interface should now display in the ATM VC Configuration table.

You may need to create a new WAN interface, or modify an existing interface, so that it uses the new VC. See the instructions for Configuring a PPP, EoA, or IPoA interfaces, depending on the type you use to communicate with your ISP.

You can verify that the new settings work by attempting to access the Internet from a LAN/USB computer. Contact your ISP for troubleshooting assistance.

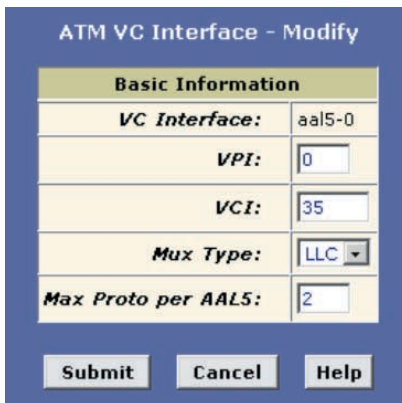
7. When you have verified that the new settings work properly, click the Admin tab, and then click Commit & Reboot in the task bar.
8. Click Commit to save your changes to permanent memory.

## Modifying ATM VCs

Your device may already be preconfigured with the necessary ATM VC properties, or the table may contain placeholder values that you must change before using the device. Contact your ISP to determine your ATM VC values. Follow these instructions to modify a preconfigured VC:

1. From the ATM VC Configuration page, click in the Action(s) column for the interface you want to modify.

The ATM VC Interface – Modify page displays, as shown in Figure 35.



Basic Information	
<b>VC Interface:</b>	aal5-0
<b>VPI:</b>	0
<b>VCI:</b>	35
<b>Mux Type:</b>	LLC
<b>Max Proto per AAL5:</b>	2

Submit Cancel Help

**Figure 35. ATM VC Interface –Modify Page**

2. Enter the new VPI and VCI values, select the MUX Type, or change the maximum number of protocols that the VC can carry, as directed by your ISP.

You cannot modify the interface type over which an existing VC operates (aal5-0, for example). If you want to change the interface type, you must delete the existing interface, create a new one, and select the desired interface type.

3. Click Submit.
4. On the Confirmation page, click Close to return to the ATM VC Configuration page.
5. Click the Admin tab, and then click Commit & Reboot in the task bar.
6. Click Commit to save your changes to permanent memory.

You can verify that the new settings work by attempting to access the Internet from a LAN/USB computer. Contact your ISP for troubleshooting assistance.

When powered on, the My ADSL Modem initiates a connection through your DSL line to your ISP.

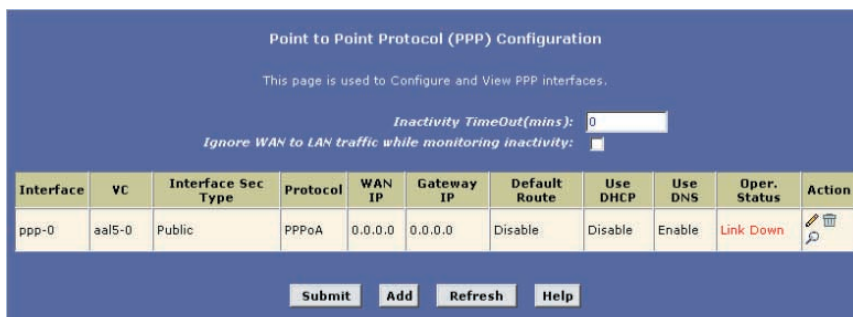
## Configuring PPP Interfaces

The point-to-point (PPP) protocol is commonly used between ISPs and their customers to identify and control various communication properties, including:

- Identifying the type of service the ISP provides to a given customer
- Identifying the customer to the ISP through a username and password login
- Enabling the ISP to assign Internet information to the customer's computers
- Your ISP may or may not use the PPP protocol. Contact your ISP to determine if you will need to change the default settings in order to connect to their server.

## Viewing Your Current PPP Configuration

To view your current PPP setup, log into Configuration Manager, click the WAN tab, and then click PPP in the task bar. The Point to Point Protocol (PPP) Configuration page displays, as shown in Figure 36.





Point to Point Protocol (PPP) Configuration

This page is used to Configure and View PPP interfaces.

Inactivity TimeOut(mins):

Ignore WAN to LAN traffic while monitoring inactivity: ☒

Interface	VC	Interface Sec Type	Protocol	WAN IP	Gateway IP	Default Route	Use DHCP	Use DNS	Oper. Status	Action
ppp-0	aal5-0	Public	PPPoA	0.0.0.0	0.0.0.0	Disable	Disable	Enable	Link Down	 

Submit Add Refresh Help

**Figure 36. Point to Point Protocol (PPP) Configuration Page**

PPP is configured as a group of software settings associated with the ADSL port. Although the device has only one physical ADSL port, the My ADSL Modem can be defined with more than one group of PPP settings. Each group of settings is called a PPP interface and is given a name, such as ppp-0, ppp-1, etc.





You can configure the following settings on the Point to Point Protocol (PPP) Configuration page:

**Inactivity TimeOut (mins):** The time in minutes that must elapse before a PPP connection times-out due to inactivity.

**Ignore WAN to LAN traffic while monitoring inactivity:** enabled, data traffic traveling in the incoming direction—from the WAN port to the LAN port—will not count as activity on the WAN port; i.e., the occurrence of WAN to LAN traffic will not prevent the connection from being terminated due to lack of activity in the WAN to LAN direction.

The PPP Configuration Table displays the following fields:

Field	Description
Interface	The predefined name of the PPP interface.
VC	The virtual circuit over which this PPP data is sent. The VC identifies the physical path the data takes to reach your ISP.
IPF Type (Interface Sec Type)	<p>The type of firewall protections that are in effect on the interface (Public, Private, or DMZ):</p> <p>A Public interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software.</p> <p>A Private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network.</p> <p>The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface -- whether from a LAN or external source -- are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness.</p>
Protocol	The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPPoE) or PPP-over-ATM (PPPoA).
WAN IP	The IP address currently assigned to your WAN (DSL) port by your ISP.
Gateway IP	The IP address of the server at your ISP that provides you access to the Internet. See Hops and gateway for a description of gateway addresses.
Default Route	Indicates whether the My ADSL Modem should use the IP address assigned to this connection as its default route. Can be Enable or Disable. See Quick Start for an explanation of default routes.
Use DHCP	When set to Enable, the device will acquire additional IP information from the ISP's DHCP server. The PPP connection itself acquires the device's IP address, mask, DNS address, and default gateway address. With the DHCP enabled, the device will acquire IP addresses for other various server types (WINS, SMTP, POP3, etc. -- these server types are listed on the DHCP Server Configuration page).

Use DNS	When set to Enable, the DNS address learned through the PPP connection will be distributed to clients of the device's DHCP server. This option is useful only when the My ADSL Modem is configured to act as a DHCP Server for your LAN. When set to Disable, LAN hosts will use the DNS address preconfigured in the DHCP pool (see Configuring DHCP Server) and in the DNS feature.
Oper. Status	Indicates whether the link is currently up or down or if a specific type of data exchange is under way (e.g., password authorization or DHCP).
Action	You can use these icons to modify  , delete  , and view additional details on  the PPP interface.
Viewing PPP Interface Details	When you click  to view additional details, the PPP Interface - Detail page displays, as shown in Figure 37.

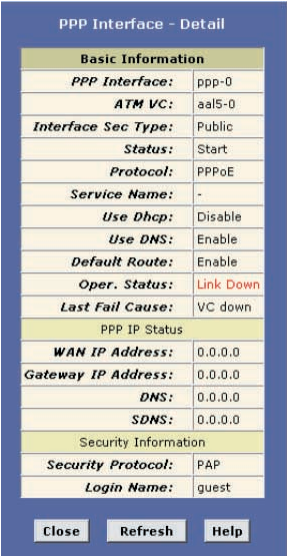


Figure 37. PPP – Detail Page

In addition to the properties defined previously, the Detail page displays these fields:

Field	Description
Status	Indicates whether the interface has been specified in the system as:
Enabled:	A connection will be established for use when the device is turned on or rebooted.

Disabled:	The PPP interface cannot currently be used.
Start:	The PPP connection will be made only when data is sent to the interface (e.g., when a LAN user attempts to use the Internet).
Service Name	(This feature is available with PPPoE interfaces but not with PPPoA interfaces.) The name of the ISP service you are using with this PPP connection. ISPs may offer different types of services (for example, for online gaming or business communications), each requiring a different login and other connection properties.
Last Fail Cause	<p>Indicates the action that ended the previous PPP session:</p> <p>No Valid PADO Recvd: The unit initiated a PPPoE handshake but did not receive a packet in reply from the ISP.</p> <p>No Valid PADS Recvd: After the initial handshake, the unit did not receive a confirmation packet from the ISP.</p> <p>Stopped by User: The user stopped the connection (for example, by changing the Configuration Manager settings for the PPP interface.)</p> <p>No Activity: The PPP communication timed out, in accordance with the timeout period specified on the PPP Configuration page.</p> <p>Auth Failure: The ISP could not authorize the connection based on the user name and/or password provided.</p> <p>PADT Recvd: The ISP issued a special packet type to terminate the PPP connection.</p> <p>VC down : The Virtual Circuit between the unit and the ISP is down.</p> <p>Internal failure: A system software failure occurred.</p>
DNS	The IP address of the DNS server (located with your ISP) used on this PPP connection.
SDNS	The IP address of the secondary DNS server (located with your ISP) used on this PPP connection.
Security Protocol	The type of PPP security your ISP uses: PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

## Login Name

The name you use to log in to your ISP each time this PPP connection is established.

**Adding a PPP Interface Definition** If you intend to use more than one type of service from your ISP, the device can be configured with multiple PPP interfaces, each with unique logon and other properties.

Follow this procedure to define properties for a PPP interface:

1. From the Point to Point Protocol (PPP) Configuration Page, click Add.

The PPP Interface – Add page displays, as shown in Figure 38.

PPP Interface - Add

**Basic Information**

PPP Interface: ppp-1

ATM VC: aal5-0

Interface Sec Type: Public

Status: Start

Protocol: ☐ PPPoA ☒ PPPoE

Service Name:

Use Dhcp: ☐ Enable ☒ Disable

Use DNS: ☐ Enable ☒ Disable

Default Route: ☒ Enable ☐ Disable

**Security Information**

Security Protocol: ☒ PAP ☐ CHAP

Login Name:

Password:

Submit Cancel Help

**Figure 38. PPP Interface – Add Page**

2. Select a PPP interface name from the drop-down list, and then enter or select data for each field.

**Note :** You can create multiple PPP interfaces only if you are using the PPPoA protocol; only one PPP interface can be defined if you are using PPPoE.

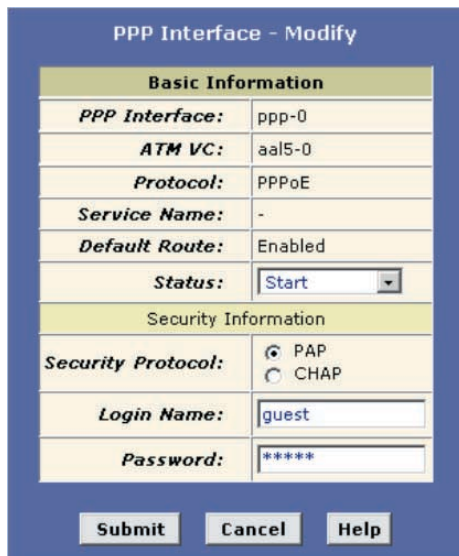
Check with your ISP which version of the protocol they require.

3. Click Submit. A page displays to confirm your changes.
4. Click Close to return to the PPP page and view the new interface in the table.
5. Click the Admin tab, and then click Commit & Reboot in the task bar.
6. Click Commit to save your changes to permanent memory.



## Modifying and Deleting PPP Interfaces

To modify a PPP interface, display the Point to Point Protocol (PPP) Configuration page and click in the Action(s) column for the interface you want to modify. The PPP Interface – Modify page displays, as shown in Figure 39.



Basic Information	
<b>PPP Interface:</b>	ppp-0
<b>ATM VC:</b>	aal5-0
<b>Protocol:</b>	PPPoE
<b>Service Name:</b>	-
<b>Default Route:</b>	Enabled
<b>Status:</b>	Start
Security Information	
<b>Security Protocol:</b>	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
<b>Login Name:</b>	guest
<b>Password:</b>	*****

Submit Cancel Help

**Figure 39. PPP Interface – Modify page**

You can change only the status of the PPP connection, the Security Protocol, your Login Name, and your Password. To modify the other settings, you must delete the interface and create a new one.

To delete a PPP Interface, display the PPP Configuration page and click in the Action column for the interface you want to delete. You should not delete a PPP Interface unless you have received instructions to do so from your ISP. Without an appropriately defined PPP Interface, you may not be able to connect to your ISP. You can recreate the PPP interface with the same name at a later time.

After modifying or deleting a PPP Interface, click Submit. Then, click the Admin tab, click Commit & Reboot in the task bar, and click Commit to save your changes to permanent memory.

## Configuring Ethernet-over-ATM

This chapter describes how to configure an Ethernet-over-ATM interface on the My ADSL Modem, if one is needed to communicate with your ISP.

### Overview of EOA

The Ethernet-over-ATM (EOA) protocol is often referred to as RFC1483, which is the Internet specification that defines it. It is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EOA protocol for data transfer with their customers' DSL modems.

EOA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EOA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.

Before creating an EOA interface or modifying the default settings, contact your ISP to determine which type of protocol they use.

**Note :** *PPP vs. EOA : Your ISP may use a protocol other than EOA for communication with the My ADSL Modem, such as the point-to-point protocol (PPP). One type of PPP, named PPP over Ethernet (PPPoE), actually works "on top" of the EOA protocol. The other type, PPP over ATM (PPPoA), does not. However, if your ISP uses either type of PPP, you do not need to separately create an EOA interface. See Configuring PPP Interfaces for instructions on creating or configuring a PPP interface.*

### Viewing Your EOA Setup

To view your current EOA configuration, log into Configuration Manager, click WAN in the task bar, and then click EOA. Figure 40 shows the RFC1483/Ethernet over ATM (EOA) Config page.



RFC1483/Ethernet over ATM(EoA) Config									
This Page is used to View, Add, Modify and Delete EOA Interfaces.									
Interface	Interface Sec Type	Lower Interface	Config IP Address	Netmask	Use Dhcp	Default Route	Gateway Address	Status	Action
eo-a-0	Public	aal5-0	9.25.67.11	255.255.255.0	Disable	Enable	9.25.67.10		
<div> <input type="button" value="Add"/> <input type="button" value="Refresh"/> <input type="button" value="Help"/> </div>									

**Figure 40. RFC1483/Ethernet over ATM (EOA) Config Page**

The EOA table contains a row for each EOA interface currently defined on the device. The table may contain no entries if your ISP does not use the EOA protocol.

The following table describes the fields on this page:

<b>Field</b>	<b>Description</b>
Interface	The name the software uses to identify the EOA interface.
IPF Type	<p>(Interface Sec Type)The type of security protections in effect on the interface (Public, Private, or DMZ):</p> <p>A Public interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software.</p> <p>A Private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network.</p> <p>The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface—whether from a LAN or external source—are subject to a level of protection that is in between those for public and private interfaces.</p>
Lower interface	EOA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port—the WAN port). This field should reflect an interface name defined in the next lower level of software over which the EOA interface will operate. This will be an ATM VC interface, such as aal5-0, as described in Configuring the ATM Virtual Circuit.
Config IP Address and Netmask	The IP address and network mask you want to assign to the interface. If the interface will be used for bridging with your ISP and you will not be using the My ADSL Modem as a router on your LAN, then you do not need to specify IP information. If you enable DHCP for this interface, then the Configured IP address will serve only as a request to the DHCP server. The actual address that is assigned by the ISP may differ if this address is not available.
Use DHCP	When Enable, this setting instructs the device to accept IP information assigned dynamically by your ISP's DHCP server. If the interface will be used for bridging with your ISP and you will not be routing data through it, leave this checkbox unselected.

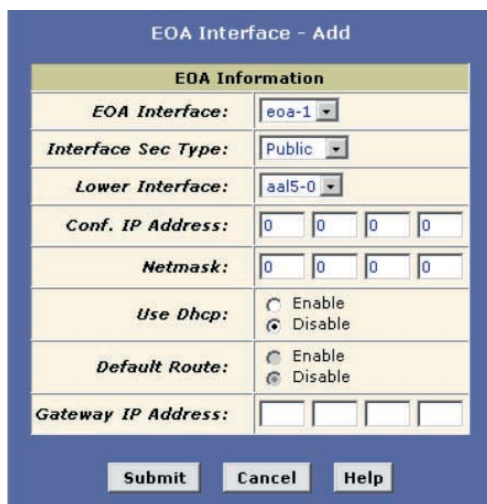
Default Route	Indicates whether the My ADSL Modem uses the IP address assigned to this interface, if any, as its default route for your LAN. Your system can have only one default route.
Gateway Address	The external IP address that the My ADSL Modem communicates with via the EOA interface to gain access to the Internet. This is typically an ISP server.
Status	A green or red ball will display to indicate that the interface is currently up or down, respectively. You cannot manually enable or disable the interface; a red ball may indicate a problem with the DSL connection.
Action	Icons you can click on to edit  or delete  the associated EOA interface.

## Adding EOA Interfaces

Follow these instructions to add an EOA interface:

1. Click the WAN tab, and then click EOA in the task bar.
2. Click Add.

The EOA Interface – Add page displays, as shown in Figure 41.



**Figure 41. EOA Interface – Add Page**

3. Select one of the predefined interface names from the EOA Interface drop down list.

4. From the IPF Type drop-down list, select the level of IP Firewall to be used on this interface.
5. In the Lower Interface field, select the lower-level interface name over which this protocol is being configured.

If you are using the My ADSL Modem as a bridge only, skip to step 10.

6. If you are using the My ADSL Modem as a router on your LAN, enter the IP address for the interface in the Conf. IP Address field, and enter the network Netmask.

This address serves as the public IP address for your entire LAN and is usually assigned by your ISP.

7. If your ISP will assign the IP address from their DHCP server, click the Enable radio button in the Use DHCP field.

When DHCP is Enabled, the address you entered in the Conf. IP Address field will be requested from the DHCP server; the server may assign a different address if necessary.

8. If you want the EOA interface to serve as the default route for Internet access for your LAN, click the Enable radio button in the Default Route field.
9. In the Gateway IP Address field, enter the address of the Internet computer to contact to gain initial access to the Internet.

10. Click Submit.

A confirmation page displays to confirm your changes.

11. Click Close to return to the EOA page and view the new interface in the table.
12. Click the Admin tab, and then click Commit & Reboot in the task bar.
13. Click Commit to save your changes to permanent memory.

# Configuring Internet Protocol-over-ATM

This chapter describes how to configure an IPoA (Internet Protocol-over-ATM) interface on the My ADSL Modem.

An IPoA interface can be used to exchange IP packets over the ATM network, without using an underlying Ethernet over ATM (EOA) connection. Typically, this type of interface is used only in product development and test environments, to eliminate unneeded variables when evaluating IP layer processing.

## Viewing Your IPoA Interface Setup

To configure an IPoA interface, log into Configuration Manager, click the WAN tab, and then click IPoA in the task bar. The IP over ATM (IPoA) Configuration page displays, as shown in Figure 42.

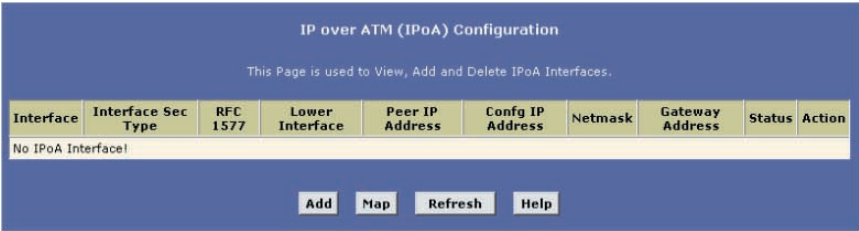


Figure 42. IPoA Configuration Page

The IPoA table contains a row for each EOA interface currently defined on the device. The table may initially contain no entries.

The following table describes the fields on this page:

Field	Description
Interface	The name the software uses to identify the IPoA interface
IPoA Type	1577 type: The PPP packets are encapsulated according to RFC 1577 for transmission over an ATM link.  Non 1577 type: RFC 1577 is not applied under this option.
Lower Interface	IPoA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port – the WAN port). This field should reflect an interface name defined in the next lower level of software over which the IPoA interface will operate. This will be an ATM VC interface, such as aal5-0.
Peer IP Address	The IP address of the remote computer you will be connecting to via the WAN interface.



IPF Type ( Interface Sec Type)	<p>The type of security protections in effect on the interface (Public, Private, or DMZ):</p> <p>A Public interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software.</p> <p>A Private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network.</p> <p>The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface—whether from a LAN or external source—are subject to a level of protection that is in between those for public and private interfaces.</p>
--------------------------------	--

## Config IP Address and Netmask

The IP address and network mask you want to assign to the interface. If DHCP is enabled, this address serves as a request to the remote computer's DHCP server, which may assign another address.

## Gateway Address

The external IP address that the My ADSL Modem communicates with via the IPoA interface to gain access to the Internet. This is typically an ISP server.

Field	Description
Status	A green or red ball will display to indicate that the interface is currently up or down, respectively. You cannot manually enable or disable the interface; a down interface may indicate a problem with the DSL connection.
Action	Icons you can click on to edit  or delete  the associated IPoA interface.

## Adding IPoA Interfaces

Follow these instructions to add an IPoA interface:

1. Display the IPoA page and click Add. The IPoA Interface – Add page displays, as shown in Figure 43.

**IPoA Interface - Add**

**IPoA Information**

**IPoA Interface:** ipoa-0

**Conf. IP Address:** 0 0 0 0

**Interface Sec Type:** Public

**Netmask:** 0 0 0 0

**RFC 1577:** ☐ Yes ☒ No

**Use DHCP:** ☐ Enable ☒ Disable

**Default Route:** ☒ Enable ☐ Disable

**Gateway IP Address:** 0 0 0 0

**Submit Cancel Help**

**Figure 43. IPoA Interface – Add Page**

2. Select the next available interface name from the IPoA Interface drop-down list.
3. In the Conf. IP Address and Netmask fields, type the address and mask that you want to assign to the IPoA interface.

If you enable the DHCP option, then the IP address you enter here will serve as a requested address; the remote computer may assign another address if necessary.
4. From the Interface Sec Type drop-down list, select the level of firewall security for the interface: Public, Private, or DMZ.
5. In the RFC 1577 field, click Yes radio button if the interface complies with the IETF specification RFC 1577, otherwise click No radio button. And click Add.
6. If the remote IPoA computer provides a DHCP server, you can click the Enable radio button in the Use DHCP field to have the IP address dynamically assigned from the server.
7. If you want the IPoA interface to serve as the default route for your LAN, click the Enable radio button in the Default Route field.
8. In the Gateway IP Address field, enter the address of the Internet computer to contact to gain initial access to the Internet.
9. Click Submit. A confirmation page will display to confirm your changes.



10. Click Close to return to the IPoA page and view the new interface in the table.
11. Click the Admin tab, and then click Commit & Reboot in the task bar.
12. Click Commit to save your changes to permanent memory.

## Configuring Bridging

---

The My ADSL Modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN. This chapter describes how to configure the My ADSL Modem to operate as a bridge.

**Note :** Before changing your bridge configuration, check with your ISP to determine the type of connection they use to exchange data with their customer's DSL modems (such as Ethernet bridging or IP routing).

### Overview of Bridges

A bridge is a device used to connect two or more networks so they can exchange data. A bridge learns the unique manufacturer-assigned hardware IDs of each computer or device on both (or all) networks it is attached to. It learns that some of the IDs represent computers attached via one of the device's interfaces and others represent computers connected via other interfaces. For example, the hardware IDs of your home computers are attached via the Ethernet port, and the hardware IDs of your ISP's computers are attached via the WAN (DSL) port. It stores the ID list and the interface associated with each ID in its bridge forwarding table.

When the bridge receives a data packet, it compares its destination hardware ID to the entries in the bridge forwarding table. When the packet's ID matches one of the entries, it forwards the packet through the interface that connects to the corresponding network. Note that the bridge does not send the data directly to the receiving computer, but broadcasts it to the receiving network, making it available to any node on that network.

On the receiving network, a LAN protocol such as Ethernet takes over, helping the packet reaches its destination.

When the bridge does not recognize a packet's destination hardware ID, it broadcasts the packet through all of its interfaces – to each network it is attached to.

**Note :** *Bridges vs. Routers : The essential difference between a bridge and a router is that a router uses a higher-level protocol (such as IP) to determine how to pass data. IP data packets contain IP addresses that specifically identify the destination computer. Routers can read this information and pass the data to the destination computer, or determine which next router to send the data to if the destination is not on a connected network.*

Bridges cannot read IP information, but instead refer to the hardware ID of the destination computer, which is also included in data packets.

Hardware IDs are unique numbers that manufacturers assign to each piece of hardware they sell. A bridge learns to recognize the hardware IDs accessible through each of its ports. When it receives a packet, the bridge simply forwards the packet through the port it associates with the given hardware ID, or through all its ports if it does not recognize the ID. The hardware ID is often referred to as the Media Access Control (MAC) address.

Routers are considered more intelligent and flexible devices than bridges, and often provide a variety of security and network administration services based on the IP protocols.

## When to Use the Bridging Feature

Although the My ADSL Modem is preconfigured to serve as a router for providing Internet connectivity to your LAN, there are several instances in which you may also want to configure bridging:

Your ISP may use protocols that require bridging with your LAN. The device can be configured to appear as a bridge when communicating with your ISP, while continuing to provide router functionality for your LAN.

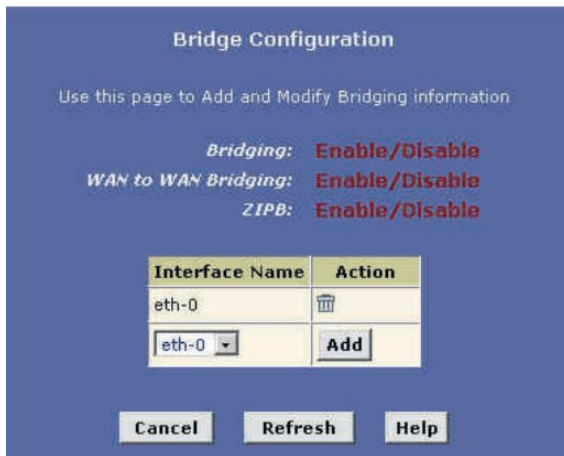
Your LAN may include computers that communicate using layer-3 protocols other than the Internet Protocol. These include IPX® and AppleTalk®. In this case, the device can be configured to act as a bridge for packets that use these protocols while continuing to serve as a router for IP data.

## Defining Bridge Interfaces

To enable bridging, you simply specify the device interfaces on which you want to bridge data, and then enable bridging mode:

1. Log into Configuration Manager and click the Bridging tab.


The Bridge Configuration page displays, as shown in Figure 44.



**Bridge Configuration**

Use this page to Add and Modify Bridging information

**Bridging:** Enable/Disable  
**WAN to WAN Bridging:** Enable/Disable  
**ZTPB:** Enable/Disable

Interface Name	Action
eth-0	
<input type="text" value="eth-0"/>	<input type="button" value="Add"/>

**Figure 44. Bridge Configuration page**

2. The page displays Bridge Configuration items, and a table for specifying the interfaces on which bridging will be performed. The table may be empty if bridging has not yet been configured.
3. Select the Interface Names on which you want to perform bridging and click Add.

For example, select eth-0 (LAN) and eoa-0 (WAN) interfaces. If you use a USB-connected computer, you can also select usb-0.

**Note :** *If you enable bridging on an interface that has already been assigned an IP address, then it is considered IP-enabled and will route (rather than bridge) IP packets received on the interface. The interface will bridge non-IP data it receives, however.*

You can determine whether the Ethernet (eth-0) and USB (usb-0) interfaces have been assigned IP addresses by displaying the IP Address Table (display the Routing tab, and then click IP Address).

These interfaces will display in the table only if they have been assigned IP addresses.

You can check whether the eoa-0 interface has been assigned an IP address by displaying the EOA configuration table (click the WAN tab, and then click EOA). If the Config IP Address field is empty and the Use DHCP field contains the word Disable, then no IP address has been assigned.

**System Mode**

This page is used to enable/disable various system features.

Feature	Enabled	Disabled
<b>Bridging:</b>	<input checked="" type="radio"/>	<input type="radio"/>
<b>WAN to WAN Bridging:</b>	<input checked="" type="radio"/>	<input type="radio"/>
<b>BRAS:</b>	<input type="radio"/>	<input checked="" type="radio"/>
<b>ZIPB:</b>	<input type="radio"/>	<input checked="" type="radio"/>


**Figure 44.1. System Mode page**

4. Click Bridging Enabled/Disabled to enter System Mode.
5. Click the Bridging Enabled radio button to turn on bridging. Do not click the ZIPB Enabled button unless you want to configure the mode.
6. Click Submit.

A page will briefly display to confirm your changes, and will return you to the Bridge Configuration page.

7. Click the Admin tab, and then click Commit & Reboot in the task bar.
8. Click Commit to save your changes to permanent memory.

## Deleting a Bridge Interface

To make an interface non-bridgeable, display the Bridge Configuration page and click  next to the interface you want to delete. Click OK to confirm the deletion. The interface remains defined in the system, but is no longer capable of performing bridging.

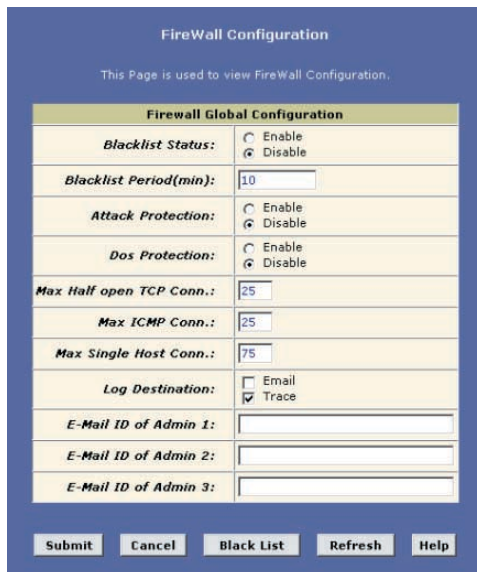
Configuration Manager provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other unwelcome or malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

## Configuring Global Firewall Settings

Follow these instructions to configure global firewall settings:

1. Log into Configuration Manager, click the Services tab, and then click  Firewall in the task bar.

The Firewall Configuration page displays, as shown in Figure 45.



The screenshot shows the 'FireWall Configuration' window. It has a title bar and a subtitle 'This Page is used to view FireWall Configuration.' Below this is a table titled 'Firewall Global Configuration'. The table contains several rows with configuration options and their current values. At the bottom of the window are five buttons: 'Submit', 'Cancel', 'Black List', 'Refresh', and 'Help'.

Firewall Global Configuration	
<b>Blacklist Status:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Blacklist Period(min):</b>	<input type="text" value="10"/>
<b>Attack Protection:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Dos Protection:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Max Half open TCP Conn.:</b>	<input type="text" value="25"/>
<b>Max ICMP Conn.:</b>	<input type="text" value="25"/>
<b>Max Single Host Conn.:</b>	<input type="text" value="75"/>
<b>Log Destination:</b>	<input type="checkbox"/> Email <input checked="" type="checkbox"/> Trace
<b>E-Mail ID of Admin 1:</b>	<input type="text"/>
<b>E-Mail ID of Admin 2:</b>	<input type="text"/>
<b>E-Mail ID of Admin 3:</b>	<input type="text"/>

Buttons: Submit, Cancel, Black List, Refresh, Help

**Figure 45. Firewall Configuration Page**

2. Configure any of the following settings that display in the Firewall Global Information table:

Field	Description
Blacklist Status	If you want the device to maintain and use a black list, click Enable. Click Disable if you do not want to maintain a list.
Blacklist Period(min)	Specifies the number of minutes that a computer's IP address will remain on the black list (i.e., all traffic originating from that computer will be blocked from passing through any interface on the My ADSL Modem). For more information, see Managing the Black List.
Attack Protection	Click the Enable radio button to use the built-in firewall protections that prevent the following common types of attacks:
IP Spoofing:	Sending packets over the WAN interface using an internal LAN IP address as the source address.
Tear Drop:	Sending packets that contain overlapping fragments.
Smurf and Fraggle:	Sending packets that use the WAN or LAN IP broadcast address as the source address.
Land Attack:	Sending packets that use the same address as the source and destination address.
Ping of Death:	Illegal IP packet length.
Dos Protection	Click the Enable radio button to use the following denial of service protections:
SYN DoS ICMP DoS Per-host DoS protection Max Half open TCP Conn.	<p>Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions.</p> <p>If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.</p>
Max ICMP Conn.	<p>Sets the percentage of concurrent IP sessions that can be used for ICMP messages.</p> <p>If the percentage is exceeded, then older ICMP IP sessions will be replaced by new sessions as the are initiated.</p>

Field	Description
Max Single Host Conn.	Sets the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.
Log Destination	Specifies how attempted violations of the firewall settings will be tracked. Records of such events can be sent via Ethernet to be handled by a system utility Ethernet to (Trace) or be e-mailed to specified administrators.
E-mail ID of Admin 1/2/3	Specifies the e-mail addresses of the administrators who should receive notices of any attempted firewall violations. Type the addresses in standard internet e-mail address format, e.g., jxsmith@onecompany.com.  The e-mail message will contain the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring the previous 30 minutes. If the ICMP protocol were being used, then instead of the source and destination ports, the e-mail will report the ICMP code and type.

3. Click Submit.
4. Click the Admin tab, and then click Commit & Reboot in the task bar.
5. Click Commit to save your changes to permanent memory.

## Managing the Black List


If data packets are received that violate the firewall settings or any of the IP filter rules, then the source IP address of the offending packets can be blocked from such accesses for a specified period of time. You can enable or disable use of the black list using the settings described above. The source computer remains on the black list for the period of time that you specify.

To view the list of currently blacklisted computers, click Black List at the bottom of the Firewall Configuration page. The Firewall Blacklisted Hosts page displays, as shown in Figure 46.



**Figure 46. Firewall Blacklisted Hosts Page**

The table displays the following information for each entry:

Field	Description
Host IP Address	The IP address of the computer that sent the packet(s) that caused the violation
Reason	A short description of the type of violation. If the packet violated an IP filter rule, the custom text from the Log Tag field will display. (See Creating IP Filter Rules)
IPF Rule ID	If the packet violated an IP filter rule, this field will display the ID assigned to the rule.
Action(s)	Displays an icon  you can click on to delete the entry from the list, if you want it to be removed prior to its automatic timed expiration.



---

## Configuring IP Filters & Blocked Protocols

---

This chapter describes two Configuration Manager features that enable you to control the data passing through your network:

The IP filter feature enables you to create rules to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN. Although IP filter rules provide a very flexible and powerful tool to enhance network security and control user activity, they can also be complex and generally require an advanced understanding of IP protocols.

The blocked protocols feature enables you to simply select from a predefined list the protocol that you want to block. All data passed to the My ADSL Modem using a blocked protocol will be discarded, without consideration of the source computer, destination computer, or the device interface on which it was received.

### Configuring IP Filters

When you define an IP filter rule and enable the feature, you instruct the My ADSL Modem to examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the size of the packet, the network or internet protocol it is carrying, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data.

If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

### Viewing Your IP Filter Configuration

To view your current IP filter configuration, log into Configuration Manager, click the Services tab, and then click IP Filter in the task bar. The IP Filter Configuration page displays, as shown in Figure 47.

IP Filter Configuration

This Page is used to View and Modify IP Filter Global and Rule Configuration.

Security Level: 

None

Public Default Action: 

Accept

Private Default Action: 

Deny

DMZ Default Action: 

Accept

Rule ID	I/F	Apply Stateful Inspection	Direction	Rule Action	In I/F	Log Option	Rule Description	Oper. Status	Action(s)
10	ALL	Disable	Incoming	Deny	N/A	Disable	-		 Stats
20	ALL	Disable	Incoming	Deny	N/A	Disable	1.Dest IP equal to 255.255.255.255		 Stats
30	Private	Enable	Incoming	Accept	N/A	Disable	-		 Stats
40	Private	Enable	Outgoing	Accept	ALL	Disable	-		 Stats
50	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq UDP 2.Dest Port equal to 53		 Stats
60	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq TCP 2.TCP Flag all 3.Dest Port equal to 53		 Stats
70	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq TCP 2.TCP Flag all 3.Dest Port equal to 25		 Stats
80	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq TCP 2.TCP Flag all 3.Dest Port equal to 110		 Stats

Submit

Cancel

Add

Session

Refresh

Help

Figure 47. IP Filter Configuration Page

The IP Filter Configuration page displays global settings that you can modify, and the IP filter rule table, which shows all currently established rules. See [Creating IP Filter Rules](#) for a description of the items that make up a rule. When rules are defined, you can use the icons that display in the Action(s) column to edit , delete , and view details on the corresponding rule.

## Configuring IP Filter Global Settings

The IP Filter Configuration page enables you to configure the following global IP filter settings.

**Security Level:** This setting determines which IP filter rules take effect, based on the security level specified in each rule. For example, when High is selected, only those rules that are assigned a security value of High will be in effect. The same is true for the Medium and Low settings.

When None is selected, IP filtering is disabled.

**Private Default Action / Public Default Action / DMZ Default Action:**

This setting specifies a default action to be taken (Accept or Deny) on Private, Public, or DMZ-type device interfaces when they receive packets that do not match any of the filtering rules. You can specify a different default action for each interface type. (You specify an interface's type when you create the interface; see the [PPP configuration page](#), for example.)

A Public interface typically connects to the Internet. PPP, EoA, and IPoA interfaces are typically public. Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. Typically, the global setting for public interfaces is Deny, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP filter rule.

A Private interface connects to your LAN, such as the Ethernet interface.

Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. Typically, the global setting for private interfaces is Accept, so that LAN computers have access to the My ADSL Modems' Internet connection.

The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface—a whether from a LAN or external source—are subject to a set of protections that is in between Public and Private interfaces in terms of restrictiveness. The global setting for DMZ-type interfaces may be set to Deny so that all attempts to access these servers are denied by default; the administrator may then configure IP filter rules to allow accesses of certain types.

## Creating IP Filter Rules

To create an IP filter rule, you set various criteria that must be met in order for the rule to be invoked. Use these instructions to add a new IP filter rule:

1. On the IP Filter Configuration page, click Add.

The IP Filter Rule - Add page displays, as shown in Figure 48.

**IP Filter Rule - Add**

☒ Enable ☐ Disable

**Basic Information**

<b>Rule ID:</b>	<input type="text"/>	<b>Action:</b>	<input type="radio"/> Accept <input checked="" type="radio"/> Deny
<b>Direction:</b>	<input type="radio"/> Incoming <input checked="" type="radio"/> Outgoing	<b>Interface:</b>	<input type="text" value="ALL"/>
<b>In Interface:</b>	<input type="text" value="ALL"/>	<b>Log Option:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Security Level:</b>	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Low	<b>Blacklist Status:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Log Tag:</b>	<input type="text"/>		
<b>Start Time (HH MM SS):</b>	<input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/>	<b>End Time (HH MM SS):</b>	<input type="text" value="23"/> <input type="text" value="59"/> <input type="text" value="59"/>

**Src IP Address:**

**Dest IP Address:**

**Protocol:**

**Store State:** ☐

**Source Port:**

**Dest Port:**

**TCP Flag:**

**ICMP Type:**

**ICMP Code:**

**IP Frag Pkt:** ☐ Yes  
☐ No  
☒ Ignore

**IP Option Pkt:** ☐ Yes  
☐ No  
☒ Ignore

**Packet Size:**

**TOD Rule Status :** ☒ Enable  
☐ Disable

**Figure 48. IP Filter Rule - Add Page**

2. Enter or select data for each field that applies to your rule. The following table describes the fields:

Field	Description
Rule ID	Each rule must be assigned a sequential ID number. Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (e.g., 10, 20, 30) so that you leave enough room between them for inserting a new rule if necessary.
Action	The action that will be taken when a packet matches the rule criteria. The action can be Accept (forward to destination) or Deny (discard the packet).
Direction	<p>Specifies whether the rule should apply to data packets that are incoming or outgoing on the selected interface.</p> <p>Incoming refers to packets coming from the LAN, and Outgoing refers to packets going to the Internet.</p> <p>You can use rules that specify the incoming direction to restrict external computers from accessing your LAN.</p>
Interface	The interface on the My ADSL Modem on which the rule will take effect. See the following examples for suggestions on choosing the appropriate interface for various rule types.
In Interface	The interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only for the outgoing direction.
Log Option	<p>When Enable is selected, a log entry will be created on the system each time this rule is invoked. The log entry will include the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring in the previous x minutes. (Logging may be helpful when troubleshooting.) This information can also be e-mailed to designated administrators. See Configuring Firewall Settings for instructions.</p>
Security Level	The security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to Medium and the global firewall level is set to Medium, then the rule will be active; but if the global firewall level is set to High or Low, then the rule will be inactive.

Blacklist Status	Specifies whether or not a violation of this rule will result in the offending computer's IP address being added to the Black List, which blocks the My ADSL Modem from forwarding packets from that source for a specified period of time. See <i>Configuring Firewall Settings</i> for instructions.																				
Log Tag	A description of up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to Enable if you configure a Log Tag.																				
Start Time, End Time	The time range during which this rule is to be in effect, specified in military units.																				
Src IP Address Dest IP Address	<p>IP address criteria for the source computer(s) (from which the packet originates) and the destination computer. In the drop-down list, you can configure the rule to be invoked on packets containing:</p> <table><tr><td>any :</td><td>any source IP address.</td></tr><tr><td>lt :</td><td>any source IP address that is numerically less than the specified address.</td></tr><tr><td>lteq :</td><td>any source IP address that is numerically less than or equal to the specified address.</td></tr><tr><td>gt :</td><td>any source IP address that is numerically greater than the specified address.</td></tr><tr><td>eq :</td><td>any source IP address that is numerically equal to the specified address.</td></tr><tr><td>neq :</td><td>any source IP address that is not equal to the specified address.</td></tr><tr><td>range:</td><td>any source IP address that is within the specified range, inclusive.</td></tr><tr><td>out of range:</td><td>any source IP address that is outside the specified range.</td></tr><tr><td>self :</td><td>the IP address of the My ADSL Modem interface on which this rule takes effect.</td></tr><tr><td>bcast:</td><td>(destination address only) Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select</td></tr></table>	any :	any source IP address.	lt :	any source IP address that is numerically less than the specified address.	lteq :	any source IP address that is numerically less than or equal to the specified address.	gt :	any source IP address that is numerically greater than the specified address.	eq :	any source IP address that is numerically equal to the specified address.	neq :	any source IP address that is not equal to the specified address.	range:	any source IP address that is within the specified range, inclusive.	out of range:	any source IP address that is outside the specified range.	self :	the IP address of the My ADSL Modem interface on which this rule takes effect.	bcast:	(destination address only) Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select
any :	any source IP address.																				
lt :	any source IP address that is numerically less than the specified address.																				
lteq :	any source IP address that is numerically less than or equal to the specified address.																				
gt :	any source IP address that is numerically greater than the specified address.																				
eq :	any source IP address that is numerically equal to the specified address.																				
neq :	any source IP address that is not equal to the specified address.																				
range:	any source IP address that is within the specified range, inclusive.																				
out of range:	any source IP address that is outside the specified range.																				
self :	the IP address of the My ADSL Modem interface on which this rule takes effect.																				
bcast:	(destination address only) Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select																				

this option, you do not need to specify the address, so the address fields are dimmed.

Protocol	<p>The basic IP protocol criteria that must be met for rule to be invoked. Using the options in the drop-down list, you can specify that packets must contain the selected protocol (eq), that they must not contain the specified protocol (neq), or that the rule can be invoked regardless of the protocol (any). TCP, UDP, and ICMP are commonly IP protocols; others can be identified by number from 0-255, as defined by the Internet Assigned Numbers Authority (IANA).</p>
Store State	<p>When this option is enabled, packets are monitored for their state (i.e., whether they are the initiating packet or a subsequent packet in an ongoing communication, etc). This option provides a degree of security by blocking/dropping packets that are not received in the anticipated state. Such packets can signify unwelcome attempt to gain access to a network.</p>
Source Port Dest Port	<p>Port number criteria for the source computer(s) (from which the packet originates) and destination computers.</p> <p>Port numbers identify the type of traffic that the computer or server can handle and are specified by the Internet Assigned Numbers Authority (IANA). For example, port number 80 indicates a Web server, 21 indicates an FTP server.</p> <p>You can choose a port type by name from the drop-down lists or, if not available in the list, specify the IANA port number in the text boxes. Select Any other port if the criteria will not be used.</p> <p>These fields will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol.</p> <p>See the description of Src IP Address for the statement options (any, eq, gt, etc.)</p>
TCP Flag	<p>Specifies whether the rule should apply only to TCP packets that contain the synchronous (SYN) flag, only to those that contain the non-synchronous (NOT-SYN) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.</p>

ICMP Type	Specifies whether the value in the type field in ICMP packet headers will be used as criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (eq) or not equal (neq) the specified value, or you can select any to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
ICMP Code	Specifies whether the value in the code field in ICMP packet headers will be used as criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (eq) or not equal (neq) the specified value, or you can select any to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
IP Frag Pkt	<p>Determines how the rule applies to IP packets that contain fragments. You can choose from the following options:</p> <p>Yes: The rule will be applied only to packets that contain fragments.</p> <p>No: The rule will be applied only to packets that do not contain fragments.</p> <p>Ignore: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.</p>
IP Option Pkt	<p>Determines whether the rule should apply to IP packets that have options specified in their packet headers.</p> <p>Yes: The rule will be applied only to packets that contain header options.</p> <p>No: The rule will be applied only to packets that do not contain header options.</p> <p>Ignore: (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.</p>
Packet Size	Specifies that the IP filter rule will take affect only on packets whose size in bytes matches this criterion. (lt = less than, gt = greater than, lteq = less than or equal to, etc.)
TOD Rule Status	<p>The Time of Day Rule Status determines how the Start Time/End Time settings are used.</p> <p>Enable: (Default) The rule is in effect for the specified time period.</p>



Disable: The rule is not in effect for the specified time period, but is effective at all other times.

3. When you are done selecting criteria, ensure that the Enable radio button is selected at the top of the page, and then click Submit.

After a confirmation page displays, the IP Filter Configuration page will redisplay with the new rule showing in the table.

If the security level of the rule matches the globally configured setting, a green ball in the Status column for that rule, indicating that the rule is now in effect. A red ball will display when the rule is disabled or if its security level is different from the globally configured level.

4. Ensure that the Security Level and Private Default Action / Public Default Action / DMZ Default Action settings on the IP Filter Configuration page are configured as needed, then click Submit

A page displays to confirm your changes.

5. Click the Admin tab, and then click Commit & Reboot in the task bar.
6. Click Commit to save your changes to permanent memory.

## **IP filter rule examples – Example 1**

Blocking a specific computer on your LAN from using accessing web servers on the Internet:

1. Add a new rule for outgoing packets on the ppp-0 interface from any incoming interface (this would include the eth-0 and usb-0 interfaces, for example).
2. Specify a source IP address of the computer you want to block.
3. Specify the Protocol = TCP and enable the Store State setting.
4. Select the TCP Protocol, and then specify a destination port = 80, which is the well-known port number for web servers.
5. Enable the rule by clicking the radio button at the top of the page.
6. Click Submit to create the rule.
7. On the IP Filter Configuration page, set the Security Level to the same level you chose for the rule, and set both the Private Default Action and the Public Default Action to Accept.
8. Click Submit, and commit your changes.

Figure 48 shows the configuration for this rule. The specified computer will not be able to access the Web, but will be able to access FTP Internet sites (and any others that use destination port numbers other than 80).

## IP filter rule examples – Example 2

Blocking Telnet accesses to the My ADSL Modem:

1. Add a new rule for packets incoming on the ppp-0 interface.
2. Specify that the packet must contain the TCP protocol, and must be destined for port 23, the well-known port number used for the Telnet protocol.
3. Enable the rule by clicking the radio button at the top of the page.
4. Click Submit to create the rule, and commit your changes.

Figure 49 shows how this rule could be configured:

**IP Filter Rule - Add**

☒ Enable ☐ Disable

Basic Information	
<b>Rule ID:</b>	<input type="text"/>
<b>Action:</b>	<input type="radio"/> Accept <input checked="" type="radio"/> Deny
<b>Direction:</b>	<input type="radio"/> Incoming <input checked="" type="radio"/> Outgoing
<b>Interface:</b>	<input type="text" value="ppp-0"/>
<b>In Interface:</b>	<input type="text" value="ALL"/>
<b>Log Option:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Security Level:</b>	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Low
<b>Blacklist Status:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Log Tag:</b>	<input type="text"/>
<b>Start Time (HH MM SS):</b>	<input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/>
<b>End Time (HH MM SS):</b>	<input type="text" value="23"/> <input type="text" value="59"/> <input type="text" value="59"/>
<b>Src IP Address:</b>	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
<b>Dest IP Address:</b>	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
<b>Protocol:</b>	<input type="text" value="eq"/> <input type="text" value="TCP"/>
<b>Store State:</b>	<input type="checkbox"/>
<b>Source Port:</b>	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/>
<b>Dest Port:</b>	<input type="text" value="eq"/> <input type="text" value="23"/> <input type="text" value="0"/>
<b>TCP Flag:</b>	<input type="text" value="All"/>
<b>ICMP Type:</b>	<input type="text" value="any"/> <input type="text" value="Echo Reply"/>
<b>ICMP Code:</b>	<input type="text" value="any"/> <input type="text" value="0"/>
<b>IP Frag Pkt:</b>	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore
<b>IP Option Pkt:</b>	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore
<b>Packet Size:</b>	<input type="text" value="any"/> <input type="text" value="0"/>
<b>TOD Rule Status :</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Figure 49. IP Filter Rule –Add page.

## Viewing IP Filter Statistics

For each rule, you can view statistics on how many packets were accepted or denied. Display the IP Filter Configuration page, and then click Stats in the row corresponding to the rule. The IP Filter Rule – Statistics page displays, as shown in Figure 50.

IP Filter Rule – Statistics

IP Filter Rule Statistic	
<b>Rule ID:</b>	10
<b>Number of Packets Matching this Rule:</b>	0 Packets

Clear
Close
Refresh
Help






**Figure 50. IP Filter Rule – Statistics Page**

You can click Clear to reset the count to zero and Refresh to display newly accumulated data.

## Managing Current IP Filter Sessions


When two computers communicate using the IP protocol, an IP session is created for the duration of the communication. The My ADSL Modem allows a fixed number of concurrent IP sessions. You can view information about each current IP session and delete sessions (for security reasons, for example).

To view all current IP sessions, display the IP Filter Configuration page, and then click Session. The IP Filter Session displays as shown in Figure 51.

IP Filter Session										
Session Index	Time to expire	Protocol	I/F	IP Address	Port	In Rule Index	In Action	Out Rule Index	Out Action	Action (s)
1	252	UDP	eth-0 Self	10.0.20.70 255.255.255.255	9830 69	30 0	Accept Unknown	30 0	Accept Unknown	
2	60	TCP	eth-0 Self	192.168.51.138 192.168.51.239	1721 80	30 0	Accept Unknown	30 0	Accept Unknown	
4	132	UDP	eth-0 Self	192.168.51.120 192.168.51.255	138 138	30 0	Accept Unknown	30 0	Accept Unknown	
8	12	UDP	eth-0 Self	192.168.51.162 192.168.51.255	138 138	0 0	Unknown Unknown	0 0	Unknown Unknown	
13	122	UDP	eth-0 Self	192.168.51.115 192.168.51.255	138 138	30 0	Accept Unknown	30 0	Accept Unknown	

**Figure 51. IP Filter Session Page**

The IP Filter Session table displays the following fields for each current IP session:

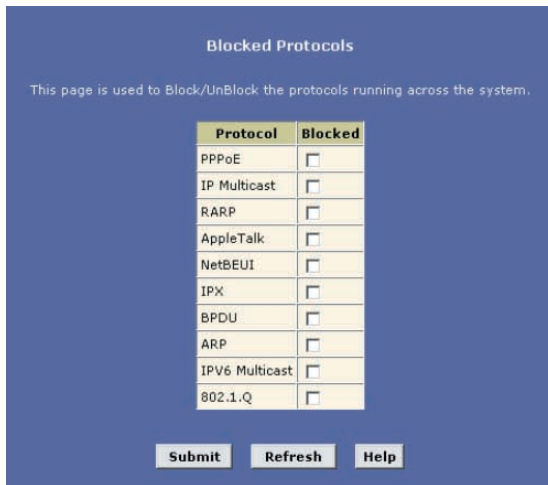
Field	Description
Session Index	The ID assigned by the system to the IP session (all sessions, whether or not they are affected by an IP filter rule, are assigned a session index).
Time to expire	/The number of seconds in which the connection will automatically expire
Protocol	The underlying IP protocol used on the connection, such as TCP, UDP, IGMP, etc.
I/F	The interface on which the IP filter rule is effective
IP Address	The IP addresses involved in the communication. The first one shown is the initiator of the communication.
Port	The hardware addresses of the ports involved in the communication
In Rule Index, Out Rule Index	The number of the IP filter rule that is applies to this session (assigned when the rule was created)
In Action, Out Action	The action (Accept, Deny, or Unknown), being taken on data coming into or going out on the interface. This action is specified in the rule definition.
Action(s)	Provides an icon you can click on  to delete the IP session. When you delete a session, the communication between is discontinued.

You can click Refresh to display newly accumulated data.

## Blocked Protocols

The Blocked Protocols feature enables you to prevent the My ADSL Modem from passing any data that uses a particular protocol. Unlike the IP filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations. However, when you are certain that a particular protocol is not needed or wanted on your network, this feature provides a convenient way to discard such data before it is passed.

To display the Blocked Protocols page, click the Services tab, and then click Blocked Protocols in the task bar. The Blocked Protocols page displays, as shown in Figure 52.



Protocol	Blocked
PPPoE	<input type="checkbox"/>
IP Multicast	<input type="checkbox"/>
RARP	<input type="checkbox"/>
AppleTalk	<input type="checkbox"/>
NetBEUI	<input type="checkbox"/>
IPX	<input type="checkbox"/>
BPDUI	<input type="checkbox"/>
ARP	<input type="checkbox"/>
IPV6 Multicast	<input type="checkbox"/>
802.1.Q	<input type="checkbox"/>

Submit Refresh Help

**Figure 52. Blocked Protocols Page**

**Warning :** *Blocking certain protocols may disrupt or disable your network communication or Internet access. If you are unfamiliar with how your network or Internet connection uses these protocols, contact your ISP before disabling.*

The following list describes each of the available protocols.

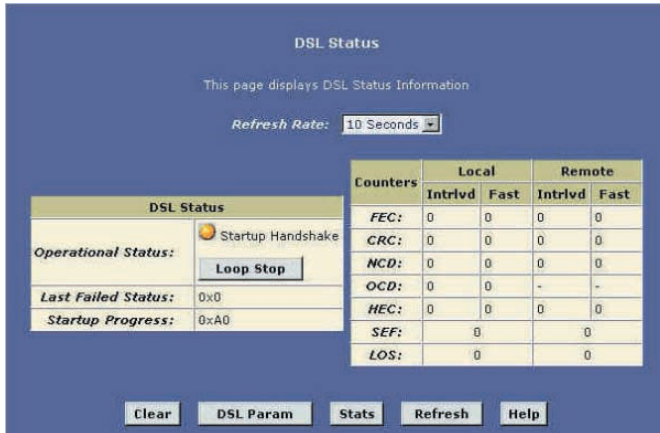
Protocol	Description
PPPoE	Point-to-Point Protocol over Ethernet. Many DSL modems use PPPoE to establish and maintain a connection with a service provider. PPPoE provides a means of logging in to the ISPs servers so that they can authenticate you as a customer and provide you access to the Internet. Check with your ISP before blocking this protocol.

IP Multicast	IP Multicast is an extension to the IP protocol. It enables individual packets to be sent to multiple hosts on the Internet, and is often used for handling e-mail mailing lists and teleconferencing/videoconferencing.
RARP	Reverse Address Resolution Protocol. This IP protocol provides a way for computers to determine their own IP addresses when they only know their hardware address (i.e., MAC addresses). Certain types of computers, such as diskless workstations, must use RARP to determine their IP address before communicating with other network devices.
AppleTalk	A networking protocol used in for Apple Macintosh® networks.
NetBEUI	NetBIOS Enhanced User Interface. On many LAN operating systems, the NetBEUI protocol provides the method by which computers identify themselves to and communicate with each other.
IPX	Internet work Packet Exchange. A networking protocol used on Novell Netware -based LANs.
BPDU	Bridge Protocol Data Unit. BPDUs are data messages that are exchanged across the switches between LANs that are connected by a bridge. BPDU packets contain information on ports, addresses, priorities, and costs, and are exchanged across bridges to detect and eliminate loops in a network.
Protocol	Description
ARP	Address Resolution Protocol. Computers on a LAN use ARP to learn the hardware addresses (i.e., MAC addresses) of other computers when they know only their IP addresses.
IPV6 Multicast	IP Multicasting under IP Protocol version 6. See IP Multicast above.
802.1.Q	This IEEE specification defines a protocol for virtual LANs on Ethernet networks. A virtual LAN is a group of PCs that function as a local area network, even though the PCs may not be physically connected. They are commonly used to facilitate administration of large networks.

To block a protocol, click the appropriate check box, and click Submit. After you have verified that the device continues to function as expected, click the Admin tab, click Commit & Reboot in the task bar, and then click Commit to save your changes to permanent memory.

## Viewing a DSL Line Information

To view configuration parameters and performance statistics for the My ADSL Modem's DSL line, log into Configuration Manager, and then click the WAN tab. The DSL Status page displays by default, as shown in Figure 53.



**Figure 53. DSL Status Page**

The DSL Status page displays current information on the DSL line performance. The page refreshes according to the setting in the Refresh Rate drop-down list, which you can configure.

In the DSL Status table, the Operational Status setting displays a red, orange, or green ball to indicate that the DSL line is idle, starting up, or up-and-running, respectively. You can click Loop Stop to end the DSL connection. To restart the connection, you can click Loop Start.

Although you generally will not need to view the remaining data, it may be helpful when troubleshooting connection or performance problems with your ISP.

You can click Clear to reset all counters to zero, and Refresh to redisplay the page with newly accumulated values.

You can click DSL Parameter to display data about the configuration of the DSL line, as shown in Figure 54.

DSL Parameter

DSL Parameters and Status	
<b>Vendor ID:</b>	00B5GSPN
<b>Revision Number:</b>	T93.3.8
<b>Serial Number:</b>	123456789abcdx
<b>Local Tx Power:</b>	0.0 dB
<b>Remote Tx Power:</b>	0.0 dB
<b>Local Line Atten.:</b>	0.5 dB
<b>Remote Line Atten.:</b>	0.5 dB
<b>Local SNR Margin:</b>	0.0 dB
<b>Remote SNR Margin:</b>	0.0 dB
<b>Self Test:</b>	Passed
<b>DSL Standard:</b>	T1.413
<b>Trellis Coding:</b>	Disable
<b>Framing Structure:</b>	Framing-0

Config Data	Up		Down	
	Intrvlcd	Fast	Intrvlcd	Fast
<b>AS0(kbps):</b>	-	-	0	0
<b>AS1(kbps):</b>	-	-	0	0
<b>LS0(kbps):</b>	0	0	-	-
<b>LS1(kbps):</b>	0	0	-	-
<b>RValue:</b>	0	0	0	0
<b>SValue:</b>	0		0	
<b>DValue:</b>	0		0	

Close

Refresh

Help

**Figure 54. DSL Parameter Page**

The DSL Parameters and Status table displays settings preconfigured by the product manufacturer or your ISP.

The Config Data table lists various types of error and defects measurements found on the DSL line.

You cannot modify this data.

From the DSL Status page, you can click Stats to display DSL line performance statistics, as shown in Figure 55.

**Figure 55. DSL Statistics Page**

DSL Statistics

No. of 15 Min. Valid Data Intervals: 0

No. of 15 Min. Invalid Data Intervals: 0

Current 15-Min Interval Statistics	
Elapsed Time(MM:SS):	0:0
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0
Current Day Statistics	
Elapsed Time(HH:MM:SS):	0:0:0
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0
Previous Day Statistics	
Monitored Time(HH:MM:SS):	0:0:0
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0

Detailed Interval Statistic (Past 24 hrs)					
1-4	5-8	9-12	13-16	17-20	21-24

Close	Refresh	Help
-------	---------	------



The DSL Statistics page reports error data relating to the last 15-minute interval, the current day, and the previous day.

At the bottom of the page, the Detailed Interval Statistic (Past 24 hrs) table displays links you can click on to display detailed data for each 15-minute interval in the past 24 hours. For example, when you click on 1-4, data displays for the 16 intervals (15-minutes each) that make up the previous 4 hours. Figure 56 shows an example.

DSL Interval Statistics				
15-Min Interval No.	Errored Seconds	Severely Errored Seconds	Unavailable Seconds	Valid Data
1	0	0	0	No
2	0	0	0	No
3	0	0	0	No
4	0	0	0	No
5	0	0	0	No
6	0	0	0	No
7	0	0	0	No
8	0	0	0	No
9	0	0	0	No
10	0	0	0	No
11	0	0	0	No
12	0	0	0	No
13	0	0	0	No
14	0	0	0	No
15	0	0	0	No
16	0	0	0	No

Detailed Interval Statistic (Past 24 hrs)					
<a href="#">1-4</a>	<a href="#">5-8</a>	<a href="#">9-12</a>	<a href="#">13-16</a>	<a href="#">17-20</a>	<a href="#">21-24</a>

<a href="#">Close</a>	<a href="#">Refresh</a>	<a href="#">Help</a>
-----------------------	-------------------------	----------------------

**Figure 56. DSL Interval Statistics Page**

---

## Administrative Tasks

---

This chapter describes the following administrative tasks that you can perform using Configuration Manager:

- Configuring User Names and Passwords
- Viewing System Alarms
- Upgrading the Software
- Using Diagnostics
- Modifying Port Settings

You can access these tasks from the Admin tab task bar. The other Admin tasks listed in the Admin tab—Configuring User Logon and Committing and Rebooting—are described in *Getting Started with the Configuration Manager*.

### Configuring User Names and Passwords

The My ADSL Modem is configured with a default user name and password combination, or login, for accessing Configuration Manager.

If you want to allow other users to access the program, you can create additional user logins and specify their privilege levels. You can also change the password for the default login or for any logins you create.

### Creating and Deleting Logins

The default login allows the user full access to all Configuration Manager features, including creating up to four additional user logins. You can assign either of two privilege levels to each additional login:

- Root-level privileges enable the user to modify all the features available in Configuration Manager. The default login has root-level privileges.
- User-level privileges enable the user to login and view – but not create or modify – system information. These users can change their own password, however.

To create additional logins or modify them, follow these instructions:

1. Log into Configuration Manager using the default user name and password, and then click the Admin tab.

The User Configuration page displays by default, as shown in Figure 57.



**User Configuration**

This page displays user information. Use this page to add/delete users and change your password. Your new password can be up to 64 characters and is case-sensitive.

User ID	Privilege	Action(s)
root	Root	

**Figure 57. User Configuration Page**

- Click Add to display the User Config-Add page, as shown in Figure 57.1



**User Config - Add**

**New User Information**

<b>User ID:</b>	<input type="text"/>
<b>Privilege:</b>	<input type="radio"/> Root <input type="radio"/> Intermediate <input checked="" type="radio"/> User
<b>Password:</b>	<input type="text"/>
<b>Confirm Password:</b>	<input type="text"/>

**Figure 57.1 User Config-Add page**

- Type the User ID and Password in the text boxes provided, and then select the privilege level for this user.

The user name can be up to 128 characters, but cannot contain spaces or special characters.

The password can be up to eight characters. Be sure to retype the password in the Confirm Password text box, exactly as before, including lower and upper case characters.

- Click Submit.
- Click the Admin tab, and then click Commit & Reboot in the task bar.
- Click Commit to save your changes to permanent memory.

You cannot change or delete the default login. To delete a subsequently created login, click in the corresponding Action(s) column in the table on the User Configuration page.

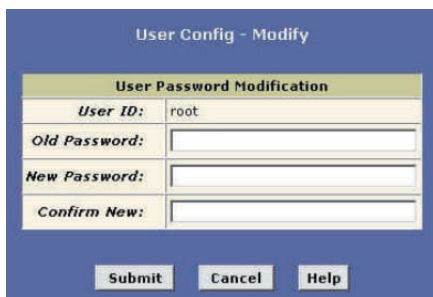
## Changing Login Passwords

You can change your own log in password and, if you have root privileges, other user's passwords. Follow these instructions to change a login password.

**Note :** *This user ID and password is used only for logging into the Configuration Manager; it is not the same as the login you may use to connect to your ISP.*

1. From the User Configuration page, click next to the login whose password you want to modify.

The User Config-Modify page displays, as shown in Figure 57.2.



The screenshot shows a web interface titled "User Config - Modify". Inside, there is a section titled "User Password Modification". This section contains four labeled text input fields: "User ID:" (with "root" entered), "Old Password:", "New Password:", and "Confirm New:". Below these fields are three buttons: "Submit", "Cancel", and "Help".

**Figure 57.2 User Config-Modify page**

2. Type the new password in exactly the same way in both text boxes.

The password can be up to eight ASCII characters long. When logging in, you must type the New password in the same upper and lower case characters that you use here.

3. Click Submit.
4. Click the Admin tab, and then click Commit & Reboot in the task bar.
5. Click Commit to save your changes to permanent memory.

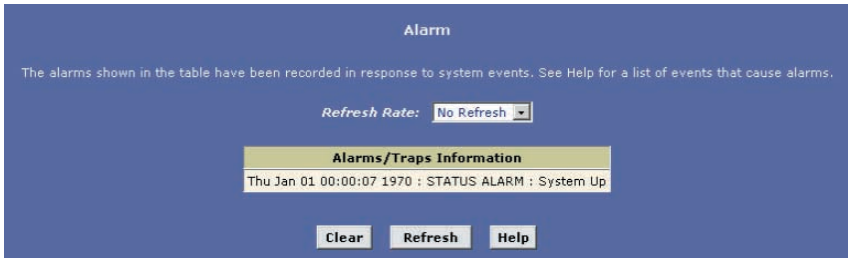
## Viewing System Alarms

You can use the Configuration Manager to view information about alarms that occur in the system. Alarms, also called traps, are caused by a variety of system events, including connection attempts, resets, and configuration changes.

Although you will not typically need to view this information, it may be helpful in working with your ISP to troubleshoot problems you encounter with the device. (Despite their name, not all alarms indicate problems in the functioning of the system.)

## Viewing the Alarm Table

To display the Alarm page, log into the Configuration Manager, click the Admin tab, and then click Alarm in the task bar. The Alarm page is shown in Figure 58.



**Figure 58. Alarm Page**

Each row in the table displays the time and date that an alarm occurred, the type of alarm, and a brief statement indicating its cause.

You can click on the Refresh Rate drop-down list to select a recurring time interval after which the page will redisplay with new data.

To remove all entries from the list, click Clear. New entries will begin accumulating and will display when you click Refresh.

## Upgrading the Software

Your ISP may from time to time provide you with an upgrade to the software running on the My ADSL Modem. All system software is contained in a single file, called an image. The image is composed of several distinct parts, each of which implements a different set of functions.

Configuration Manager provides an easy way to upload a new software image, or a specific part of the image, to the memory on the My ADSL Modem. To upgrade the image, follow this procedure:

### Local Image Upgrade

1. Log into Configuration Manager, click the Admin tab, and then click Local Image Upgrade in the task bar.

The Local Image Upgrade page is shown in Figure 59.



**Figure 59. Local Image Upgrade Page**

2. In the Source Filename text box, type the path and file name of the file as provided by your ISP. You can click Browse... to search for it on your hard drive.

The name of the upgrade file must be one of the following:

- TEImage.bin
- TEDsl.gsz
- TEAppl.gsz
- Filesys.bin
- TEPatch.bin

3. Click Upload.

The following message box displays at the bottom of the page:

Loading New Software:

Please do not interrupt the upgrade process. A status page will appear automatically when loading is completed (about 1 minute)

When loading is complete, the following message displays (the file name may differ):

File: TEDsl.gsz successfully saved to flash. Please reboot for the new image to take effect.

4. Turn power to the unit off, wait a few seconds, and turn it on again.

The new software will now be in effect. If the system fails to boot or is not working properly, contact your ISP for troubleshooting assistance.

## Remote Image Upgrade

1. Log into Configuration Manager, click Admin tab, and then click Remote Image Upgrade in the task bar.

The Remote Image Upgrade page is shown in Figure 59.1.

**Figure 59.1. Remote Image Upgrade page**

2. In the IP Address text boxes, type the IP address of the server from which the file is to be downloaded. Contact your ISP if you do not have this information.
3. In the Upgrade File text box, type the complete name of the file to be downloaded.

**Note :** *The name of the upgrade file must be one of the following:*

*-TEImage.bin*

*-TEPatch.bin*

4. In the Username and Password fields, type the information required to log on the ISP's server (if needed).
5. Click Upload.

An alert window pops up displaying the following message:

Image upgrade may take a few minutes after which the system will reboot.

Click OK to start the image upgrade.

When image upgrade is complete, the following message displays:

Remote Image Upgrade Successful...

6. The system will proceed to reboot itself automatically. Wait 1 minute to allow the reboot to complete, then refresh your browser and log in again to the device.

## Using Diagnostics

The diagnostics feature executes a series of test of your system software and hardware connections. Use this feature when working with your ISP to troubleshoot problems.

Follow these instructions to begin the diagnostics program:

1. Log into Configuration Manager, click the Admin tab, and then click Diagnostics in the task bar. Figure 60 shows the Diagnostics page.

Diagnostics		
This page is used for performing diagnostics on the system.		
ATM VC: aal5-0		
<b>Testing Connectivity to modem</b>		
Testing Ethernet connection	UNKNOWN	<a href="#">Help</a>
Testing ADSL line for sync	UNKNOWN	<a href="#">Help</a>
Testing Ethernet connection to ATM	UNKNOWN	<a href="#">Help</a>
<b>Testing Telco Connectivity</b>		
Testing ATM OAM segment ping	UNKNOWN	<a href="#">Help</a>
Testing ATM OAM end to end ping	UNKNOWN	<a href="#">Help</a>
<b>Testing ISP Connectivity</b>		
Testing PPPoE server connectivity	UNKNOWN	<a href="#">Help</a>
Testing PPPoE server session	UNKNOWN	<a href="#">Help</a>
Testing authentication with server	UNKNOWN	<a href="#">Help</a>
Validating assigned IP address 0.0.0.0	UNKNOWN	<a href="#">Help</a>
<b>Testing Internet Connectivity</b>		
Ping default gateway 0.0.0.0	UNKNOWN	<a href="#">Help</a>
Ping Primary Domain Name Server	UNKNOWN	<a href="#">Help</a>
Query DNS for www.globespanvirata.com	UNKNOWN	<a href="#">Help</a>
Ping www.globespanvirata.com	UNKNOWN	<a href="#">Help</a>
<input type="button" value="Submit"/> <input type="button" value="Help"/>		

**Figure 60. Diagnostics Page**

2. From the WAN Interface drop-down list, select the name of the WAN interface currently defined on your system.
3. Click Submit.

The diagnostics utility will run a series of test to check whether the device's connections are up and working. This takes only a few seconds and the results for each test are displayed on screen. A test may be skipped if the program determines that no suitable interface is configured on which to run the test.

You can click Help to display an explanation of each test. Work with your ISP to interpret the results of the diagnostic tests.



## Modifying Port Settings

### Overview of IP port numbers

The header information in an IP data packet specifies a destination port number. Routers use the port number along with the specified IP addresses to forward the packet to its intended recipient.

For example, all IP data packets that the My ADSL Modem receives from the Internet specify the same IP address (your public IP address) as the destination. However, depending on the port number contained in data packets, the My ADSL Modem may pass the packet on to its embedded Web or Telnet servers, or to another computer on the network.

The Internet community has developed a list of common server types such as HTTP, Telnet, e-mail, and many others, and assigned a unique port number to each. These are not mandatory, but are useful in promoting communication between separately administered LANs.

### Modifying the My ADSL Modem's port numbers

In some cases, you may want to assign non-standard port numbers to the HTTP and Telnet servers that are embedded on the My ADSL Modem. The following scenario is one example where changing the HTTP port number may be necessary:

You have an externally visible Web server on your LAN, with a NAT rule (RDR flavor) that redirects incoming HTTP packets to that Web server. When incoming packets contain a destination IP address of your public IP address (which is assigned to the My ADSL Modem's WAN port) and the standard Web server port number of 80, the NAT rule recognizes the port number and redirects the packets to your Web server's local IP address.

Assume in this scenario that you also want to enable external access to the My ADSL Modem's Configuration Manager, so that your ISP can log in and manage your system, for example. Accessing Configuration Manager requires accessing the My ADSL Modem's own Web server (also called its HTTP server). In this case, you would want to use the Port Settings feature to assign a non-standard port number to the My ADSL Modem's HTTP server. Without a non-standard port number, the NAT rule would redirect your ISP's log in attempt to your LAN HTTP server rather than to the HTTP server on the My ADSL Modem.

Thereafter, when your ISP wants to log on to your Configuration Manager, they would type your IP address in their browser, followed by a colon and the non-standard port number, as shown in this example: `http://10.0.1.16:61000`

Your ISP may also have special circumstances that require changing the port numbers; contact them before making any changes here.

Follow these steps to modify port settings:

1. Log into Configuration Manager, click the Admin tab, and then click Port Settings in the task bar. The Port Settings page is shown in Figure 61.

**Port Settings**

This page is used to modify various port settings across the system.

<b>HTTP Port:</b> (80, 61000-62000)	<input type="text" value="80"/>
<b>Telnet Port:</b> (23, 61000-62000)	<input type="text" value="23"/>
<b>FTP Port:</b> (21, 61000-62000)	<input type="text" value="21"/>

**Figure 61. Port Settings Page**

2. Type the new port number(s) in the appropriate text box(es) and click Submit.

The default port numbers are shown in Figure 61. You can enter non-standard port numbers in the range 61000-62000.

3. Click Commit & Reboot in the task bar, and click Commit to save your changes to permanent memory.
4. On the Commit & Reboot page, click Reboot.

Note that the new settings will not be effective until you reboot the system.

## Appendix A: IP Addresses, Network Masks, and Subnets

### IP Addresses

*Note : This section pertains only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.*

This section assumes basic knowledge of binary numbers, bits, and bytes. For details on this subject, see Appendix B.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called dotted decimal notation. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

### Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information.

- **Network ID** Identifies a particular network within the Internet or intranet
- **Host ID** Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's class (see following section). Table 4 shows the structure of an IP address.

	Field 1	Field 2	Field 3	Field4
<b>Class A</b>	Network ID	Host ID		
<b>Class B</b>	Network ID		Host ID	
<b>Class C</b>	Network ID			Host ID

**IP Address structure**

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

## Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

The class can be determined easily from field1:

field1 = 1-126: Class A

field1 = 128-191: Class B

field1 = 192-223: Class C

(field1 values not shown are reserved for special uses)

A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

## Subnet masks

Definition : A mask looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."

Subnet masks are used to define subnets (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask: 255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field 3 are part of the network ID, but note how the mask specifies that the first bit in field 4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 0 to 127 (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 0 to 63.

*Note : Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:*

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

These are called default because they are used when a network is initially configured, at which time it has no subnets.

## Binary Numbers

In everyday life, we use the decimal system of numbers. In decimal, numbers are written using the ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. Computers, however, do not use decimal. Instead, they use binary.

Definition (binary numbers) : Binary numbers are numbers written using only the two digits 0 and 1, e.g., 110100.

Hint : Does "base ten" sound familiar? (Think grade school.) Base ten is just another name for decimal. Similarly, base two is binary.

Just as each digit in a decimal number represents a multiple of 10 (1, 10, 100, 1000, 10,000, etc.), each digit in a binary number represents a multiple of 2 (1, 2, 4, 8, 16, etc.). For example:

Decimal				Binary			
1,000's	100's	10's	1's	8's	4's	2's	1's
-	-	1	3 =	1	1	0	1

Also, since binary uses only two digits to represent all numbers, a binary number has more digits than the same number in decimal. In the example above, you can see that the decimal number 13 is the same as the binary number 1101 ( $8 + 4 + 1 = 13$ ).

## Bits and bytes

---

Computers handle binary numbers by grouping them into units of distinct sizes. The smallest unit is called a bit, and the most commonly used unit is called a byte.

Definition (bit and byte) : A bit is a single binary digit, i.e., 0 or 1.

A byte is a group of eight consecutive bits (the ) number of bits can vary with computers, but is almost always eight), e.g., 11011001. The value of a byte ranges from 0 (00000000) to 255 (11111111). The following shows the values of the eight digits in a byte along with a sample value:

128's	64's	32's	16's	8's	4's	2's	1's
1	0	1	0	1	1	0	1

The decimal value of this byte is 173 ( $128 + 32 + 8 + 4 + 1 = 173$ ).

## Appendix B: Troubleshooting

This troubleshooting suggests solutions for problems you may encounter in installing or using the My ADSL Modem, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

### LEDs

*Power LED does not illuminate after product is turned on.*

Verify that you are using the power cable provided with the device and that it is securely connected to the My ADSL Modem and a wall socket/power strip.

*ACT WAN LED does not illuminate after phone cable is attached.*

Verify that a standard telephone cable (called an RJ-11 cable) like the one provided is securely connected to the ADSL port and your wall phone jack. Allow about 30 seconds for the device to negotiate a connection with your ISP.

*LINK LAN LED does not illuminate after Ethernet cable is attached.*

Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the My ADSL Modem. Make sure the PC and/or hub is turned on.

Verify that you are using a straight-through type Ethernet cable to the uplink port on a hub. If you connected the device to an ordinary hub port (not Uplink), you must use a straight-through cable. (To check: hold the connectors at each end of the cable side-by-side with the plastic spring facing down. Looking at the wires from left to right, if the first, second, third, and sixth wires are the same color on the two connectors, then it is a straight-through type.)

Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.

### Internet Access

*My PC cannot access Internet*

Use the ping utility, discussed in the following section, to check whether your PC can communicate with the My ADSL Modem's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.

If you statically assigned a private IP address to the computer, (not a registered public address), verify the following:

- Check that the gateway IP address on the computer is your public IP address (see the Quick Start chapter, Part 2 for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically.

- Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.
- Verify that a Network Address Translation rule has been defined on the My ADSL Modem to translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules. Or, configure the PC to accept an address assigned by another device (see the Quick Start, Part 2). The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool (see the instructions in Chapter to view the address pool)

*My LAN PCs cannot display web pages on the Internet.*

Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the My ADSL Modem is correct, then You can use the ping utility to test connectivity with your ISP's DNS server.

## Configuration Manager Program

*I forgot/lost my Configuration Manager user ID or password.*

If you have not changed the password from the default, try using root as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing the Reset button on the back panel of the device three times (using a pointed object such as a pen tip). Then, type the default User ID and password shown above.

WARNING: Resetting the device removes any custom settings and returns all settings to their default values.

*I cannot access the configuration Manager program from your browser.*

Use the ping utility, discussed in the following section, to check whether your PC can communicate with the My ADSL Modem's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.

Verify that you are using Internet Explorer V5.0 or later, or Netscape Navigator v6.1 or later. Support for Javascript® must be enabled in your browser. Support for Java® may also be required.

Verify that the PC's IP address is defined as being on the same subnet as the IP Address assigned to the LAN port on the My ADSL Modem

*My changes to Configuration Manager are not being retained.*

Be sure to use the Commit function after any changes.



## Diagnosing Problem using IP Utilities

### ping

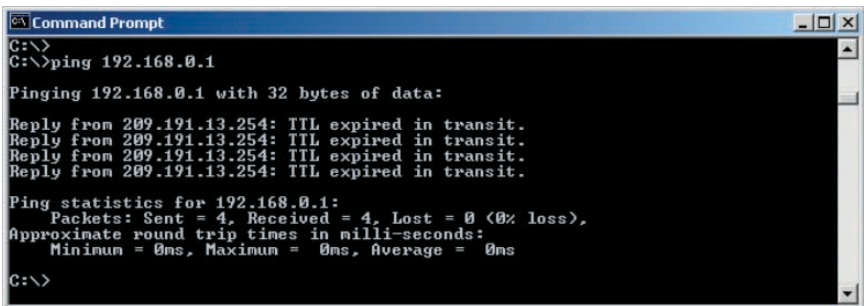
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following:

```
ping 192.168.1.1
```

Click OK. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window displays like that shown in Figure 62



```
Command Prompt
C:\>
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

**Figure 62. Using the ping Utility**

If the target computer cannot be located, you will receive the message Request timed out.

Using the ping command, you can test whether the path to the My ADSL Modem is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for [www.yahoo.com](http://www.yahoo.com) (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

## Nslookup

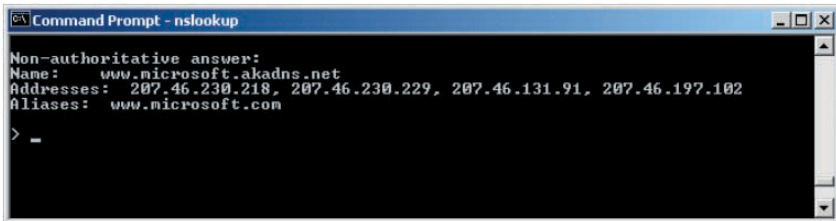
You can use the nslookup command to determine the IP address associated with an internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the Start button, and then click Run. In the Open text box, type the following:

```
nslookup
```

Click OK. A Command Prompt-nslookup window displays with a bracket prompt (>). At the prompt, type the name of the internet address your are interested in, such as `www.microsoft.com`.

The window will display the associate IP address, if known, as shown in Figure 63



**Figure 63. Using the nslookup Utility**

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information. To exit from the nslookup utility, type `exit` and press Enter at the command prompt.

---

## Glossary

---

10BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See also data rate, Ethernet.
100BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See also data rate, Ethernet.
ADSL	Asymmetric Digital Subscriber Line. The most commonly deployed flavor of DSL for home users. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.
analog	Of data, having a form is analogous to the data's original waveform. The voice component in DSL is an analog signal. See also digital.
ATM	Asynchronous Transfer Mode A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See also data rate.
authenticate	To verify a user's identity, such as by prompting for a password.
binary	The "base two" system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See also bit, IP address, network mask.
bit	Short for "binary digit," a bit is a number that can have two values, 0 or 1. See also binary.
bps	bits per second

bridging	Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The My ADSL Modem can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See also routing.
broadband	A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
Broadcast	To send data to all computers on a network.
CO	Central Office A circuit switch that terminates all the local access lines in a particular geographic serving area; a physical building where the local switching equipment is found. xDSL lines running from a subscriber's home connect at their serving central office.
DHCP	Dynamic Host Configuration Protocol DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
DHCP relay	Dynamic Host Configuration Protocol relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the My ADSL Modem's interfaces can be configured as a DHCP relay. See DHCP.
DHCP server	Dynamic Host Configuration Protocol server. A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.
digital	Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See also analog.
DNS	Domain Name System. The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See also domain name.

domain name	A domain name is a user-friendly name used in place of its associated IP address. For example, <a href="http://www.globespan.net">www.globespan.net</a> is the domain name associated with IP address 209.191.4.240. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site, e.g., <a href="http://www.globespan.net/index.html">http://www.globespan.net/index.html</a> . See also DNS.
download	To transfer data in the downstream direction, i.e., from the Internet to the user.
DSL	Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also BASE-T, 100BASE-T, twisted pair.
Filtering	To screen out selected types of data, based on filtering rules. Filtering can be applied in one direction (upstream or downstream), or in both directions.
filtering rule	A rule that specifies what kinds of data a routing device will accept and/or reject. Filtering rules are defined to operate on an interface (or multiple interfaces) and in a particular direction (upstream, downstream, or both).
Firewall	Any method of protecting a computer or LAN connected to the Internet from intrusion or attack from the outside. Some firewall protection can be provided by packet filtering and Network Address Translation services.
FTP	File Transfer Protocol - A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.
GGP	Gateway to Gateway Protocol. An Internet protocol that specifies how gateway routers communicate with each other.
Gbps	Abbreviation for Gigabits (GIG-uh-bits) per second, or one billion bits per second. Internet data rates are often expressed in Gbps.
GRE	Generic Routing Encapsulation. TCP/IP protocol suite, transport layer encapsulation protocol.

hop	When you send data through the Internet, it is sent first from your computer to a router, and then from one router to another until it finally reaches a router that is directly connected to the recipient. Each individual “leg” of the data’s journey is called a hop.
hop count	The number of hops that data has taken on its route to its destination. Alternatively, the maximum number of hops that a packet is allowed to take before being discarded , See also TTL.
host	A device (usually a computer) connected to a network.
HTTP	Hyper-Text Transfer Protocol HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See also web browser
ICMP	Internet Control Message Protocol An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.
IGMP	Internet Group Management Protocol An Internet protocol that enables a computer to share information about its membership in multicast groups with adjacent routers. A multicast group of computers is one whose members have designated as interested in receiving specific content from the others. Multicasting to an IGMP group can be used to simultaneously update the address books of a group of mobile computer users or to send company newsletters to a distribution list.
in-line filter	See Microfilter
Internet	The global collection of interconnected networks used for both private and business communications.
intranet	A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.
IP	See TCP/IP.
IP address	Internet Protocol address The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See also domain name, network mask.

ISP	Internet Service Provider A company that provides Internet access to its customers, usually for a fee.
LAN	Local Area Network A network limited to a small geographic area, such as a home, office, or small building.
LED	Light Emitting Diode An electronic light-emitting device. The indicator lights on the front of the My ADSL Modem are LEDs.
MAC address	Media Access Control address The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of characters.
mask	: See network mask.
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.
Microfilter	In splitterless deployments, a microfilter is a device that removes the data frequencies in the DSL signal, so that telephone users do not experience interference (noise) from the data signals. Microfilter types include in-line (installs between phone and jack) and wall-mount (telephone jack with built-in microfilter). See also splitterless.
NAT	Network Address Translation A service performed by many routers that translates your network's publicly known IP address into a Private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.
NAT rule	A defined method for translating between public and private IP addresses on your LAN.
network	A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.
network mask	A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See also binary, IP address, subnet

NIC	Network Interface Card An adapter card that plugs into your computer and provides the physical interface to your network cabling, which for Ethernet NICs is typically an RJ-45 connector. See Ethernet, RJ-45.
packet	Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).
ping	Packet Internet (or Inter-Network) Groper A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.
port	A physical access point to a device such as a computer or router, through which data flows into and out of the device.
POTS	Plain Old Telephone Service Traditional analog telephone service using copper telephone lines. Pronounced pots. See also PSTN.
POTS splitter :	See splitter.
PPP	Point-to-Point Protocol A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the My ADSL Modem uses two forms of PPP called PPPoA and PPPoE. See also PPPoA, PPPoE.
PPPoA	Point-to-Point Protocol over ATM One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.
PPPoE	Point-to-Point Protocol over Ethernet One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.
protocol	A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.
remote	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.



---

RIP	Routing Information Protocol The original TCP/IP routing protocol. There are two versions of RIP: version and version II.
RJ-11	Registered Jack Standard-11 The standard plug used to connect telephones, fax machines, modems, etc. to a telephone jack. It is a 6-pin connector usually containing four wires.
RJ-45	Registered Jack Standard-45 The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
routing	Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.
rule	See filtering rule, NAT rule.
SDNS	Secondary Domain Name System (server) A DNS server that can be used if the primary DSN server is not available. See DNS.
SNMP	Simple Network Management Protocol The TCP/IP protocol used for network management.
splitter	A device that splits off the voice component of the DSL signal to a separate line, so that data and telephone service each have their own wiring and jacks. The splitter is installed by your telephone company where the DSL line enters your home. The CO also contains splitters that separate the voice and data signals, sending voice to the PSTN and data on high-speed lines to the Internet. See also CO, PSTN, splitterless, microfilter.
splitterless	A type of DSL installation where no splitter is installed, saving the cost of a service call by the telephone company. Instead, each jack in the home carries both voice and data, requiring a microfilter for each telephone to prevent interference from the data signal. ADSL is usually splitterless; if you are unsure if your installation has a splitter, ask your DSL provider. See also splitter, microfilter.
subnet	A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask which selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See also network mask.

subnet mask	A mask that defines a subnet. See also network mask.
TCP	See TCP/IP.
TCP/IP	Transmission Control Protocol/Internet Protocol The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.
Telnet	An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.
TFTP	Trivial File Transfer Protocol. A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
TTL	Time To Live A field in an IP packet that limits the life span of that packet. Originally meant as a time duration, the TTL is usually represented instead as a maximum hop count; each router that receives a packet decrements this field by one. When the TTL reaches zero, the packet is discarded.
twisted pair	The ordinary copper telephone wiring long used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See also 10BASE-T, 100BASE-T, Ethernet.
upstream	The direction of data transmission from the user to the Internet.
USB	Universal Serial Bus A serial interface that lets you connect devices such as printers, scanners, etc. to your computer by simply plugging them in. The My ADSL Modem is equipped with a USB interface for connecting to a stand-alone PC.
VC	Virtual Circuit A connection from your ADSL router to your ISP.

VCI	Virtual Circuit Identifier Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See also VC.
VPI	Virtual Path Identifier Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See also VC.
WAN	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the My ADSL Modem, WAN refers to the Internet.
Web browser	A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See also HTTP, web site, WWW.
Web page	A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the Home page. See also hyperlink, web site.
Web site	A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See also hyperlink, web page.
WWW	World Wide Web Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.

## Registering your NetComm Product

---

All NetComm Limited (“NetComm”) products have a standard 12 month warranty from date of purchase against defects in manufacturing and that the products will operate in accordance with the specifications outlined in the User Guide. However some products have an extended warranty option (please refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at:

**[www.netcomm.com.au](http://www.netcomm.com.au)**

## Contact Information

If you have any technical difficulties with your product, please do not hesitate to contact NetComm’s Customer Support Department.

Email: [support@netcomm.com.au](mailto:support@netcomm.com.au)

Fax: (+612) 9424-2010

Web: [www.netcomm.com.au](http://www.netcomm.com.au)

**NOTE:** *NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in this User Guide or contact a Network Specialist.*

---

## Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

## Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

- (1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.
- (2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
  - Change the direction or relocate the receiving antenna.
  - Increase the separation between this equipment and the receiver.
  - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
  - Consult an experienced radio/TV technician for help.
- (3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

## Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

## Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at [www.netcomm.com.au](http://www.netcomm.com.au).



# NetComm™

## My ADSL Modem

### PACKAGE CONTENTS

NB3 ADSL Ethernet/USB Modem  
Cat-5 RJ45 straight-through Ethernet Cable  
RJ11 Line Cord  
USB Cable  
605 to RJ11 Line Adaptor  
Power Pack 12V DC, 600mA  
Driver/Manual/Utility Software CD  
Installation Guide

### 3 YEAR WARRANTY\*

1 year warranty out of the box.  
Extra 2 years **FREE** with online registration  
at [www.netcomm.com.au](http://www.netcomm.com.au)

\* Conditional upon registration online.



NetComm is the name Australians trust for reliable data communications. Only NetComm develops its products specially for Australian conditions, making NetComm the first choice for quality and reliability. Listed on the Australian Stock Exchange (ASX: NTC), NetComm is Australia's own data communications and networking solutions provider. For more information on this and other NetComm products, please visit [www.netcomm.com.au](http://www.netcomm.com.au)

NetComm Limited, ABN 85 002 490 486 • PO Box 1200, Lane Cove NSW 2066 Australia.

PHONE (02) 9424 2070 • FAX (02) 9424 2010 • EMAIL [sales@netcomm.com.au](mailto:sales@netcomm.com.au)

Trademarks and registered trademarks are the property of NetComm Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the enclosed product. Product Code: NB3