DUAL ADSL MODEM
USER'S MANUAL

WTC ELECTRONICS

To the Internet World
with an Advantage™

FCC NOTICE

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC FULES.
OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITION:
(1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND
(2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDERSIRED OPERATION.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not
occur in a particular installation. If this equipment does cause harmful interference to
radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures :

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit difference from that to which
  the receiver is connected.

- Consult the dealer of an experienced radio/TV technician for help.

NOTE : The manufacturer is not responsible for any radio or TV interference caused by
unauthorized modifications to this equipment. Such modifications could void the user's
authority to operate the equipment.

Table of Contents

1. Introduction

Congratulations on becoming the owner of WTM4151 ADSL Ethernet Router. 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 install and set up your WTM4151 ADSL Bridge/Router, and how to customize its configuration to get the most out of your new product.

Features

1. WTM4151 provides a Downstream up to 8 Mbps, Upstream 1 Mbps
2. Supports standard compliance G.DMT, G.LITE ANNEX-A
3. Perfect ADSL solution basis of Ethernet
4. Supports various service protocols
5. Provides UBR/CBR ATM service
6. Provides Ethernet port for LAN configuration and USB port (Optional). Both ports can be used simultaneously.
7. One ADSL line and IP address can be shared to multi-users.
8. The general user can install and configure WTM4151 easily.
9. Supports software upgrade
10. Data pump, which can program basis of DSP
11. No external Interleave RAM, 16Kbytes of internal memory
12. Supports 8 bits of VPI and 16 bits VCI address range
13. Host-based Soft SAR unspecified Bit Rate (UBR) service supported
14. 802.1D self-learning transparent bridging supported
15. It can transmit maximum 18,000 feet between the distance of CO equipment and subscriber terminal
16. High compatibility with various of DSLAMS

Specifications

1. Standard Compliance
   - ◆ T1.413 Issue 2 and ITU G.dmt (G.992.1) standards Annex A
   - ◆ Splitterless ITU G.lite (G.992.2) specification

2. Protocols
   - ◆ ATM Protocols
     - WAN mode support
       PPP over ATM (RFC 2364) and PPP over Ethernet (RFC 2516)
     - LAN mode support
       Bridged/Routed Ethernet over ATM (RFC 1483)
     - ATM Forum UNI 3.1/4.0 PVC
     - Up to 8 PVCs, ATM SAR, ATM AAL5, OAM F4/F5
   - ◆ Router Mode
     - Static IP routing, RIPv2
     - DHCP Server and Client, NAT, NAPT, ICMP, IGMP, VPN, IP Filtering
       Built-in Firewall

3. Connector
   - ◆ 2 RJ-11 Connector (ADSL Line & Phone)
   - ◆ 1 RJ-45 Connector (Ethernet)
   - ◆ 1 USB Connector

4. PC Interface
   - ◆ Ethernet Interface (IEEE 802.3 10Base-T RJ-45)
   - ◆ USB Interface (USB Option)

5. Transmission Rate
   - ◆ Downstream Max 8 Mbps, Upstream Max 1 Mbps

6. LED Indicators
   - ◆ POWER, LINK, ACT, LAN, DIAG

7. Power
   - ◆ Input Voltage: AC 110~220
   - ◆ Frequency: 50~60Hz

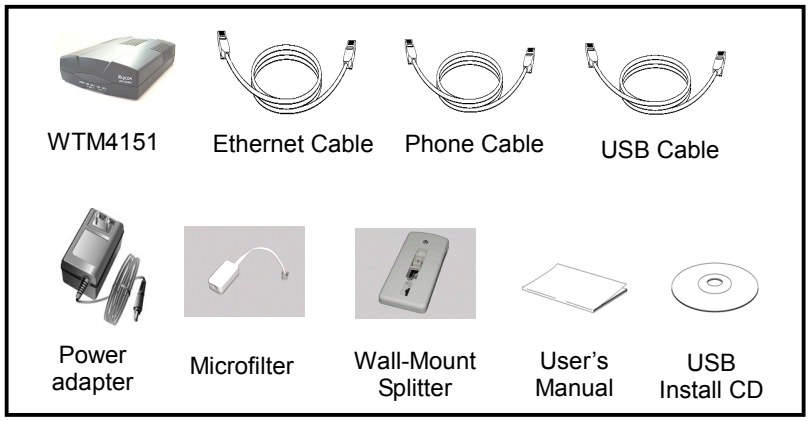
8. Use Environment
   - ◆ Temperature: -20℃~70℃
   - ◆ Operation Temperature: 0℃~40℃
   - ◆ Operation Humidity: 0%~90% (Non-condensing)

9. Dimension
   - ◆ 190(L) × 142(W) × 40(H)

Parts check

In addition to this document, your WTM4151 should arrive with the following:

1. WTM4151 Modem 1 piece
2. Ethernet cable (straight-through category-5) 1 piece (1.5m)
3. USB cable 1 piece (A, B Type 1.5m) (Optional)
4. Phone cable 1 piece (RJ-11 1.8m)
5. Power Adapter 1 piece
6. User Manual 1 piece
7. USB installation CD (Optional)
8. Microfilter 3~5 pieces
9. Wall-Mount Splitter 1 piece



System Requirement

In order to use your WTM4151 ADSL/Ethernet router, you must have the following:

1. ADSL service up and running on your telephone line, with at least one public Internet address for your LAN

2. One or more computers each containing an Ethernet 10Base-T/100Base-T network interface card (NIC) and/or a single computer with a USB port

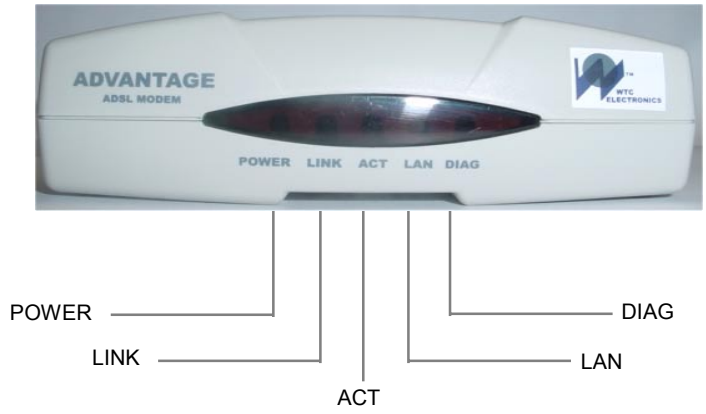
3. An Ethernet hub/switch, if you are connecting the device to more than one computer

4. For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.0 or later, or Netscape v4.7 or later

2. Getting to know WTM4151

Front Panel

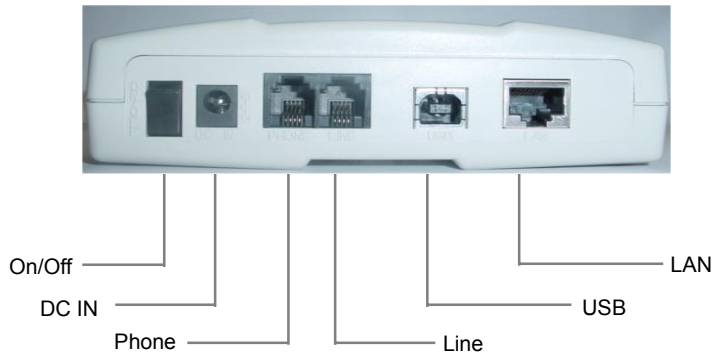
The front panel contains lights called LEDs that indicate the status of the unit.



LED	COLOR	STATUS	DESCRIPTION
POWER	RED	SOLID	On: Modem is powered on Off: Modem is powered off
LINK	GREEN	SOLID	On: ADSL Link established and active Off: No ADSL Link
ACT	GREEN	FLASHING	Flashes when ADSL data activity occurs May appear solid when data traffic is heavy
LAN	GREEN	SOLID	On: LAN Link established and active Off: No LAN Link
DIAG	GREEN	FLASHING	Flashes on/off at boot-up to indicate that the device software is operational. Turns off after a few seconds

Rear Panel

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



Label	Port	Function
On/Off	Power Switch	ON/OFF Switch of Modem Power
USB	USB Port	USB Connector Connects to your PC (Optional)
Phone	Phone Line Port	RJ-11 Phone Connector Connects to your phone
Line	ADSL Line Port	RJ-11 ADSL Line Connector Connects with ADSL Line
LAN	Ethernet Port	RJ-45 Ethernet Connector Connects to your PC Ethernet Port

3. Quick Start

This Quick Start provides basic instructions for connecting the WTM4151 to a computer or LAN and to the Internet.

1. Part 1 describes setting up the hardware.
2. Part 2 describes how to configure Internet properties on your computer(s) and how to install the software for using a computer attached to the USB port
3. Part 3 describes the default settings on the WTM4151, and refers you to the appropriate chapter for instructions on modifying the defaults.

This Quick Start assumes that you have already established 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 for additional configuration instructions.

Part 1- Connecting the Hardware

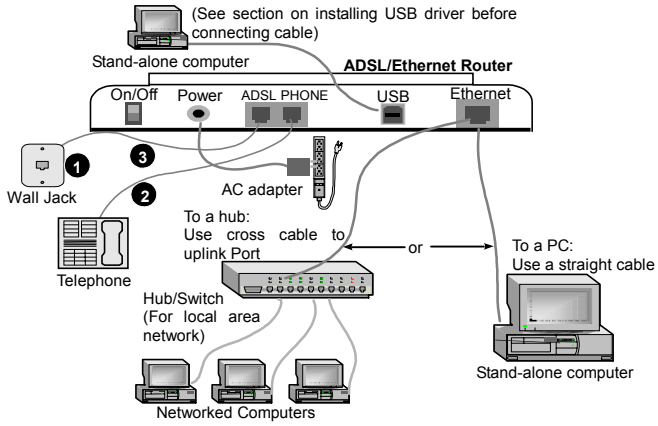
In Part 1, you connect the device to the phone jack, the power outlet, and your computer or network.

WARNING

Before you begin, turn the power off for a devices. *These include your computer(s), your LAN hub/switch (if ap licable), and the WTM4151.*

Figure 1 illustrates the hardware connections. The layout of the ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

Figure 1. Overview of Hardware Connections



Step 1. Connect the ADSL cable and optional telephone.

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.
You can attach a telephone line to the device. This is helpful when the ADSL line uses the only convenient wall phone jack. If desired, connect the telephone cable to the port labeled PHONE.

WARNING

*Although you use the same type of cable, Th ADSL and PHONE ports are **not** interchangeable. Do not route t ADSL connection through the PHONE port.*

Step 2. Connect the Ethernet cable.

If you are using the WTM4151 with a single computer, attach one end of a "straight" Ethernet cable to the port labeled LAN and the other to your computer's Ethernet port.
If you are connecting a LAN to the device, use a crossover cable to connect it to the uplink port on the hub.
See Appendix B "Troubleshooting," for a description of these cable types.

Step 3. Attach the power connector.

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

Step 4. Turn on the WTM4151 and power up your systems.

Press the Power switch on the back panel of the device to the ON position.
Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Step 5: Install USB software and connect the USB cable.

You can attach a single computer to the device using a USB cable. The USB port is useful if you have an USB-enabled PC that does not have a network interface card for attaching to your Ethernet network.
Before attaching the USB cable, you must install a USB driver and configure the computer. For complete instructions, see page 12.

Part 2- Configuring your Computers

Part 2 of the Quick Start provides instructions for configuring the Internet settings on your computers to work with the WTM4151.

Before you begin

By default, the WTM4151 automatically assigns all required Internet settings to your PCs. You need only to configure the PCs to accept the information when it is assigned.

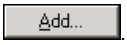

Note

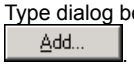
In some cases, you may want to assign Internet inf mation manually to some or all of your computers rather than allow the /TM4151 to do so. See "Assigning static internet information to your PCs" c page 11 for instructions.

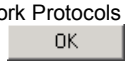
These instructions assume that your PCs are already connected to a LAN through their network interface cards (NICs) and the appropriate Ethernet adapter software.
If you are attaching a PC via the USB port, see the USB configuration instructions on page 12.
Follow the instructions that correspond to the operating system installed on each PC.

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.
   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.
3. If TCP/IP does not display as an installed component, click 

   The Select Network Component Type dialog box displays.
4. Select **Protocol**, and then click 

   The Select Network Protocol dialog box displays.
5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
6. Click 

to return to the Network dialog box, and then click 

again.
   You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
7. Click 

to restart the PC and complete the TCP/IP installation.
   Next, configure the PCs to accept IP information assigned by the WTM4151
8. Open the Control Panel window, and then click the Network icon.

9. 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.
10. In the TCP/IP Properties dialog box, click the IP Address tab.
11. Click the radio button labeled **Obtain an IP address automatically**.
12. Click the DNS Configuration tab, and then 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.
   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 9.
4. If TCP/IP does not display as an installed component, click Add...
5. In the Select Network Protocol dialog box, select **TCP/IP**, and then click OK.
   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.
6. 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 WTM4151:
7. Open the Control Panel window, and then double-click the Network icon.
8. In the Network dialog box, click the Protocols tab.
9. In the Protocols tab, select **TCP/IP**, and then click Properties.
10. In the Microsoft TCP/IP Properties dialog box, click the radio button labeled **Obtain an IP address from a DHCP server**.
11. Click OK twice to confirm and save your changes, and then 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**.
   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 10.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click Install...
5. In the Select Network Component Type dialog box, select **Protocol**, and then click Add...
6. 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.
7. If prompted, click OK to restart your computer with the new settings.
   Next, configure the PCs to accept IP information assigned by the WTM4151:
8. In the Control Panel, double-click the Network and Dial-up Connections icon.
9. In Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select **Properties**.
10. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)**, and then click Properties.
11. 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**.
12. Click OK twice to confirm and save your changes, and then close the Control Panel.

Window ME PCs

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 Network icon, and then select **Properties**.
   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 11.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click Add...
5. In the Select Network Component Type dialog box, select **Protocol**, and then click Add...

6. Select **Microsoft** in the Manufacturers box.
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 Me 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.
   Next, configure the PCs to accept IP information assigned by the WTM4151:
9. In the Control Panel, double-click the Network and Dial-up Connections icon.
10. In Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.
11. In the Network Properties dialog box, select **TCP/IP**, and then click Properties.
12. In the TCP/IP Settings dialog box, click the radio button labeled **Server assigned IP address**. Also click the radio button labeled **Server assigned name server address**.
13. Click OK twice to confirm and save your changes, and then close the Control Panel.

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 WTM4151 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 Appendix A.)

Before you begin, contact your ISP if you do not already have the following information:

- 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 your WTM4151. By default, the LAN port is assigned this IP address: **192.168.1.1**. (You can change this number, or your ISP can assign another number. See Chapter 5 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 instructions on pages 8 through 11 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, clicks the radio buttons that enable you to enter the information manually.

Note

Your PCs must have IP addresses that place the in the same subnet as the WTM4151's LAN port. If you manually assign P information to all your LAN PCs, you can follow the instructions in Chap r 5 to change the LAN port IP address accordingly.

Configuring a computer connected to the USB port (If applicable)

If your WTM4151 includes a USB port for connecting to a PC, you must install the provided USB driver software on the PC. The driver enables Ethernet-over-USB communication with the WTM4151.

Configuring the USB computer is a two-part process:

- In Part 1, you install the USB driver on the PC.
- In Part 2, you configure the IP properties on the USB PC.

Part 3. Installing the USB Driver:

Ensure that the USB cable **is not connected** to the USB port on the PC or to the USB port on the device.
The installation program will prompt you when to connect the cable.

1. Copy the USB installation file to a temporary directory on the USB computer.
2. In the folder where you copied the files, double-click on *setup.exe* to launch the installation program.
   The Welcome dialog box displays, as shown in Figure 2.

Figure 2. USB Driver Installation: Welcome Screen

3. Click Next > to display the Software License Agreement dialog box, as

shown in Figu

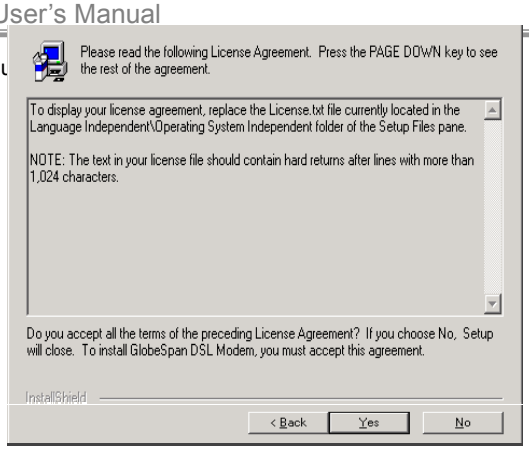
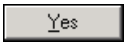
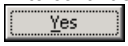


Figure 3. USB Driver Installation: Software License Agreement

4. After reviewing the license agreement, click 

to continue.

5. If a Microsoft digital signature dialog box displays, click 

to continue.
The installation program will begin copying the necessary installation files to the required locations. When finished, the Setup Complete dialog box will display, as shown in Figure 4.

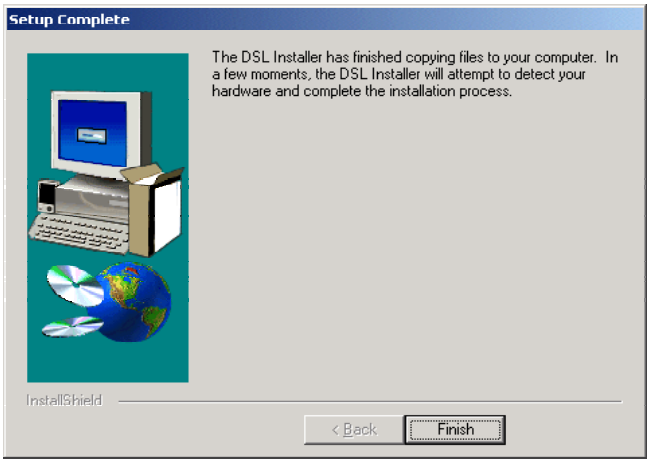


Figure 4. USB Driver Installation: Setup Complete

6. Click 

.
A DSL Installer dialog box displays while the program searches for your USB hardware. After a few seconds, a second dialog box displays to prompt you to attach the USB cable, as shown in Figure 5

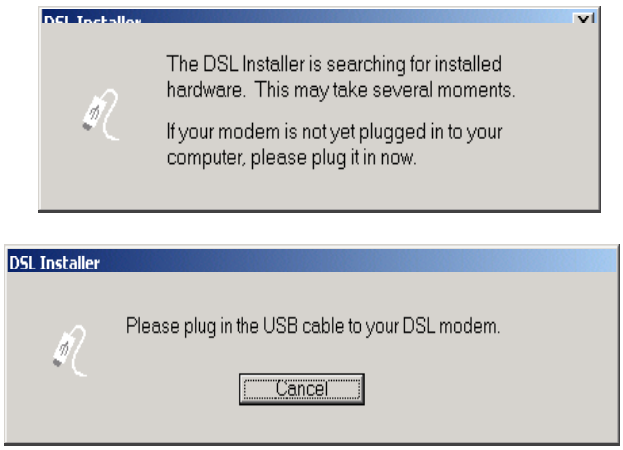


Figure 5. USB Driver Installation: DSL Installer

7. Attach the USB cable to the WTM4151 and to your PC.
   The USB cable provided has a flat connector on one end (called Type A) and a square connector on the other (Type B). Connect the flat connector to your PC and the square connector to the WTM4151.
   A window displays briefly, indicating that the system has found new hardware.
8. If a Microsoft digital signature dialog box displays, click Yes to continue.
   The System Settings Change dialog box displays to prompt you to restart your computer, as shown in Figure 6.

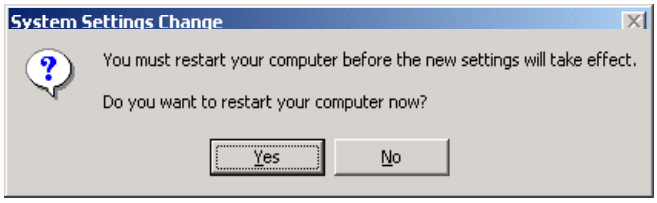


Figure 6. USB Driver Installation: System Settings Change

9. Click Yes to restart your computer.
   When your computer finishes rebooting, make sure that the installer program displays as an item on your Windows Start menu:

10. Click the Start button, point to **Programs DSL Modem**, and click on **Configure**.
    The DSL Modem Installer dialog box should display, as shown in Figure 7

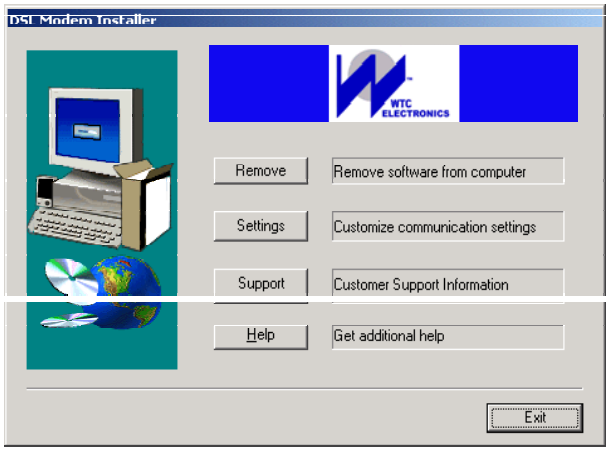


Figure 7. DSL Modem Installer Dialog Box

11. Click 

.

Part 4. Configuring IP properties on the USB PC.

Now that the USB driver installation is complete, you must configure the USB PC so that its IP properties place
it on the same subnet as the WTM4151's USB port.
There are two ways to do this:

- The WTM4151 is configured to assign an appropriate IP address to the USB PC. If you want to use this automatic assignment feature, called "DHCP server," you must configure the USB PC to accept dynamically assigned IP information. Follow the instruction on pages 8 through 11 that correspond to the operating system installed on the PC.
- If you want to assign a static IP address to the PC, follow the instructions on page 11 and use the following information.

  - In the Network and Dial-up Connections window, be sure to select the icon that corresponds to your new USB connection (not the one that corresponds to your Ethernet NIC). When you display the properties for the icon, the following text should display in the Connect Using text box:
    GlobeSpan USB IAD LAN Modem #n

- The USB port on the WTM4151 is pre-configured with these properties (you cannot change these values):

USB port IP address: *192.168.2.1*
USB port subnet mask: *255.255.255.0*

Therefore, your PC must be configured as follows:

IP address: *192.168.2.n*

(Where n is a number from 2 to 254)

Subnet mask: *255.255.255.0*

Default gateway: *192.168.2.1*

Part 5 — Configuring the WTM4151

The WTM4151 is pre-configured with default settings for use with a typical home or small office network setup.
Table lists important default settings (other are described in the subsequent chapters). Verify that they meet the needs of your network, or 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 modifying any settings, review Chapter 4 for general information about using the Configuration Manager program. We strongly recommend that you contact your ISP prior to changing the default configuration.

Table. Default Settings

Option	Default Setting	Explanation/Instructions
ISP Connection Properties	Login user name: guest Login password: guest	The login user name and password are used to authenticate you as a customer of your ISP using the Point-to-Point protocol (PPP). See Chapter 12 for instructions on changing these and other PPP values.
ATM Properties	One ATM interface defined with these properties: Supports aal5 VPI = 0 VCI = 35 MUX type: LLC	The VPI and VCI values determine the path of your connection to your ISP. Contact them to determine if these defaults need to be changed, and see Chapter 13 for additional instructions.
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with two pools of addresses: For LAN computers: 192.168.1.2 through 192.168.1.13 For USB computer:	The WTM4151 maintains a pool of 12 private IP addresses for dynamic assignment to your LAN computers and a pool containing 1 IP address for assignment to your USB computer. To use this service, you must have set up your

Option	Default Setting	Explanation/Instructions
	192.168.2.2 (for both, subnet mask = 255.255.255.0)	computers to accept IP information dynamically, as described in Part 2 of the Quick Start. See Chapter 8 for an explanation of the DHCP service.
NAT (Network Address Translation)	NAPT rule enabled	Your computers' private IP addresses (see DHCP above) will be translated to your public IP address whenever they access the Internet. See Chapter 9 for a description of the NAT service.
LAN Port IP Address	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 Chapter 5 for instructions.
USB Port IP Address	Assigned static IP address: 192.168.2.1 subnet mask: 255.255.255.0	This is the IP address assigned to the USB port on the device. You cannot change this address.

Testing your Installation

The Quick Start process you just completed should enable any computer on your LAN to use the WTM4151's ADSL connection to access the Internet.
To test the connection, turn on the device, wait about 30 seconds, and then verify that its LEDs are illuminated as shown in Table.

Table . LED Indicators

This LED:	...should be:
PWR	Solid red to indicate that the device is turned on. If this light is not on, check the power cable attachment.
DIAG	Flashing on/off while the device is booting. After about 10-15 seconds, it should turn off.
LAN	Solid green to indicate that the device can communicate with your LAN.
LINK	Solid green to indicate that the device has successfully established a connection with your ISP.
ACT	Flashing when the device is sending or receiving data from the Internet. It may be unlit, flashing, or appear solid depending on the current activity.

If the LEDs illuminate as expected, test your Internet connection from a LAN computer (and from the USB computer, if applicable): Open your web browser, and

type the URL of any external website (such as http://www.yahoo.com). The LED labeled WAN ACT should be blinking rapidly and may appear solid as the device connects to the site.
If the LEDs do not illuminate as expected or the web page does not display:

- Ensure that the default settings shown on page 16 are appropriate for your network setup.
- See Appendix B, "Troubleshooting" for tips on correcting a variety of common problems.
- Contact your ISP customer support for assistance

4. Getting started with configuration Manager

Your WTM4151 includes 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 WTM4151 via the LAN port. This chapter describes how to use the Configuration Manager.

Note

Your WTM4151 may already be configured to prov e Internet connectivity for your network. If it works properly with the preco igured settings, then you may not need to use the Configuration Manag . Contact your ISP to determine which settings you may need to change any.

Accessing the Configuration Manager

The Configuration Manager program is preinstalled into memory on your WTM4151. 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 3).
- A web browser installed on the PC. The program is designed to work best with Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions.

You can access the program from any computer connected to the WTM4151 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://192.168.2.1

   These are the predefined IP addresses for the LAN and USB ports on your WTM4151. A login screen displays, as shown in Figure 8.

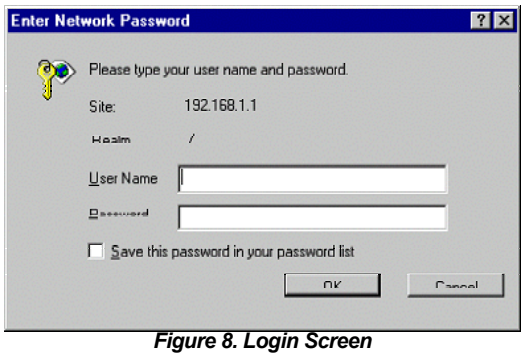


Figure 8. Login Screen

2. Enter your user name and password, and then click OK.
3. The first time you launch the program, use these defaults:

Default User Name:	root
Default Password	root

Note

You can change the password at any time
(see "Changing your log-in password on page 24)
The user name cannot be changed.

The System View page displays each time you launch the program (shown in Figure 9 on page 21).

Navigating Through the Program

You can use these page elements to navigate through the program:

Task Bar

The task bar displays at the top of all main pages to provide a consistent way to access all program functions. One of two sets of options can display:
The basic task bar options display when you first access the program:

|System | Device Info | LAN Config | User Config | Commit & Reboot | IP Address |

Figure 4. Task Bar—Basic Options

When you click the **Advanced** link at the right of the page, menu options for advanced functions display in the task bar:

|IP Route | DHCP | NAT | RIP | Alarm | PPP | ATM VCC | DSL | IP Filter | EOA | Bridging | IPoA |

Figure 5. Task Bar—Advanced Options

You can click **Basic** at the right side of the page to redisplay the basic functions.

Commonly Used Buttons

Button	*Function*
Submit	Stores in *temporary* system memory any changes you have made on the current page. See "Committing your changes" on page 25 for instructions on storing changes permanently.
Refresh	Redisplays the current page with updated statistics.
Clear	When accumulated statistics are displaying, this button resets the statistics to their initial values.
Help	Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.

Viewing Basic System information

The System View page displays when you first access the program:

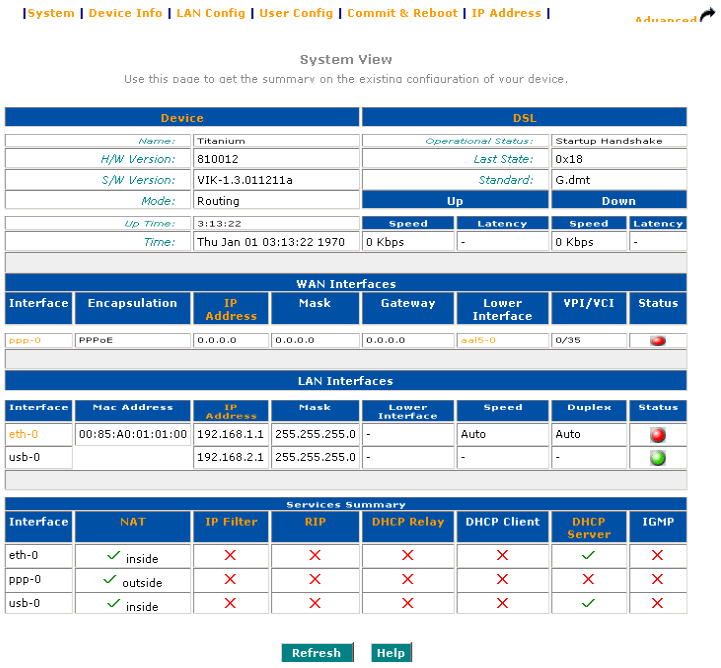


Figure 9 System View Page

The System View table provides a snapshot of your system configuration. You can click on the table headings that are highlighted in orange lettering to display a more details on those settings or the configuration page for that feature. The following table describes the groups of data shown on the System View page and, where appropriate, refers you to the appropriate chapters in this document for more information:

Table Heading	Description
Device	Displays basic information about the WTM4151 hardware and software versions, the system uptime (since the last reboot), and the preconfigured operating mode.
DSL	Displays performance statistics for the DSL line. You can click the **DSL** link in the Advanced title bar to display additional DSL settings, which are described in Chapter 14
WAN Interfaces	Displays the software name(s) and various settings for the interfaces on the device that communicate 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 PPP, ATM VCC, EOA, and IPoA chapters (Chapters 12,13,16 and 18 respectively) for more information about the interfaces defined on you system.
LAN Interfaces	Displays the software names and various settings for the interfaces on the device that communicate directly with your network. These typically include at least one Ethernet interface, named *eth-0*, and may include a USB interface named *usb-0*. You can configure some properties of the Ethernet interface, as described in Chapter 5. The USB interface properties are not configurable.
Services Summary	Displays the following service that the WTM4151 performs to help you manage your network: o Translating private IP addresses to your public IP address (NAT, Chapter 9). o Setting up filtering rules that accept or deny incoming or outgoing data. (IP Filter, Chapter 15). o Enabling router-to-router communication (RIP, Chapter 10). o Dynamic assignment or receipt of IP information (DHCP, Chapter 8). o Message forwarding based on Internet Group assignment (IGMP, not configurable).

You can display the System View page from other locations in the program by clicking **System** in the basic task bar.

You can view additional system information by clicking **Device Info** in the task bar. The following page displays:

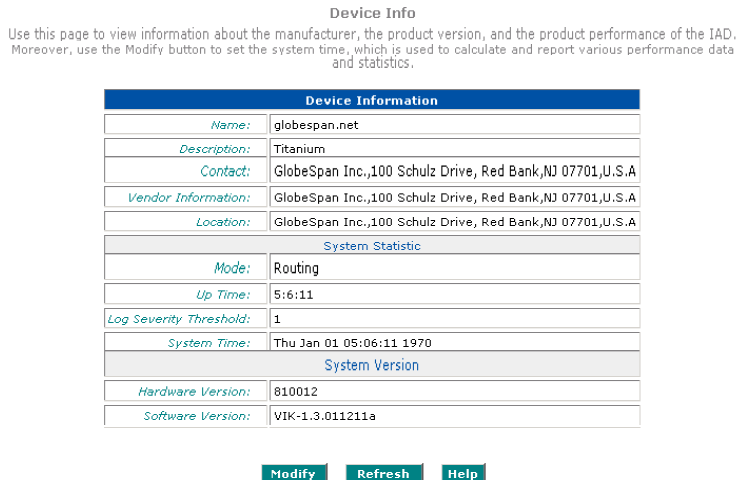


Figure 10. Device Info Page

The Device Information table displays additional contact information for your vendor. You can click Modify at the bottom of the page to change the system date and time, as described in the following section.

Changing the System Date and Time

Note

Changing the WTM4151 date and time does not a ect the date and time on your PCs.

To change the date and time:

1. Click **Device Info** in the task bar, then click Modify on the Device Info page. The System – Modify page displays in a separate browser window:

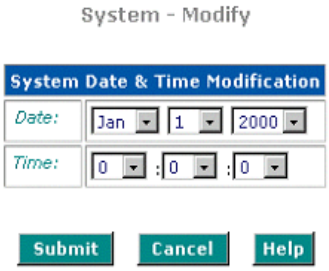


Figure 11. System – Modify Page

2. Use the drop-down lists to select a new date and time.
3. Click Submit.
   A page displays to confirm your change.
4. Click Close to return to the Device Information page.
5. Click **Commit & Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

Changing Your Login Password

The first time you log into the Configuration Manager, you use the default user ID and password (*root* and *root*). The system allows only one user ID and password. Only the password can be changed.

Note

This user ID and password is only used for logging o the Configuration Manager; it is not the same as the login you may us to connect to your ISP (described in Chapter 12).

To change the Configuration Manager login password:

1. Click **User Config** in the top task bar. The User Password Configuration page displays:

Figure 12. User Password Configuration Page

2. Type your current password in the Old Password text box.
3. Type the new password in the New Password text box and again in the Confirm New text box.
   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.
4. Click Submit.
5. Click **Commit & Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

Committing Your Changes and Rebooting the Device

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.
To save your changes for future use, you can use the commit function. This function saves your changes from RAM to permanent storage (called flash memory).

Note

***Submitting** changes saves them only until the de ce is reset or powered down. **Committing** changes saves them permane ly.*

Follow these steps to commit changes to permanent storage.

1. In the task bar, click **Commit & Reboot**.
   The Commit & Reboot page displays:

Figure 13. Commit & Reboot Page

2. Click Commit. (Disregard the selection in the Reboot Mode drop-down list; it does not affect the commit process.)
   The 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 as below)

Rebooting the device using Configuration Manager

If you change the LAN IP address information (see Chapter 5), you must reboot the system after committing the changes in order to activate them. All other changes are activated when you commit them (no reboot is needed).
If, after rebooting the device, you find that it does not operate properly with the new configuration, you can reboot using options that reactivate a previous configuration or the manufacturer's default configuration.

To reboot the device, display the Commit and 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:

etting	Description
Reboot from Last Configuration	Reboots the device using the current settings in permanent memory, including any changes you just committed.
Reboot from Backup Configuration	Reboots 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	Reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.

5. Setting the LAN IP Address

This chapter describes how to change the WTM4151's LAN IP address, or configure it to be assigned automatically by another device.

What is the LAN IP Address?

Your WTM4151 communicates with your network through its LAN port. To allow for Internet communication, the LAN port must be identified by a unique IP address, like your other computers. The IP address associated with this port is called the LAN IP address.

Note

The public IP address assigned to you by your ISP i ***not*** *your LAN IP address. The public IP address identifies the WAN (DSL) port on your WTM4151 to the Internet.*

Your device is preconfigured with a default LAN IP address of 192.168.1.1. You can change the default to reflect the set of IP addresses that you want to use with your network.
You can also configure the device to use a LAN IP address that is assigned dynamically from a DHCP server on your network. When IP information is assigned by another device, the WTM4151 is said to be acting as a *DHCP client* of that device.

Note

The WTM4151 itself can function as a DHCP serve r your LAN computers, as described in Chapter 8, ***but not for its own LAN ort****.*

Changing the LAN IP Address

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

1. Launch Configuration Manager, and then click **LAN Config** in the task bar.
   The LAN Configuration page displays, as shown in Figure 14.

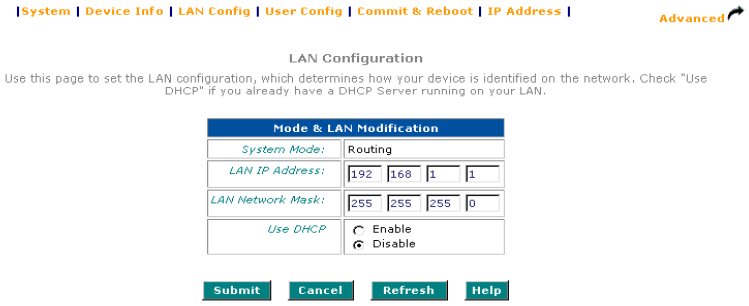


Figure 14. LAN Configuration Page

The fields on this page are defined as follows:

System Mode	The preconfigured mode in which your device operates.
LAN IP Address	The IP address your computers use to identify the device's LAN port.
LAN Network Mask	The LAN Network mask identifies which parts of the LAN IP Address refer to your network as a whole and which parts refer specifically to nodes on the network (a node can be thought of as any port on the network, such as the WTM4151's LAN port and the network interface cards on your PCs). See Appendix A for an explanation of IP addresses and masks.
Use DHCP	When checked, this setting instructs the device to accept LAN IP information assigned dynamically from another DHCP server already configured on your network. The WTM4151 cannot act as a DHCP server for its own LAN port.

2. Enter a LAN IP address and network mask, or click the **Use DHCP** check box.

   - If you are using routing services on you 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. Note that the IP address you assign must be on 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 Appendix A for an explanation of IP addresses and network masks.
   - If another computer on your LAN provides DHCP services for your network, you can click the **Use DHCP** checkbox. Check with your ISP to determine if this is advisable. The LAN IP Address and LAN Network Mask fields are dimmed to indicate that the information will not be used (the data is retained for future use, however).
     For a description of how DHCP works, see Chapter 8.

3. Click 

to confirm the changes.
   The connection between your computer and the WTM4151 will be terminated, because the IP address on which the communication was based has now changed.
4. In your Web browser, type the new LAN IP address and log in to the software when prompted.
5. Click **Commit & Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

6. Viewing System Information and Performance Statistics

The interfaces on your WTM4151 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 Appendix A for a description of IP addresses and masks.

Viewing your WTM4151's IP addresses

Click **IP Address** in the task bar. The IP Address Table page displays, as shown in Figure 15.

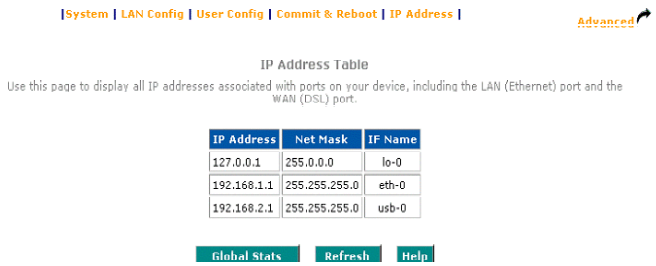


Figure 15. IP Address Table Page

The table lists the IP addresses, network masks ("Net Mask"), 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 Chapter 5 for instructions on configuring this address.
- The IP address of the device's USB port, named *usb-0*, which is assigned automatically at start-up. You cannot configure 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* or *eoa-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 is a special address that 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 Global 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.

Figure 16 shows the IP Global Statistics page:

IP Global Statistics

IP Datagrams Statistic	Values
IP Received:	433 Packets
IP Received w/ Header Error:	0 Packets
IP Received w/ Wrong Address:	135 Packets
IP Received w/ Unknown Protocol:	0 Packets
IP Routing Discarded:	0 Packets
IP Datagrams Forwarded	
Forwarded Datagrams:	135 Packets
Input IP Datagrams	
Input IP Discarded:	0 Packets
Input IP Delivered To User-Protocol:	298 Packets
Output IP Datagrms	
IP Requests For Transmission w/ User-Protocol:	774 Packets
Output IP Discarded:	0 Packets
Output IP Discarded w/ No Route:	0 Packets
IP Datagrms / Reassemble	
Maximum # of Seconds IP Waits For Reassemble:	60 Second(s)
IP Received Which Needed To Be Reassembled:	0 Packets
IP Successfully Re-assembled:	0 Packets
IP Fails To Re-Assemble:	0 Packets
IP Datagrmas / Fragment	
IP Successfully Fragmented:	0 Packets
IP Fails To Fragment:	0 Packets
IP Fragments Created:	0 Packets

Figure 16. IP Global Statistics Page

To clear out all past data and reset the statistics to their initial state, click Clear. To display updated statistics showing any new data since you opened the page, click Refresh.

7. 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 device uses to make these decisions.

Comparing IP routing to 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 Appendix A)
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 WTM4151 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 your WTM4151. 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 WTM4151 itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. Your ISP assigns this default gateway automatically whenever the device negotiates an Internet connection. (The process for adding a default route is described on page 34.)

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 WTM4151's routing table, click the **Advanced** link at the right side of the page, and then click **IP Route** in the task bar. The following page displays:

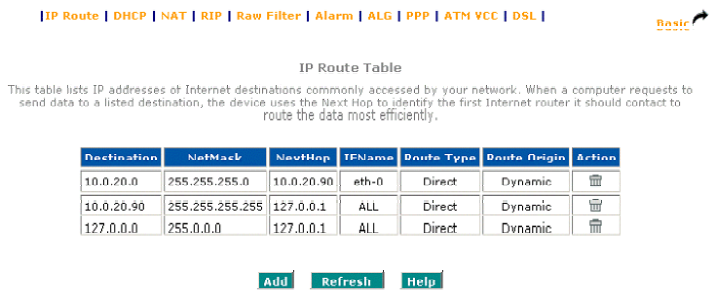


Figure 17 IP Route Table Page

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 routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.

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

Table. IP Routing Table Fields

Field	Description
Destination	Specifies the IP address of the destination computer. The destination can specify 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 Appendix A for an explanation of network masks. The default gateway uses a netmask of 0.0.0.0.
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.

Field	Description
Route Type	Displays whether the route is direct or indirect. 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. 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.
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 Chapter 10), 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 18.

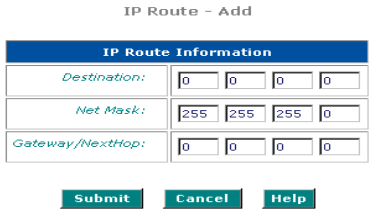


Figure 18. IP Route – Add Page

2. Specify the destination, network mask, and gateway or next hop for this route.
   For a description of these fields, refer to Table on page 33.
   To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the Destination and Net Mask 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 create, the routing table displays system default values in these fields.
3. Click Submit.
   The IP Routing Table will now display the new route.
4. Click **Commit & Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

8. Configuring Dynamic Host Configuration Protocol

You can configure your network and WTM4151 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 your MTR 1000GL or a router located with your ISP — to assign temporary IP addresses to your computers whenever they want to use to the Internet. The assigning device is called a *DHCP server*, and the receiving device is a *DHCP client*.

If you used the Quick Start instructions in Chapte , you either configured each LAN PC with an IP address, or you specifie hat it will receive IP information dynamically (automatically). If you cho e to have the information assigned dynamically, then you confi red your PCs as DHCP clients that will accept IP addresses assigned fro a DCHP server such as the WTM4151.

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 initiates a new Internet connection.

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.

WTM4151 DHCP modes

The device can be configured as a DHCP server, DHCP relay agent, or, in some cases, a DHCP 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. Both DHCP server and NAT are enabled in the default configuration.

- If your ISP performs the DCHP server function for your network, then you can configure the device as a DHCP relay agent. When the WTM4151 receives a request for Internet access from a computer on your network, it contacts your ISP for the necessary IP information, and then relays the assigned information back to the computer.
- If you have another PC or device on your network that is already performing the DHCP server function, then you can configure the LAN port on the WTM4151 to be a DHCP client of that server (as are your PCs). This configuration is not discussed in this chapter. See Chapter 5 for instructions.


Note

You can input settings for both DHCP server and HCP relay mode, and then activate either mode at any time. De-activate settings are retained for your future use.

Configuring DHCP Server

Before you begin, determine the pool of IP addresses you want to make available for distribution to your computers. These addresses can be multiple public addresses that you have purchased from your ISP, but are typically private addresses that you create. (LAN administrators often create private IP addresses for use only on their networks. See "**Overview of NAT**" on page 41)


Note

*By default, the device is configured as a DHCP sen r, with a predefined IP address pool of 192.168.1.2 through 192.168.1.13 (ıbnet mask 255.255.255.0). To change this range of addresses :ee "**Viewing, modifying, and deleting address pools**" on page).*

The procedure for configuring the WTM4151 as a DHCP server has three parts, described in detail in the sections that follow:

- In Part 1, you create an IP address pool.
- In Part 2, you enable the device as a DHCP server.
- In Part 3, you configure your PCs to accept the assigned IP addresses

Part 1. Creating IP address pools

1. Launch the Configuration Manager, click **Advanced** in the task bar, and then click **DHCP**. The DHCP Configuration page displays:

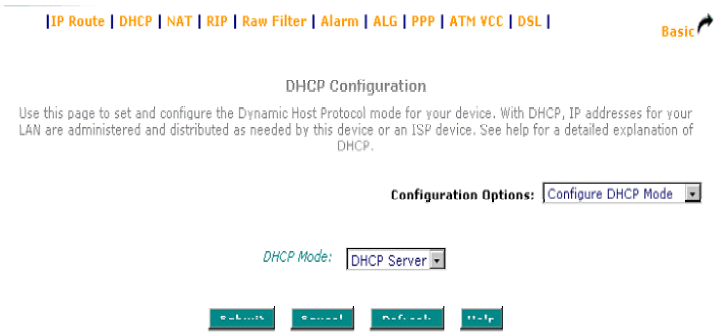


Figure 19. DHCP Configuration Page

2. Select **Configure DHCP Server** from the Configuration Options drop-down list. The DHCP Server Configuration Page displays:

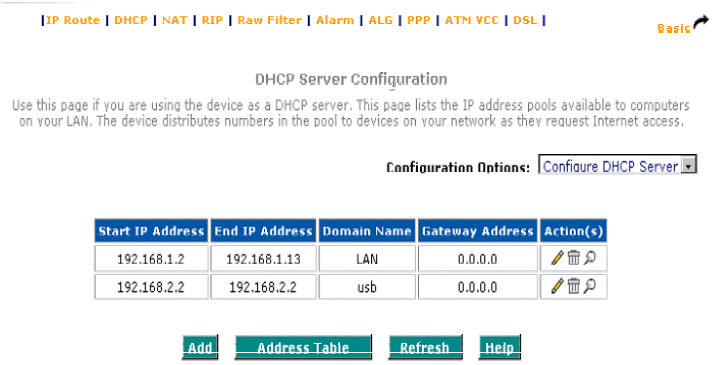


Figure 20. DHCP Server Configuration Page

Each pool you create displays in a row on the table on this page. You can create up to eight pools. In this example, one pool has been created for the LAN interface and another for the USB interface. Additional pools may be needed when the device is configured with multiple LAN interfaces.

3. To add an IP address pool, click **Add**.
The DHCP Server Pool – Add page displays.

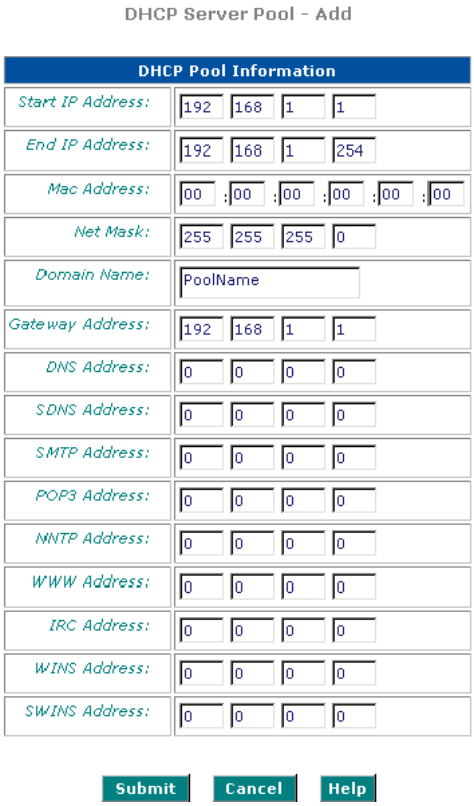


Figure 21. DHCP Server Pool – Add Page

4. The *Start IP Address*, *End IP Address*, *Net Mask*, and *Gateway Address* fields are required; the others are optional.

Field	Description
Start/End IP Addresses	Specify the lowest and highest addresses in the pool.
Mac Address	Use this field only if you want to assign a specific IP address to a specific computer (that is, you are creating an exception to the dynamic assignment of addresses). The IP address you specify will be assigned to the computer that corresponds to this MAC address. (A MAC address is

Field	Description
	a manufacturer-assigned hardware ID that is unique for each device on a network.) 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.
Net Mask	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 Appendix A. You can use the network mask to distinguish which pool of addresses should be distributed to a particular subset of computers on your LAN (called a *subnet*).
Domain Name	A user-friendly name that refers to the group of computers (subnet) that will be assigned addresses from this pool.
Gateway Address	The address of the default gateway for computers that receive IP addresses from this pool. The default gateway is the IP address that the computers first contact to communicate with the Internet. Typically, it is the device's LAN port IP address. See "Hops and gateways" on page 31 for an explanation of gateway addresses.
DNS	The IP address of the *Domain Name Server* to be used by computers that receive IP addresses from this pool. The DNS translates common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, this server is located with your ISP.
SDSN...SWINS (optional)	The IP addresses of devices that perform various services for computers that receive IP addresses from this pool. Typically, these devices are servers located with your ISP. See the glossary for a definition of each type of server.

5. Click Submit.
   A confirmation page displays to indicate that the pool has been added successfully.
6. Click Close to return to the DHCP Configuration page.

Part 2. Enabling DHCP Server Mode

After you have defined a DHCP pool, you set the device to operate in DHCP server mode. (It may already be set, by default.)

1. From the DHCP Mode drop-down list, select **DHCP Server**, and then click Submit.
   A page displays to confirm the change.
2. Click **Commit and Reboot** in the basic task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

Part 3. Configuring your PCs as DHCP clients

For each computer that you want to configure to receive IP information automatically, 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). The procedure for enabling DHCP on each PC is described in detail in the Quick Start, Part 2.

Viewing, modifying, and deleting address pools

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

To perform this action	...click this icon:
Delete an IP address pool	
Modify an IP address pool	
View details for an IP address pool	

You can modify an address pool to change the domain name associated with the pool or to exclude IP addresses within its range from distribution. You may want to exclude an address if you have already designated it for fixed use with a specific device, or for any other reason do not want to make it available to your network. To change any other properties of the pool, such as the starting and ending IP addresses, you must delete the pool and create a new one.
The DHCP Server Pool – Modify page is shown in Figure 22

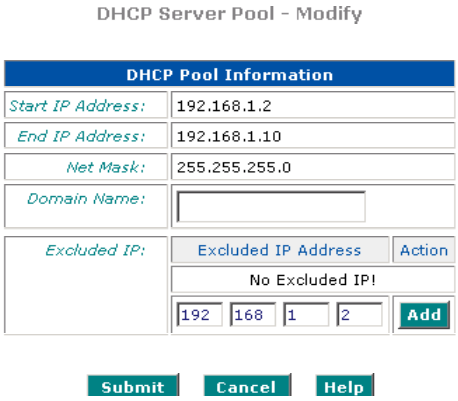


Figure 22. DHCP Server Pool – Modify Page

To exclude an address from distribution, type it in the fields provided and click Add. Click Submit after entering your changes. Be sure to use the Commit feature to save your changes to permanent memory, as described on page 25.

Viewing current DHCP address assignments

When your WTM4151 functions as a DHCP server for your LAN, it keeps a record of any addresses it has leased to your computers. To view a table of all current IP address assignments, display the DHCP Server Configuration page, and then click Address Table.

A page displays similar to the on shown in Figure 23.

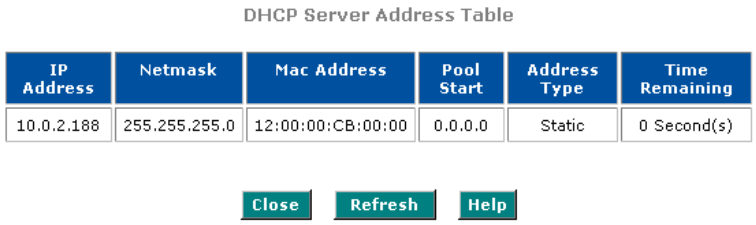


Figure 23. DHCP Address Table Page

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, which identifies the network ID and host ID portions of the address (see Appendix A).
Mac Address	A hardware ID for the device to which the number has been assigned.
Pool Start	The lower boundary of the address pool (provided to identify the pool from which the leased number came).
Address Type	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.

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, your WTM4151 contacts your ISP to obtain an IP address (and other information), and then forwards that information to the computer.

Before you begin, be sure to have the IP address and network mask of your ISP's DHCP server.

The process for configuring the device as a DHCP relay agent has three parts, which are described in the sections that follow:

- Part 1: Defining the DHCP relay interface
- Part 2: Enabling DHCP relay mode
- Part 3: Configuring your PCs to accept the assigned IP addresses

Part 1. Defining the DHCP relay interface(s)

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

1. Launch the Configuration Manager, click **Advanced** in the task bar, and then click **DHCP**.
2. From the Configuration Options drop-down list, select **Configure DHCP Relay**.
   The DHCP Relay Configuration page displays:

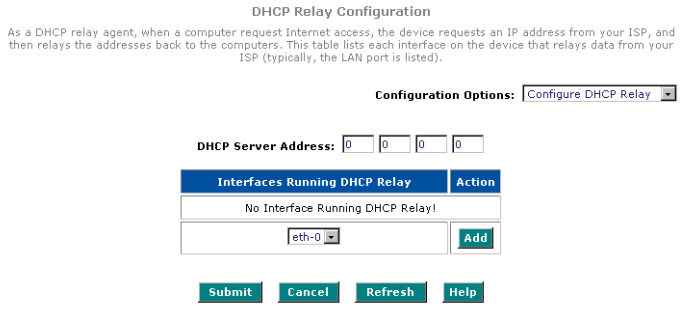


Figure 24. DHCP Relay Configuration Page

This page provides a text box for entering the IP address of your ISPs DHCP server and a table that lists the interfaces on your WTM4151 that can relay DHCP information.

3. Type the IP address of your ISP's DHCP server in the fields provided.
   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. If the interface named eth-0 is not already displaying, select it from the drop-down list and click Add.
   The eth-0 interface specifies that your default Ethernet (LAN) interface is running DHCP relay for your LAN. Typically, this is the only interface you need to specify here. If your WTM4151 has additional interfaces that you want to perform DHCP relay, you can select and add them.
   You can delete an interface from the table by clicking  in the right column.

5. Click Submit.
   A page displays to confirm your changes.

Part 2. Enabling DHCP relay mode

1. From the DHCP Mode drop-down list, select **DHCP Relay**, and then click Submit.
   A page displays to confirm the change.
2. Click **Commit and Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

Part 3. Configuring your PCs as DHCP clients

For each computer that you want to configure to receive IP information automatically, 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). The procedure for enabling DHCP on each PC is described in detail in the Quick Start, Part 2.

9. 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.

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 Chapter 8) On the WTM4151, 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 bunc ed together in a specific format for efficient transmission over the Inte et. Such packets are the building blocks of all Internet communica n. Each packet contains header information that identifies th IP address of the computer that initiates the communication (th **source IP address**), the port number that the router associates w that computer (the **source port number**), the IP address of the rgeted Internet computer (the **destination IP address**), and ther information.*

When this type of rule is applied, because the source IP address is swapped out, it appears to other Internet computers as if the data packets are coming from the computer assigned your public IP address (in this case, the WTM4151).
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 WTM4151 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. These addresses are not useful on the Internet, however.
- They provide a measure of security for you LAN by enabling you to assign private IP addresses. The WTM4151 prevents external access your privately addressed computers (except when using an RDR rule discussed on page 53). In addition, the private addresses are replaced in all outbound data

packets; so external computers never see the private addresses anyway.

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.

Your Default NAT Setup

By default, NAT is enabled, with an NAPT rule configured to perform the following translation:

These p vate IP addresses:	...a › translated to:
192.168.1.2 192.168.1.3 . . . 192.168.1.13	Your ISP-assigned public IP address

For a description of NAPT rules, see page 52. This default NAT setup assumes that, on each LAN computer, you configured TCP/IP properties as follows:

- You selected the check box that enables them to receive their IP addresses automatically (that is, to use a DHCP server);
  or,
- You assigned static IP addresses to your PCs in the range 192.168.1.2 through 192.168.1.13.

If your computers are not configured in one of these ways, you can either change the IP addresses on your computers to match the NAT setup (see the Quick Start instructions in Chapter 3, Part 2), or delete this NAT rule and add a new one that matches the addresses you assigned to your computers (see Adding NAT rules on page 52 for instructions).

Viewing Your NAT Configuration

To view your NAT settings, launch the Configuration Manager, click **Advanced**, and then click **NAT**. The NAT Configuration page displays, as shown in Figure 25

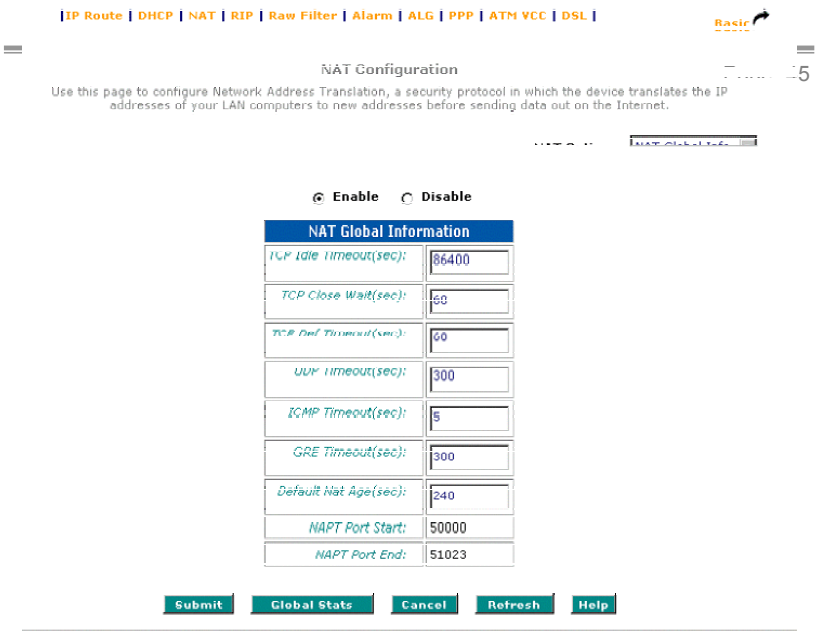


Figure 25 NAT Configuration Page

The NAT Configuration page contains the following elements:

- The NAT Options drop-down list, which provides access to the Global Information page (shown by default), the NAT Rule Configuration page, and the NAT Translations page, which shows current translations.
- Enable/Disable radio buttons, which allow you to turn on or off the NAT feature.
- The NAT Global Information table, which displays settings that apply to all NAT rule translations.
- Buttons you use to submit or cancel changes, display global statistics, and access help.

The NAT Global Information table contains the following fields:

Field	Description
TCP Idle Timeout (sec)	For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
TCP Close Wait (sec)	For a NAT translation on data using the TCP protocol, after a communication session has been closed, the translation will no longer be performed if no matching data packets are

Field	Description
	received after the specified time has elapsed.
TCP Def Timeout (sec)	For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
UDP Timeout (sec)	Same as TCP Idle Timeout, but for UDP packets.
ICMP Timeout (sec)	Same as TCP Idle Timeout, but for ICMP packets.
GRE Timeout (sec)	Same as TCP Idle Timeout, but for GRE packets.
Default NAT Age (sec)	For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid.
NAPT Port Start/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 use the Commit feature to commit your changes to permanent system memory (see page 25).

You can click Global Stats to view accumulated data on how many NAT rules have been invoked and how much data has been translated. A page similar to the one shown in Figure 26 displays.

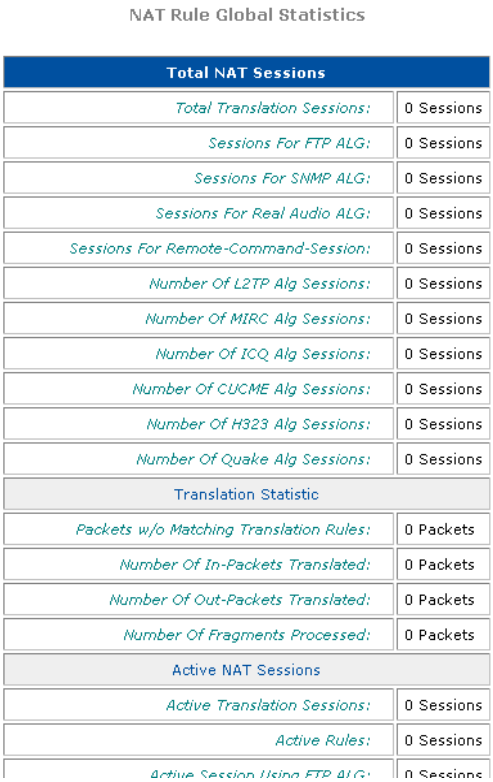


Figure 26. NAT Rule Global Statistics Page

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 NAT Rule Configuration page displays, as shown in Figure 27.

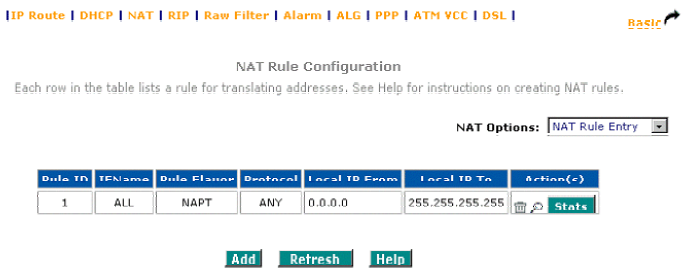


Figure 27 NAT Rule Configuration Page

The 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 a rule of the specified flavor (pages 52 through 60).

From the 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(s) column. A page similar to the one show in Figure 28 displays:

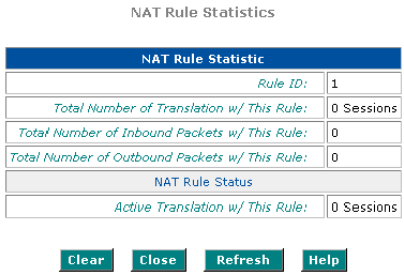


Figure 28 NAT Rule Statistics Page

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. The NAT Translations page displays, as shown in Figure 29

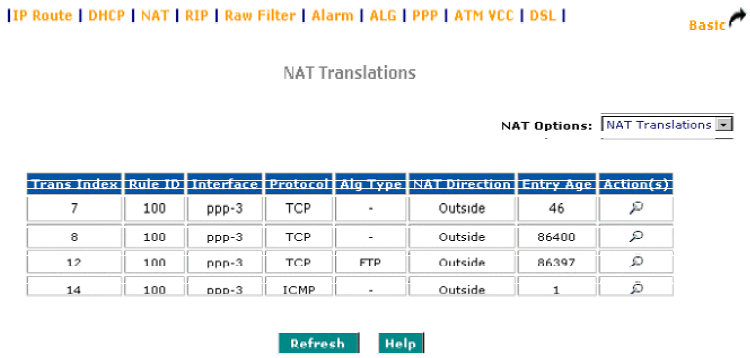


Figure 29 NAT Translations Page

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 (incoming or outgoing) of the translation (from the port definition).
Entry Age	The elapsed time, in seconds, of the NAT translation session.

You can click in the Action(s) column to view additional details about a NAT translation session, as shown in Figure 30.

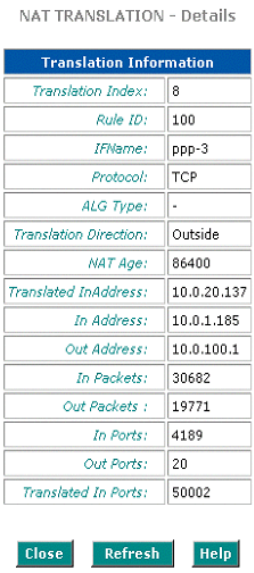


Figure 30. NAT Translation – Details Page

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

Field	Description
Translated In Address	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/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 the various NAT flavors.

Note

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

The NAPT 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 address. This type of rule uses the NAT flavor NAPT, which was used in your default configuration. The NAPT flavor translates private source IP addresses to a single public IP address. The NAPT rule also translates the source port numbers to port numbers that are defined on the NAT Global Configuration page (see page 46). The Introduction to NAT on page 44 describes how the NAPT rule works.

Note

By default, the device is configured with an NAPT e that translates all LAN-side IP addresses to the public address assig ed to the WAN port.

1. From the NAT Configuration page, click Add.
   The NAT Rule – Add page displays, as shown in Figure 31

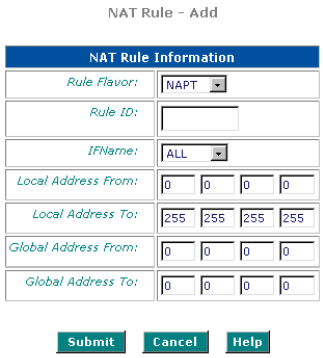


Figure 31 NAT Rule – Add Page (NAPT Flavor)

2. Click the Rule ID drop-down list to assign a number to the rule.
   The Rule ID determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Be sure to assign the Rule ID so that the higher priority rules are invoked before lower-priority 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.

3. In the Rule Flavor drop-down list, select **NAPT**, if necessary.
4. From the IFName drop-down list, select the interface on the WTM4151 to which this rule applies.
   Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (which may be named *ppp-0* or *eoa-0* in the Configuration Manager) to connect your LAN to your ISP, it is the usual IFName selection.
5. Select a protocol to which this rule applies, or choose **ALL**.
   This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data.
   By associating a protocol with this type of NAT rule, you ensure that all data using that protocol is sent to the Internet referencing the public Internet address as the source computer. However, data packets that use protocols not specified here will not undergo translation; their packet headers will reflect the true source address of the LAN computer (and, because they contain private IP addresses, these packets will not be routable on the Internet).
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 want to be translated. Or, type the same address in both fields to specify a single value.
   To specify that data from all LAN addresses should be translated, type 0 (zero) in each "From Field" and 255 in each "To Field."
   If you use non-sequential private addresses, you can create an additional NAPT rule for each separate range of addresses.
   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 Chapter 8).
7. When you have completed entering all information, click Submit.
   A page displays to confirm the change.
8. Click Close to return to the NAT Configuration page.
   The new rule should display in the NAT Rule table.
9. On the NAT Configuration page, ensure that the Enable radio button is turned on.
10. On the NAT Configuration page, click Submit.
    A page displays to confirm your changes.
11. Click **Commit and Reboot** in the task bar, and then follow the instructions on page 25 to commit 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 bimap rule described on ɜge 58), the WTM4151 blocks attempts by external computers to access ɔur LAN computers.

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

Your WTM4151 receives a packet from the Internet containing a request for access to your Web server. The packet header contains your public IP address (which is assigned to the WTM4151's WAN port) as the destination IP address, and *80* as the destination port number. Port #80 is commonly used for web servers. Because you have set up an RDR rule for incoming packets with destination port 80, the WTM4151 recognizes the data as a request for Web server access. The WTM4151 changes the destination IP address in the packet to the private IP address assigned to your Web server and forwards the data packet to it.
Your Web server sends data packets in response. Before the WTM4151 forwards these packets 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.

Figure 32 shows the fields used to establish an RDR rule.

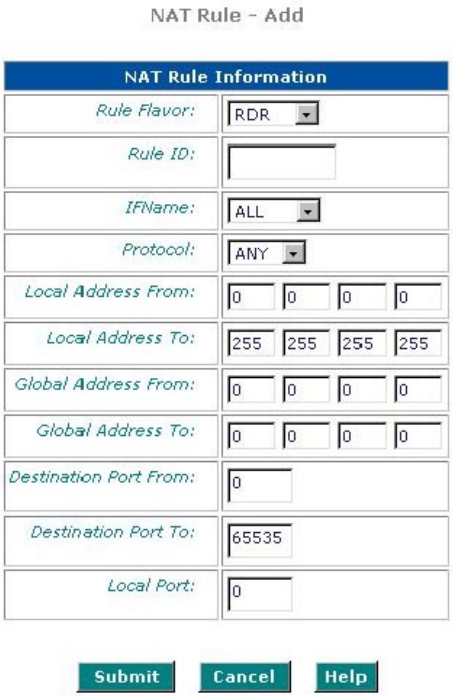


Figure 32. NAT Rule – Add Page (RDR Flavor)

Follow these instructions to add an RDR rule:

1. Display the NAT Rule – Add Page, choose a Rule ID, and select **RDR** as the Rule Flavor.
   See Step 2 on page 52 for instructions on assigning rule IDs.
2. Select the interface and, if desired, a protocol that this rule applies to, as explained in Step 4,5 on page.53.
3. 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 4 and 5 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 Chapter 8).

4. 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 interfaces, in both fields type the IP address of the interface to which this rule applies. 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 a range of them, type the starting and ending IP addresses of the range.
5. Enter a destination addresses (or a range) and port ID (or a range) as criteria for incoming traffic.
   Depending on which other fields you define in this step, incoming traffic that meets this criteria will be redirected to the address (es) specified in step 3 (assuming it comes through the interface specified in step 2).

- Enter a starting and ending IP address in the Destination Address From and Destination Address To fields if incoming traffic destined for these addresses should be redirected.
  You can also enter a single address in both fields.
- When your WTM4151 receives a data packet intended for a destination address (es), it replaces the destination IP address (es) with the private IP address (es) you specified in step 3. The edited packet can then be forwarded to the new destination address—the LAN computer(s).
- Enter a starting and ending port number in the Destination Port From and Destination Port To fields if incoming traffic destined for these port types should be redirected to the address (es) specified in step 3. Or, enter the same address in both fields.
  For example, if you grant public access to a Web server on your LAN, you would expect that incoming packets destined for that computer would contain the port number 80. This setting serves as a filter; data packets not containing this port number would not be forwarded internally.

6. 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 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 can then be routed appropriately to the web server.

The basic rule: Performing 1:1 translations

The basic flavor translates the private (LAN-side) IP address to a public (WAN-side) address, like NAPT rules. However, unlike NAPT 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 NAPT rule.
Figure 33 shows the fields used for adding a basic rule.

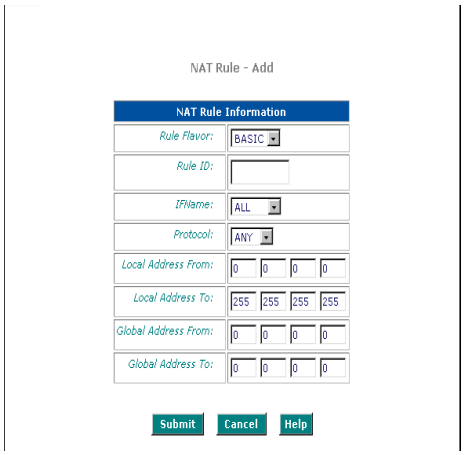


Figure 33 NAT Rule – Add Page (basic Flavor)

To add a basic rule, follow these instructions:

1. Display the NAT Rule – Add Page, choose a Rule ID, and select **BASIC** as the Rule Flavor.
2. Select the interface and, if desired, a protocol that this rule applies to, as explained on page 53.
3. 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 4). The address (or range of addresses) should correspond to a private address (or addresses) already in use on your network These may be assigned statically to

your PCs, or assigned dynamically using DHCP, as discussed in Chapter 8.

4. In the Global Address From and Global Address To fields, type the starting and ending address that identify the pool of public IP addresses to which to translate your private addresses. Or, type the same address in both fields (if you also specified a single address in step 3).

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" on page 56 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 the IP addresses, server type (such as FTP or Web server), or both. Figure 34 shows the fields used to establish a filter rule.

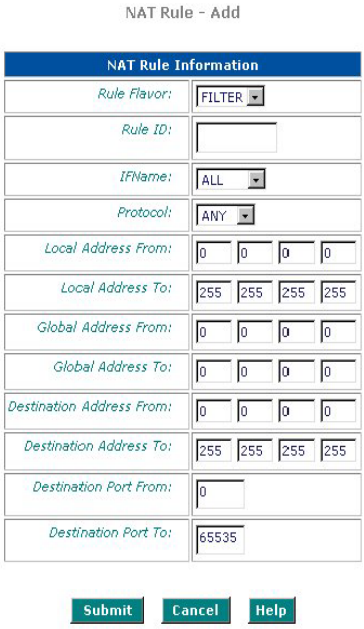


Figure 34 NAT Rule - Add Page (filter Flavor)

Follow these instructions to add a filter rule:

1. Display the NAT Rule – Add Page, choose a Rule ID, and select FILTER as the Rule Flavor.
2. Select the interface and, if desired, a protocol that this rule applies to, as explained on page 53.

3. 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 4). The address (or range of addresses) should correspond to a private address (es) already in use on your network. These may be assigned statically to your PCs or assigned dynamically using DHCP, as discussed in Chapter 8.
4. 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 3).
5. Specify a Destination Address or addresses, Destination Port (or ports), or both. You can specify a single value by entering that value in both 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.
- Specify a destination ports (or range) if you want this rule to apply to any outbound traffic to the types of servers identified by that port number.
  For example, if you do not specify a destination address, but specify a Destination Port From/To of 21, then this translation will occur on all accesses by your LAN to all external FTP servers (that is, when one of your LAN computers communicates with an external FTP server, the source IP address in the packet headers is changed to the public address, not the initiator's private IP address).
  Common port numbers include:
  20, 21—FTP (file transfer protocol) server
  25—SMTP (simple mail transfer protocol) server
  80—HTTP (World Wide Web) server
- Specify both a destination address (or range) and a destination port (or range) if you want this translation rule to apply to accesses to the specified server type at the specified location.

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 WTM4151 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.

Figure 35 shows the fields used to establish a bimap rule.

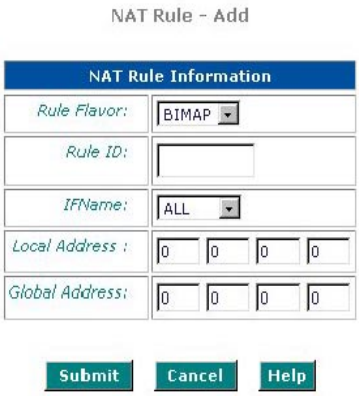


Figure 35. NAT Rule – Add Page (bimap Flavor)

To add a bimap rule, follow these instructions:

1. Display the NAT Rule – Add Page, choose a Rule ID, and select BIMAP as the Rule Flavor.
2. Select the interface and, if desired, a protocol that this rule applies to, as explained on page 53
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.

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

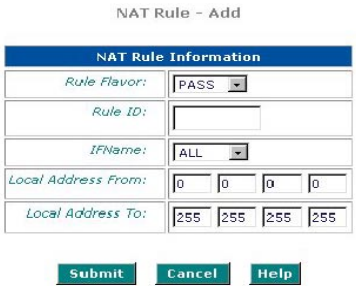


Figure 36 NAT Rule – Add Page (pass Flavor)

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. In 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.
To add a pass rule, follow these instructions:

1. Display the NAT Rule – Add Page, choose a Rule ID, and select Pass as the Rule Flavor.
2. Select the interface and, if desired, a protocol that this rule applies to, as explained on page 53.
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.

10. Configuring the Routing Information Protocol

Your WTM4151 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 your WTM4151 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 WTM4151, 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 WTM4151). The WTM4151 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 WTM4151's Interfaces with RIP

The following instructions describe how to enable RIP on your WTM4151.

Note

In order for the WTM4151 to communicate with oth devices using RIP, you must also enable the other devices to use the proto ol. See the product documentation for those devices.

1. Launch the Configuration Manager, click **Advanced** in the task bar, and then click **RIP**.
   The RIP Configuration page displays, as shown in Figure 37

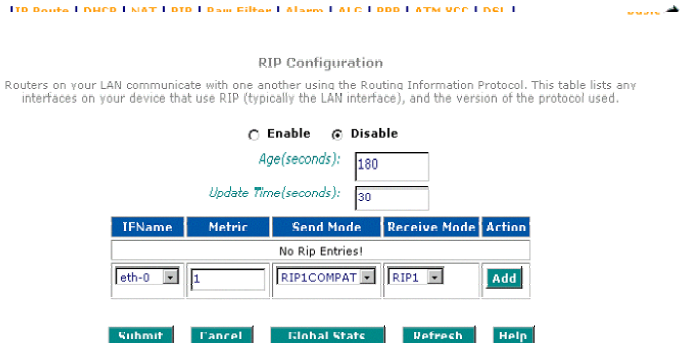


Figure 37 RIP Configuration Page

   The page contains radio buttons for enabling or disabling 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 and Update Time.
   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 WTM4151 will send out its routing table its neighbors.

3. In the **IFName** 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.
   (See page 29 for a description of various interfaces and their names.)
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 and Receive Modes.
   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 WTM4151 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 ou 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 **Commit and Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.


Note

You can delete an existing RIP entry by clicking n 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 your WTM4151.

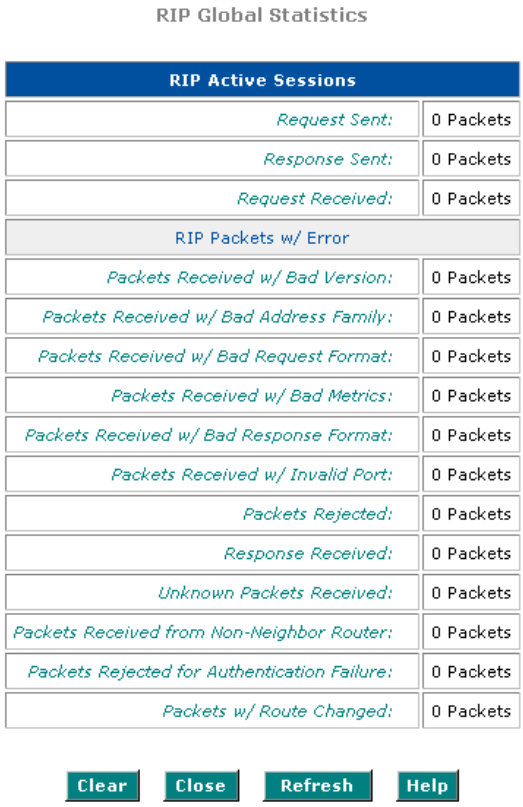


Figure 38 RIP Global Statistics Page

You can click Clear to reset all statistics to 0 and Refresh to display any newly accumulated data.

11. 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 change.
Although you will not typically need to view this information, it may be helpful in working with your ISP to troubleshoot problems you encounter in 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 **Advanced** on the right side of the page, and then click **Alarm** in the task bar.
The Alarm page displays, as shown in Figure 39.

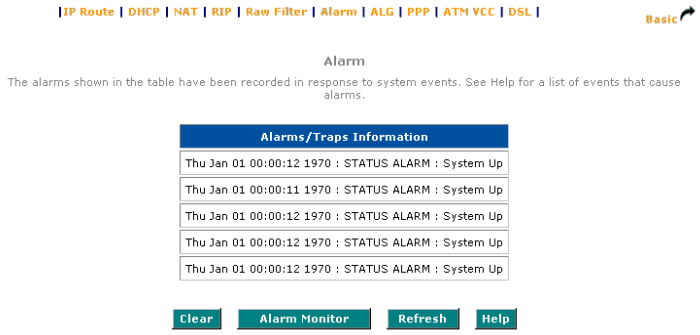


Figure 39 Alarm Page

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.

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

Displaying the Alarm Monitor in a Separate Window

If you want to display an automatically updating Alarm table, you can click Alarm Monitor to display a separate Alarm Monitor window, as shown in Figure 40

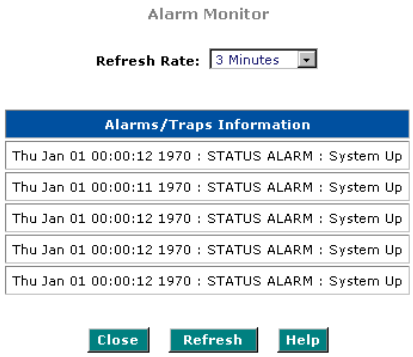


Figure 40 Alarm Monitor Window

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.
You can leave the Alarm Monitor window open and active even after closing the Configuration Manager.

12. Configuring Your PPP Connection

When powered on, your WTM4151 initiates a connection through your DSL line to your ISP. The WTM4151 communicates with your ISP's server using the *Point-to-Point Protocol* (PPP).
This chapter describes how to configure the PPP protocol. Contact your ISP to determine if you will need to change the default settings in order to connect to their server.

Overview of PPP

The 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
- Enabling the ISP to assign Internet information to the customer's computers

Viewing Your Current PPP Configuration

To view your current PPP setup, launch the Configuration Manager, click **Advanced** in the task bar, and then click **PPP**. The PPP Configuration page displays a table with basic information about your PPP setup, as shown in Figure 41.

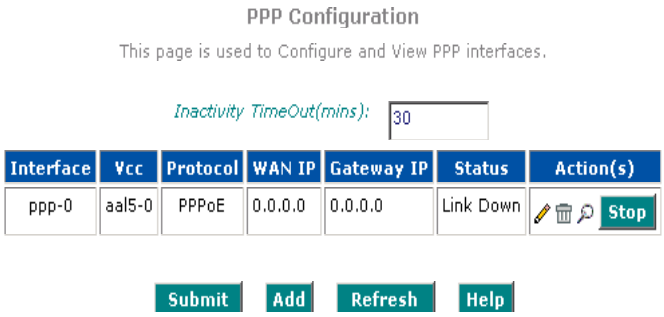


Figure 41 PPP Configuration Page

PPP is configured as a group of software settings associated with the ADSL port. Although the device has only one physical ADSL port, the WTM4151 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. Your WTM4151 is preconfigured with one PPP interface, named *ppp-0*.

The fields that display on the PPP Configuration Page are defined as follows:

Field	Description
Inactivity Timeout (mins)	The number of minutes of inactivity on the PPP interface after which the link will need to be reestablished. After timing out, you will need to log in to your ISP again to re-establish service.
Interface	The predefined name of the PPP interface.
VCC	The Virtual Channel Connection over which this PPP data is sent. The VCC identifies the physical path the data takes to reach your ISP. See Chapter 13 for more information.
Protocol	The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPoE) or PPP-over-ATM (PPoA).
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 gateways" on page 31 for a description of gateway addresses.
Status	Indicates whether the link is currently up or down. *Up* indicates that you are currently logged on to your ISP for using the Internet; *Down* indicates that you are not currently logged in.
Actions	You can use these icons to edit ( ), delete ( ), and view ( ) details on a PPP interface.

When you click to view additional details, the PPP Interface - Detail page displays, as shown in Figure 42.

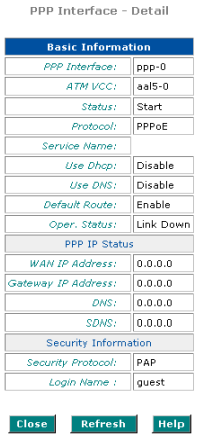


Figure 42 PPP – Detail Page

In addition to the properties defined on page 68, the PPP Interface – Detail table displays these fields:

Field	Description
Service Name	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.
Default Route	Indicates whether the WTM4151 should use the IP address assigned to this connection as its default route. Can be *Enabled* or *Disabled*. See Chapter 7 for an explanation of default routes.
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 may 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 PPP Configuration Page, click Add.
   The PPP Interface – Add page displays, as shown in Figure 43.

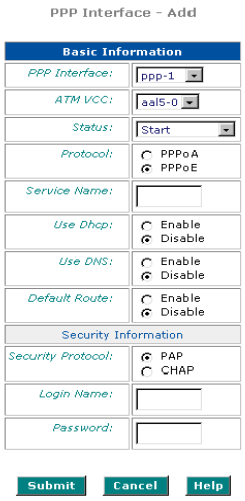


Figure 43. PPP Interface – Add Page

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 re using the PPoA protocol. You can define only one PPP interface c be define if you are using PPPoE. Check with your ISP which version the protocol they require.

The fields are defined in the tables on page 68 and 69.

3. Click Submit.
4. Click **Commit & Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

Modifying and Deleting PPP Interfaces

Modifying a PPP interface's security protocol, login name, and password

To modify a PPP interface, display the 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 44.

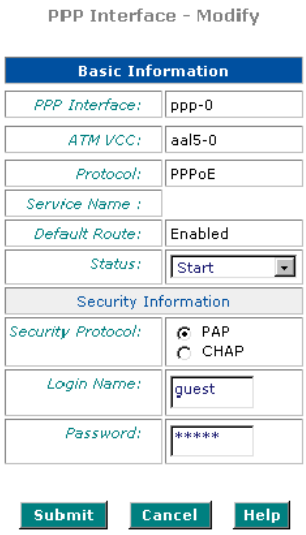


Figure 44 PPP Interface – Modify

You can change the security protocol, your login name, and your password only. To modify the other settings, you must delete the interface and create a new one. After you click Submit, be sure to use the Commit feature to commit your changes to permanent memory, as described on page

Deleting a PPP interface

Do not delete a PPP interface unless you have received instructions to do so from your ISP. Without an appropriately defined PPP interface, you will not be able to connect to your ISP

To delete a PPP interface, display the PPP Configuration page and click in the Action(s) column for the interface you want to delete. Then, use the Commit feature to commit your changes to permanent memory, as described on page

You can recreate the PPP interface with the same name at a later time

13. Configuring the ATM VCC

As your LAN computers access the Internet via the WTM4151, 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.
This chapter describes how to configure the ATM *virtual channel connection (VCC)*, which defines the path WTM4151 uses to communicate with your ISP over the ATM network.

Viewing Your ATM VCC Setup

To view your current configuration, launch Configuration Manager, click **Advanced**, and then click **ATM VCC** in the task bar. The ATM VCC Configuration page displays, as shown in Figure 45.

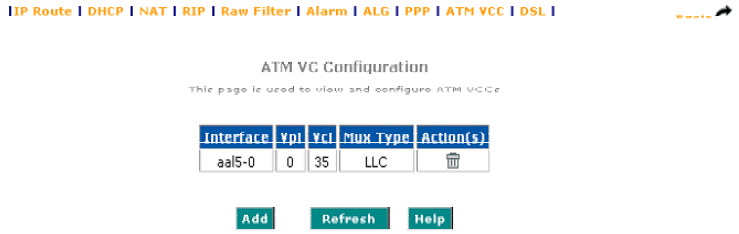


Figure 45 ATM VCC Configuration Page

The ATM VCC Configuration table displays a row for each *VCC interface* currently configured (usually only one). Each set of VCC properties (the VPI, VPI, and Mux Type) is considered an interface because it defines a data path to the device over the ATM network. VCC interfaces are completely defined in software, and then associated with the DSL (WAN) port.

Note

Your device may already be preconfigured with the ecessary ATM VCC interface properties, or the table may contain placeh der values that you must change before using the device. Contact your iP to determine whether you should change any existing values.

You can delete an ATM interface from the ATM Configuration page, by clicking in the Action(s) column.

Adding and Changing ATM VCC Properties

You may need to change the ATM VCC properties if your ISP provides settings that differ from those that were preconfigured. To change the properties associated with a VCC interface, you must delete the VCC interface, and then add a new interface of the same name with new settings.
You may need to create more than one VCC interface if you use multiple services with your ISP.
Before creating a new VCC interface, contact your ISP for the following information:

- VPI
- VCI
- Mux Type: (LLC or VC)

Follow this procedure to add a new VCC interface:

1. From the ATM
   The ATM VCC

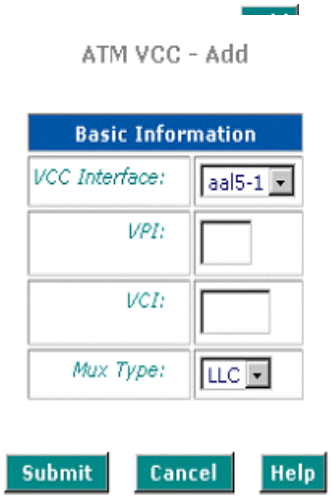


Figure 46 ATM VCC – Add Page

2. Select an interface name from the VCC 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. Click Submit.
5. Click **Commit & Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.
   The new interface should now display in the ATM VCC Configuration table.

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.

14. Viewing DSL Parameters

To view configuration parameters and performance statistics for the WTM4151's DSL line, launch Configuration Manager, click **Advanced**, and then click **DSL** in the task bar. The DSL Status page displays, as shown in Figure 47.

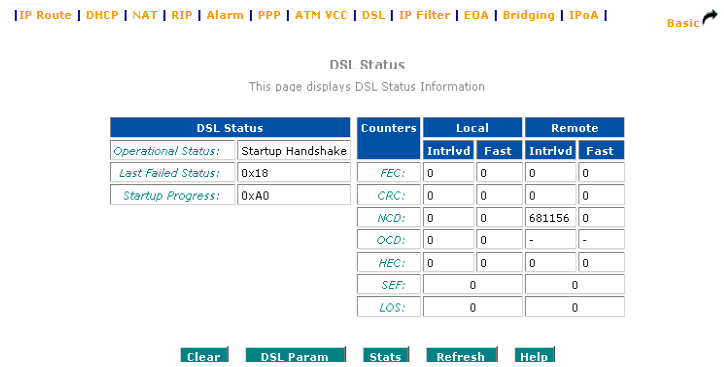


Figure 47 DSL Status Page

The DSL Status page displays current information on the DSL line performance. The page refreshes about every 10 seconds. You can click Clear to reset all counters to zero, and Refresh to redisplay the page with newly accumulated values. Although you generally will not need to view this data, it may be helpful when troubleshooting connection or performance problems with your ISP.

You can click DSL Param to display data about the configuration of the DSL line, as shown in Figure 48. You cannot modify this data.

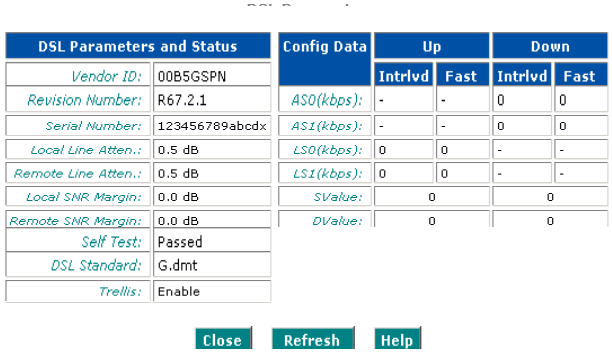


Figure 48 DSL Parameters Page

- 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

From the DSL Sta line performance statistics, as show

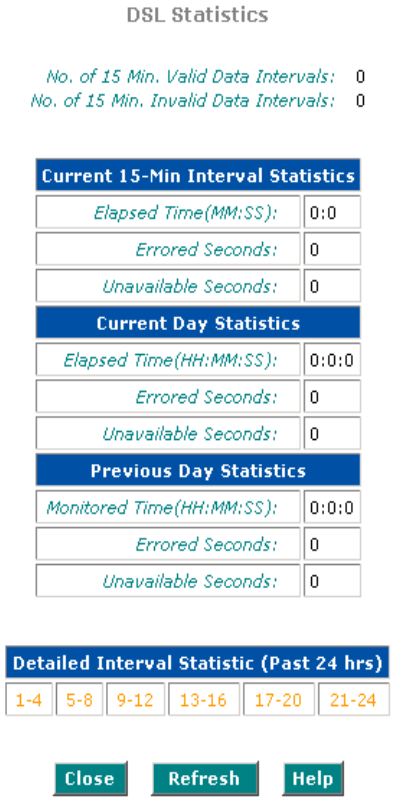


Figure 49 DSL Statistics Page

The DSL Statistics page reports error data relating to the last 15-minute interval, the current day, and the previous day.
The Detailed Interval Statistic 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 15-minute such intervals that make up the previous 4 hours (there are 16 of these).

DSL Interval Statistics

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

Detailed Interval Statistic (Past 24 hrs)

1-4 | 5-8 | 9-12 | 13-16 | 17-20 | 21-24

Close Refresh Help

Figure 50 DSL Interval Statistics Page

15. Configuring IP Filters

The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet. This chapter explains how to create IP filter rules.

Overview

IP filters enable you to control the types of data that pass to and from your network. You can create IP filter rules that block certain computers on your LAN from accessing certain types of data or Internet locations. You can also block incoming access to computers on your LAN.
When you define an IP filter rule and enable the feature, you instruct the WTM4151 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 be either accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

Note

No IP filter rules are predefined and the feature is disabled by default on the WTM4151. All valid data packets are accepted and forwarded to their destination.

Viewing Your IP Filter Configuration

To view your current IP filter configuration, launch Configuration Manager, click **Advanced** in the task bar, and then click **IP filter**. The IP Filter page displays, as shown in Figure 51.

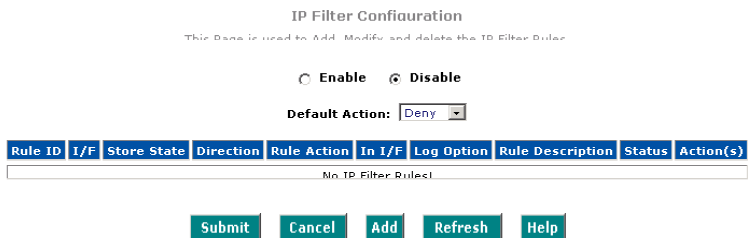


Figure 51 IP Filter Page

The IP Filter page contains the following elements:

- **Enable/Disable radio buttons:** By default, IP filtering is disabled. If you create rules and want them to take effect, you must click the Enable button. If you disable the feature, existing rules will be retained for future use.
- **Default Action drop-down list:** If IP filtering is enabled; you must specify a default action to take effect on all packets that do not match any of the filtering rules. The default action can be *Accept* (forward the packet toward its destination) or *Deny* (discard the packet). Some network administrators may choose to create rules that to deny specific types of packets, and accept by default all packets that do not meet the rules (i.e., the default action is set to *Accept*. For greater security, others may choose to deny all packets by default, and then create rules that enable specific types of communication.
- **IP Filter Rule Table:** The table displays a row for each currently established rule. The IP filter table may be empty when you first view this page. See page 78 for a description of the items that make up a rule. When rules are defined, you can use the icons that display in the Actions column to edit ( ), delete ( ), and view details on ( ) the corresponding rule.

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, and refer to the examples on page 83 for assistance:

1. On the main IP Filter page, click Add.
   The IP Filter Rule – Add page displays, as shown in Figure 52.

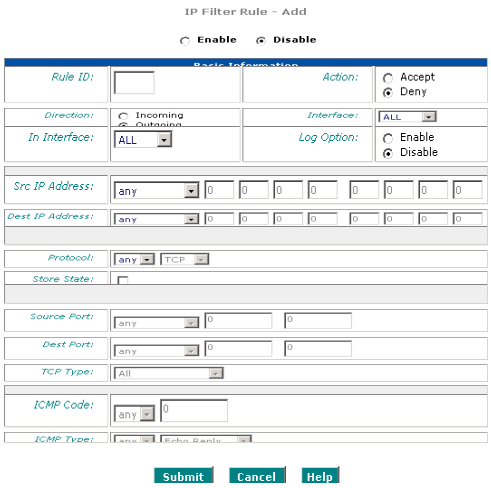


Figure 52. IP Filter Rule – Add Page

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

Field	Des ription
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	Specifies 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	Specifies whether the rule should apply to data packets that are incoming or outgoing on the selected interface. *Incoming* refers to packets coming from the LAN, and *outgoing* refers to packets going to the Internet. You can use rules that specify the incoming direction to prevent outside accesses to your LAN. You can use rules that specify the outgoing direction to block LAN accesses to the Internet.
Interface	Specifies the interface on the WTM4151 on which the rule will take effect. To block LAN accesses to the Internet, you can select either the LAN or WAN interface (if you select "LAN", be careful not to inadvertently define the rule to block access to the device itself). To block outside accesses to the device, such as Telnet access, select the WAN interface.

Field	Des ription
In Interface	Specifies 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 and is useful only when the device is configured with both a LAN and a USB interface, or with multiple LAN or WAN interfaces. For example, if your device connects to two subnets (that is, it has two LAN interfaces, eth-0 and eth-1) and you want to block one of the subnets (say, eth-1) from accessing the web, you would create an outgoing rule on the WAN interface that denies HTTP accesses. You would specify the eth-1 as the incoming interface.
Log Option	Specifies whether on not a log entry will be created on the system each time this rule is invoked. You can log all packets that match the criteria, all packets that do not match the criteria, or all packets of either type. Or, you can disable the logging option. (This feature is made available only for troubleshooting with your ISP.)
Src IP Address	Specifies IP address criteria for the source computer(s) from which the packet originates. In the drop-down list, you can configure the rule to be invoked on packets containing: **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.
Dest IP Address	Specifies IP address rule criteria for the destination computer(s) (i.e., the IP address of the computer to which the packet is being sent). See the description of Src IP Address for the selection options.

Field	Des ription
Protocol	Specifies 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).
Store State	If this option is enabled, then *stateful filtering* is performed and the rule is also applied in the other direction on the given interface during an IP session.
Source Port	Specifies port number criteria for the computer(s) from which the packet originates. This field will be dimmed (unavailable for entry) if you have not specified protocol criteria. See the description of Src IP Address for the selection options.
Dest Port	Specifies port number criteria for the destination computer(s) (i.e., the port number of the type of computer to which the packet is being sent. See the description of Src IP Address for the selection options.
TCP Type	Specifies whether the type of TCP protocol should be restricted to only those packets containing synchronous TCP or only those that do not use synchronous TCP. You can also select *any* if no restriction applies. This field will be dimmed (unavailable for entry) if you have not specified that the protocol must equal *TCP*.
ICMP Code	Specifies whether the value in the code field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (eq), or not equal the specified value, or you can select any to enable the rule to be invoked regardless of the ICMP code field. This field will be dimmed (unavailable for entry) if you have not specified that the protocol must equal *ICMP*.

Field	Des ription
ICMP Type	Specifies whether the value in the type field in ICMP packet headers will be used as a 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 regardless of the ICMP code field. This field will be dimmed (unavailable for entry) if you have not specified that the protocol must equal ICMP.

3. When you are done selecting criteria, click Submit.
   After a confirmation page displays, the IP Filter Configuration page will redisplay with the new rule showing in the table.
   Note that a red ball displays in the Status column, indicating that the rule is currently disabled. All rules are disabled by default when created. You must modify the rule to enable it:
4. In the Action column, click .
   The IP Filter Rule – M... e 53.

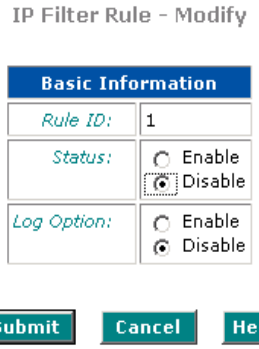


Figure 53. IP Filter Rule – Modify Page

5. In the Status row, click the Enable radio button, and then click Submit.
   The IP Filter Configuration page redisplays with a green ball in the Status column for that rule, indicating that the rule is now enabled.
6. On the IP Filter Configuration page, click the **Enable** radio button to enable the IP filter service.

WARNING

Do not enable the IP filter feature unless you ...ave defined rules and specified a default action. Doing so may res... in filtering out content that you intend to let pass.

7. From the Default Action drop-down list, select **Accept** or **Deny**, depending how you have structured your Rules.
8. Click Submit.
   A page displays to confirm your changes.
9. Click **Commit and Reboot** in the basic task bar, and then follow the instructions on page 25 to commit 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. Define a 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 that the packets must contain the source port associated with the computer you want to block. Alternatively, if the computer is assigned a static IP address, you could specify that value as the criteria.
3. Specify that the packet must be destined for port 80, which is the well-known port number for web servers.
4. Click Submit to create the rule, and then click  to modify the rule and enable it.
5. Choose a default action, enable the IP filtering feature, and commit your changes.
   Figure 54 shows how this rule could be configured:

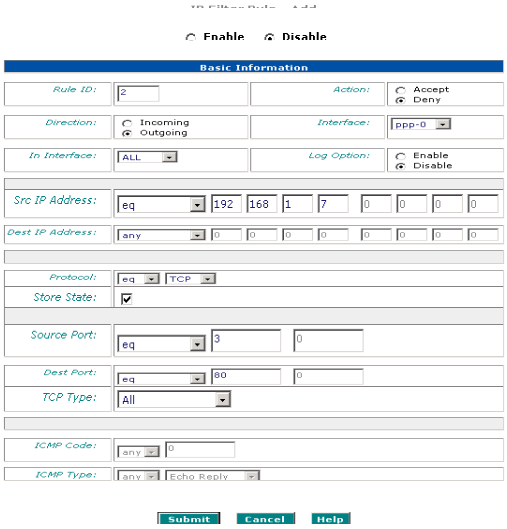


Figure 54 IP Filter Rule Example 1

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).

Example 2. Blocking Telnet accesses to the WTM4151:

1. Define a new rule for incoming 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 for Telnet communication.
3. Click Submit to create the rule, and then click to modify the rule and enable it.
4. Choose a default action, enable the IP filtering feature, and commit your changes.

Figure 55. Shows how this rule could be configured:

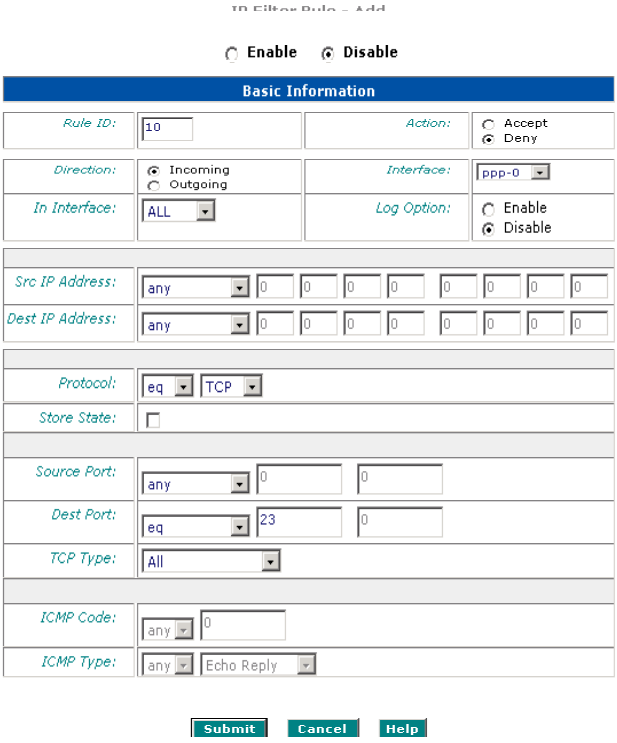


Figure 55 IP Filter Rule Example 2

Viewing IP Filter Statistics

For each rule, you can view statistics on how many packets were accepted or denied. Click Stats in the corresponding row in the IP Filter Rule table. A page such as the following displays:

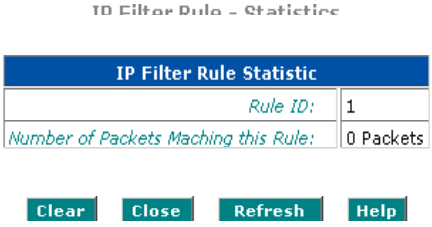


Figure 56 IP Filter Rule – Statistics Page

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

16 Configuring EOA Interfaces

This chapter describes how to configure an EOA (Ethernet over ATM) interface on the WTM4151, if one is needed to communicate with your ISP.

Overview of EOA

The EOA protocol 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 tha EOA for communication with your WTM4151, such as the poi 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 (PPoA), does not. However, if your ISP uses either type of PP, you* ***do not*** *need to create an EOA interface. See Chapter 12 for instructions on co guring a PPP interface.*

Viewing Your EOA Setup

To view your current EOA configuration, launch the Configuration Manager, click **Advanced** in the task bar, and then click **EOA**. Figure 57 shows the EOA configuration page.

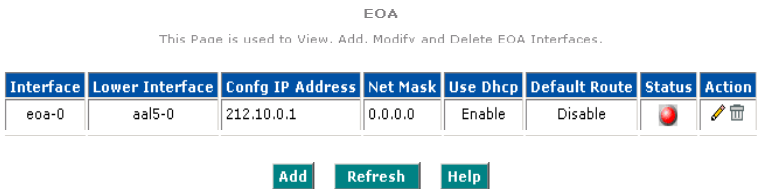


Figure 57 EOA Page

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:

Field	Description
Interface	The name the software uses to identify the EOA interface.
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 VCC interface, such as *aal5-0*, as described in Chapter 13.
Config IP Address and *Net Mask*	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 WTM4151 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 checked, 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 WTM4151 should use the IP address assigned to this interface, if any, as its default route for your LAN. This can be *Enable* or *Disable*. See Chapter 7 for an explanation of default routes.
Status	A green or red ball will display to indicate that the interface is currently enabled or disabled, respectively. You cannot manually enable or disable the interface; a disabled interface 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. Display the EOA
   The EOA Interfac

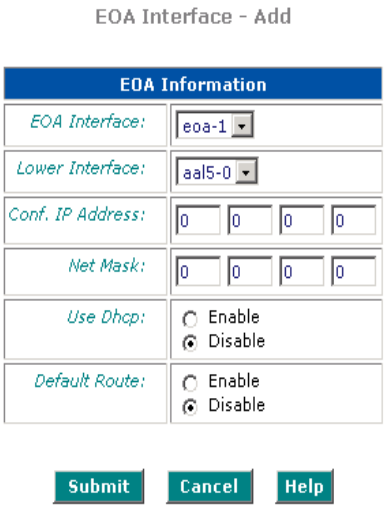


Figure 58 EOA Interface – Add Page

2. Select one of the predefined interface names from the EOA Interface drop down list.
3. In the Lower Interface field, select the lower-level interface name over which this protocol is being configured. Typically, an EOA interface is configured to operate over an aal5 interface, such as aal5-0.
   If you are using the WTM4151 as a bridge only, skip to step 5.
4. If you are using the WTM4151 as a router on your LAN, enter the IP address and network mask you want to assign to the interface. This address serves as the public IP address for your entire LAN and is usually assigned by your ISP.
   Or, if your ISP will assign this information, click the Enable radio button to set up the DHCP service.
   Also, specify whether this interface should serve as the default route for your LAN for accessing the Internet.
5. Click Submit.
   A confirmation page display to confirm your changes
6. Click **Commit & Reboot** in the basic task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

17. Configuring Bridging

WTM4151 can be configured to act as a bridging device between your LAN and 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 WTM4151 to operate as a bridge.


Note

Before changing your bridge configuration, check w h your ISP to determine the type of connection they use to exchange data w h 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 learns that some of the IDs represent computers attached via one of the WTM4151's interfaces and others represent computers connected via other interfaces. It stores the ID list and the interfaces associate with each 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 network where that device resides. 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 the 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 bet een a bridge and a router is that a router uses a higher-level protocol (ch as the IP) to determine how to pass data. IP data packets conta IP addresses that specifically identify the destination computer. Rout s can read this information and pass the data to the destination co puter, or determine which next router to send the data to if the destinat n is not on a connected network.*

Bridges cannot read or use IP information, but inst d use the manufacturer-assigned hardware IDs to determine e port through which it should send the data packet.

Routers are considered more intelligent and flexibl devices than bridges, and often provide a variety of security and network dministration services.

Using the WTM4151's Bridging Feature

Although the WTM4151 is preconfigured to serve as a router for providing Internet connectivity to you 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.

In both cases, you need to specify the device's interfaces as bridge interfaces.

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. Launch Configuration Manager, click **Advanced**, and then click **Bridging** in the task bar.
   The Bridge Configuration page displays, as shown in Figure 59.

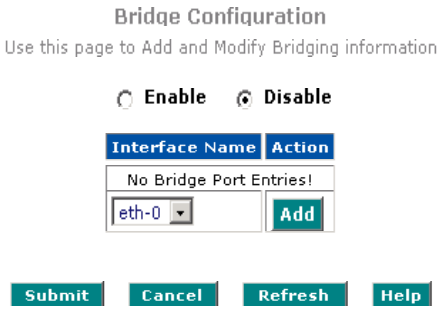


Figure 59 Bridge Configuration Page

The table may be empty if bridging has not yet been established.

2. 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 such protocols on an USB-connected computer, you can also select *usb-0*.

Note

If you do not have an eoa-0 interface, but instead h ve an interface named ppp-0 *or* ipoa-0*, your device is not currently configu ed with a WAN interface that allows bridging with your ISP. You may want t heck with your ISP to determine whether they use this protocol. See Cha er 16 for instructions on creating an EOA interface.*

Note

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

You can determine whether the Ethernet (eth-0) an USB (usb-0) interfaces have been assigned IP addresses by displaying the P Address Table (in the basic task bar, click **IP Address***). These interfaces ill display in the table only if they have been assigned IP addresses.*

You can check whether the eoa-0 interface has bee assigned an IP address by displaying the EOA configuration table (the advanced task bar, click **EOA***). If the Config IP Address field is empty a l the Use DHCP field contains the word* Disable*, then no IP address has b en assigned.*

3. Click the **Enable** radio button to turn on bridging.
4. Click Submit.
   A page will display to confirm your changes.
5. Click **Commit & Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

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 bridging.

18 Configuring IPoA Interfaces

This chapter describes how to configure an IPoA (Internet Protocol over ATM) interface on the WTM4151.
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 environments, to eliminate unneeded variables when testing IP layer processing.

Viewing Your IPoA Interface Setup

To configure an IPoA interface, launch Configuration Manager, click **Advanced**, and then click **IPoA** in the task bar. The IPoA page displays, as shown in Figure 60.

Figure 60 IPoA 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
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 VCC interface, such as *aal5-0*, as described in Chapter 13.
Config IP Address and *Net Mask*	The IP address and network mask you want to assign to the interface.
Status	A green or red ball will display to indicate that the interface is currently enabled or disabled, respectively.

Field	Description
	You cannot manually enable or disable the interface; a disabled interface may indicate a problem with the DSL connection.
Action	Icons you can click on to edit ( ) or delete ( ) the associated EOA 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 61.

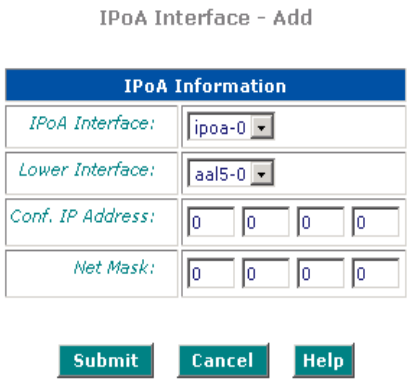


Figure 61 IPoA Interface – Add Page

2. Select one of the predefined interface names from the IPoA Interface drop down list.
3. In the Lower Interface dialog box, select the lower-level interface name over which this protocol is being configured. Typically, an IPoA interface is configured to operate over an aal5 interface.
   Enter the IP address and network mask you want to assign to the interface.
4. Click Submit.
   A confirmation page will display to confirm your changes.
5. Click **Commit & Reboot** in the task bar, and then follow the instructions on page 25 to commit your changes to permanent memory.

Appendix A
IP Addresses, Network Masks, and Subnets

IP Addresses

Note

This section pertains only to IP addresses for IPv4 (ersion 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary nu bers, bits and bytes.

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 shows the structure of an IP address.

Table. IP Address structure

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

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
mask

A mask *looks like a regular IP address, but co tains a pattern of bits that tells what parts of an IP address are the n twork ID and what parts are the host ID: bits set to 1 mean "this bit is p rt of the network ID" and bits set to 0 mean "this bit is part of the ho t 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 ac tional network ID bits, and thus no subnets. Such a mask is called a defa 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 wh n a network is initially configured, at which time it has no subnets.*

Appendix B
Trouble Shooting

This appendix suggests solutions for problems you may encounter in installing or using your WTM4151, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Problem	Troubleshooting Suggestion
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 WTM4151 and a wall socket/power strip.
LINK WAN LED does not illuminate after phone cable is attached.	Verify that a standard telephone cable like the one provided is securely connected to the ADSL port and your wall phone jack. Wait 30 seconds to allow 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 WTM4151. Make sure the PC and/or hub is turned on. Verify that you are using a cross-type Ethernet cable to the uplink port on a hub or a straight-through type cable to a stand-alone PC. (Hold the connectors at each end of the cable side-by-side in the same position. If the order of their color-coded wire pairs is the same, it is a straight-through type.) Contact Customer Support if your cable is not the correct type. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled Cat 5. 10Mbit/sec cables may tolerate lower quality cables.
DIAG LED stays illuminated after turning the device on.	The DIAG LED should turn off after about 10-15 seconds. If it does not, turn off the WTM4151, wait 10 seconds, and then turn it back on.
Internet Access	
PC cannot access Internet	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the WTM4151'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

Problem	Troubleshooting Suggestion
	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, 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 (see the Quick Start instructions, Part 2). • 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 WTM4151 to translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules (see Chapter 9). 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 8 to view the address pool).
PCs cannot display web pages on the Internet.	Verify that the DNS server specified on the PCs is correct for your ISP, as discussed in the item above. You can use the ping utility, discussed in the following section, to test connectivity with your ISP's DNS server.
Configuration Manager Program	
You forgot/lost your 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 (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.
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 WTM4151'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

Problem	Troubleshooting Suggestion
	later, or Netscape Navigator v4.7 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 WTM4151.
Changes to Configuration Manager are not being retained.	Be sure to use the Commit function after any changes. This function is described on page 25

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 you are trying to communicate with.
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 

. 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.

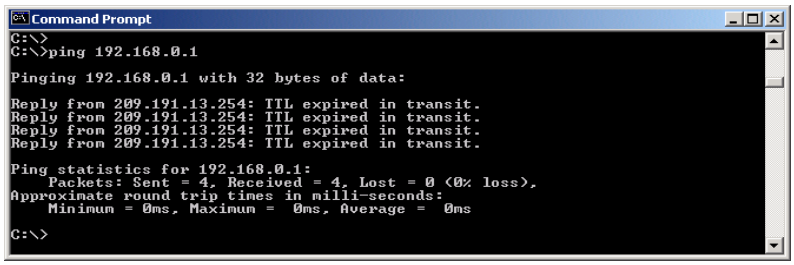


Figure 62. Using the ping Utility

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 your WTM4151 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 (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 

. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address you are interested in, such as www.microsoft.com.

The window will display the associate IP address, if known, as shown in Figure 63

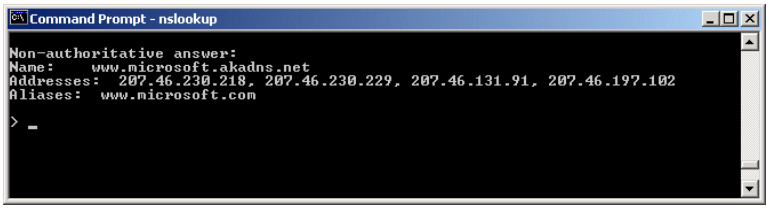


Figure 63 Using the nslookup Utility

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.

Appendix C
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 WTM4151 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.
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 WTM4151'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, www.globespan.net is the domain name associated with IP address 209.191.4.240. Domain names must be unique; the Internet Corporation controls their assignment 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., http://www.globespan.net/index.html. *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 10BASE-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 the 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. Packet filtering and Network Address Translation services can provide some firewall protection.
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.
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 web browsers can display it. *See also web browser, web site*.
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.
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 WTM4151 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, "IP Addresses Explained" section*.
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 or not 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 WTM4151 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 I 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 has their own wiring and jacks. Your telephone company installs the splitter 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 time duration, the TTL is usually represented instead as a maximum hop count. 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*.
Pstream	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 WTM4151 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 WTM4151, WAN refers to the Internet.
Web browser	A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and also 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, and WWW*.

3731 Wilshire Blvd. Suite 506. Los Angeles, CA 90010. Tel: 213-380-7555, Fax: 213-380-1736. Http://www.wtcelectronics.com. Email: sales@wtcelectronics.com.

WTC Electronics
3731 Wilshire Blvd., Suite 506
Los Angeles, CA 90010
Tel: (213) 380-7555
Fax: (213) 380-1736
http://www.wtcelectronics.com