PROLINE® G90-6100 (MODEL 6100)
PROLINE® G90-6110 (MODEL 6110)

USER GUIDE

CONTENTS

1. PRODUCT DESCRIPTION

The Westell® ProLine® G90 DSL modem provides reliable, high-speed, Internet access to your existing home or office phone line. Your ADSL connection is "always-on" ending the hassles of dial-up modems and busy signals. Installation is easy... no tools... no headaches. Simply connect the hardware, apply power, and perform the simple software configuration for your Modem and you are on the Internet.

This DSL modem is capable of data rates hundreds of times faster than a traditional analog modem. But unlike analog modems, Westell's DSL modem allows you to use the same phone line for simultaneous voice/fax communications and high-speed Internet access, eliminating the need for dedicated phone lines for voice and data needs.

Hereafter, the Westell® ProLine® G90 DSL modem will be referred to as the "modem."

This modem is powered by an ENERGY STAR® qualified adapter.

2. SAFETY INSTRUCTIONS

- Never install any telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch non-insulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

WARNING

Risk of electric shock. Voltages up to 140 Vdc (with reference to ground) may be present on telecommunications circuits.

3. REGULATORY INFORMATION

3.1 FCC Compliance Note

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

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

PART 68 - COMPLIANCE REGISTRATION

This equipment (Models 6100, 6110) complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. A label on the bottom of this equipment contains, among other information, the Ringer Equivalence Number (REN) and the product identifier. For products approved after July 23, 2001 the product identifier is in the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g. 03 is a REN of 0.3). The REN is used to determine the number of devices that may be connected to a telephone line. For earlier products, the REN is separately shown on the label. If requested, this number must be provided to the telephone company.

Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most, but no all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

This equipment is designated to connect to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant. An FCC compliant telephone cord and modular plug is provided with the equipment. See the Installation Information section of this User Guide for details.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instruction for details.

If this terminal equipment (Models 6100, 6110) causes harm to the telephone network, the telephone company may request you to disconnect the equipment until the problem is resolved. The telephone company will notify you in advance if temporary discontinuance of service is required. If advance notification is not practical, the telephone company will notify you as soon as possible. You will be advised of your right to file a complaint with the FCC if you believe such action is necessary.

If you experience trouble with this equipment (Models 6100, 6110), do not try to repair the equipment yourself. The equipment cannot be repaired in the field and must be returned to the manufacturer. Repairs to certified equipment should be coordinated by a representative, and designated by the supplier. Refer to section 12 in this User Guide for further details.

The telephone company may make changes to their facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice in order for you to make the modifications necessary to maintain uninterrupted service.

If your home has specially wired alarm equipment connected to the telephone line, ensure that the installation of this equipment (Models 6100, 6110) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection of this equipment to party line service is subject to state tariffs.

3.2 Canada Certification Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operations and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The department does not guarantee the equipment will operate to the user's satisfaction.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specification. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specification were met. It does not imply that Industry Canada approved the equipment. The Ringer Equivalence Number (REN) is 0.0. The Ringer Equivalence Number that is assigned to each piece of terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local Telecommunication Company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Connection to a party line service is subject to state tariffs. Contact the state public utility commission, public service commission, or corporation commission for information.

If your home has specially wired alarm equipment connected to the telephone line, ensure that the installation of this equipment (Models 6100, 6110) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

If you experience trouble with this equipment (Models 6100, 6110), do not try to repair the equipment yourself. The equipment cannot be repaired in the field and must be returned to the manufacturer. Repairs to certified equipment should be coordinated by a representative, and designated by the supplier. Refer to section 12 in this User Guide for further details.

The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

Users should ensure, for their own protection, that the electrical ground connections of the power utility, telephone lines, and internal, metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

⚠ CAUTION ⚠

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

4. HARDWARE FEATURES

4.1 LED Indicators

This section explains the LED States and Descriptions. LED indicators are used to verify the unit's operation and status.

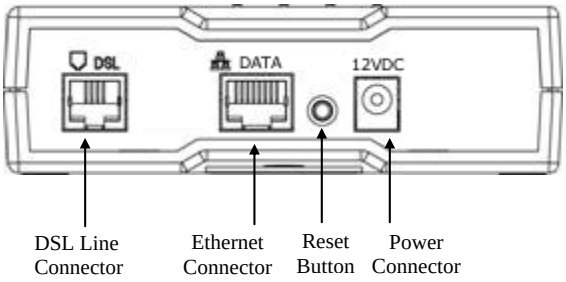
LED States and Descriptions

LED	State	Description
POWER	**Solid Green**	Modem power is ON.
	OFF	Modem power is OFF.
	Solid Red	POST (Power On Self Test), Failure (not bootable) or Device Malfunction. Note: The Power LED should be red no longer than two seconds after the power on self test passes.
ETHERNET	**Solid Green**	Powered device is connected to the associated port (includes devices with wake-on LAN capability where slight voltage is supplied to an Ethernet connection). Note: When using the optional uplink port (E1), Ethernet LAN connection is limited to E2, E3, and E4.
	Flashing Green	10/100 Base-T LAN activity is present (traffic in either direction)
	OFF	Modem power is OFF, no cable or no powered device is connected to the associated port.
USB	**Solid Green**	USB link established.
	Flashing Green	USB LAN activity present (traffic in either direction).
	OFF	No USB link established.
DSL	**Solid Green**	Good DSL link.
	Flashing Green	DSL attempting to sync.
	Solid Amber	Modem is in safeboot mode.
	OFF	Modem power is OFF.
INTERNET	**Solid Green**	Internet link established. With DSL up, the modem has a WAN IP address from IPCP or DHCP; or a static IP is configured; or PPP negotiation has successfully completed (if used) and no traffic is detected.
	Flashing Green	IP connection established and IP Traffic is passing through device (in either direction). Note: If the IP or PPP session is dropped due to an idle timeout, the light will remain solid green, if a DSL connection is still present. If the session is dropped for any other reason, the light is turned OFF. The light will turn red when it attempts to reconnect and DHCP or PPP fails).
	Solid Red	Device attempted to become IP connected and failed (no DHCP response, no PPP response, PPP authentication failed, no IP address from IPCP, etc.).
	OFF	Modem power is OFF or the DSL connection is not present.

4.2 Cable Connectors and Locations

- DSL connector (RJ-11)
- Ethernet (RJ-45) connector DATA port
- Reset push button
- Power connector (12 VDC) barrel

Model 6100 and Model 6110 - Rear View



4.3 Connector Descriptions

The following chart displays the modem's connector types.

NAME	TYPE	FUNCTION
DSL	Modular 6-pin (RJ-11) DSL jack	Connects the modem to a telephone jack that has active DSL service or to the DSL port of a POTS splitter.
DATA	Modular 8-pin (RJ-45) Ethernet jack	Connects the modem to a PC or Hub via 10/100 BaseT Ethernet.
12VDC	Barrel connector	Connects the 12 VDC power connector to an AC wall jack.

4.4 Installation Requirements

This section explains the hardware installation procedures for installing your modem.

To install the modem, you will need the following:

- Active DSL line
- Network Interface Card (NIC) installed in your PC, or
- Available USB port installed in your PC

IMPORTANT: Please wait until you have received notification from your Internet service provider (ISP) that your DSL line has been activated before installing your modem.

4.5 Before You Begin

Make sure that your kit contains the following items:

- Westell ProLine G90 DSL modem
- Power Supply
- Y-cable comprising:
  - Built-in 10/100 BaseT Ethernet cable—labeled PC/Ethernet, yellow
  - Built-in USB cable—labeled PC/USB, blue
- RJ-11 Phone cable
- CD-ROM containing User Guide in PDF format

4.6 Microfilters

DSL signals must be blocked from reaching each telephone, answering machine, fax machine, computer modem, or any similar conventional device. Failure to do so may degrade telephone voice quality and DSL performance. Install a microfilter if you desire to use the DSL-equipped line jack for telephone, answering machine, fax machine, or other telephone device connections. Microfilter installation requires no tools or telephone rewiring. Just unplug the telephone device from the baseboard or wall mount and snap in a microfilter; next, snap in the telephone device. You can purchase microfilters from your local electronics retailer, or contact the original provider of your DSL equipment.

5. HARDWARE INSTALLATIONS

The following instructions explain how to install your modem using 10/100 Base-T Ethernet or USB connections. Before you begin, please read the following notes:

NOTE:

1. If your Ethernet card does not auto-negotiate, set it to half duplex. Refer to the Ethernet card manufacturer's instructions for installing and configuring your Ethernet card.
2. If you are using your modem in conjunction with an Ethernet Hub or Switch, refer to the manufacturer's instructions for proper installation and configuration.
3. When using a microfilter, confirm that the DSL RJ-11 phone cable is connected to the DSL port of the DSL/HPN non-filtered jack.
4. It is recommended that you use a surge suppressor to protect equipment attached to the power supply. **Use only the power supply provided with your kit.**
5. Depending on the installation method you are using, additional Ethernet cables may be required. Ethernet cables and DSL filters can be purchased at your local computer hardware retailer.

5.1 Connecting Your Modem to a DSL Network

To connect your modem to a network provisioned with active DSL service, please follow these steps:

1. Connect the DSL phone from the connector marked **DSL** on the rear panel of the modem to the telephone wall jack provisioned with DSL service. Please use the DSL phone cable that was provided with your kit.

   IMPORTANT: Plug the RJ-11 DSL phone cable from the modem into the DSL port of the microfilter plugged into the telephone jack at the wall.

2. Plug the small end of the power supply cord into the connector marked **12VDC** on the rear panel of the modem. Plug the other end of the power supply into an AC wall socket.
3. Check to see if the **POWER** LED is solid green. Solid green indicates that the modem is functioning properly.
4. Check to see if the **DSL** LED is solid green. If it is solid green, DSL is functioning properly.
5. Log on to your account, and establish an Internet connection, as explained later in section 7, "Accessing Your Modem."
6. Check to see if the modem's **INTERNET** LED is solid green. Solid green indicates that the Internet link has been established. (Flashing green indicates the presence of IP traffic.)

Congratulations! You have completed the installation. Now, go to section 5.1.1, "Connecting Ethernet Devices to Your Modem," or section 5.1.2, "Connecting USB Devices to Your Modem," depending on your PC's configuration.

5.1.1 Connecting Ethernet Devices to Your Modem

To network computers in your home or office to your modem using an Ethernet installation, please follow these steps:

1. Ensure that you have connected your modem to your broadband service using the installation method explained earlier in section 5.1, "Connecting Your Modem to a DSL Network."
2. Obtain an Ethernet cable. Connect the Ethernet cable from the **DATA** port on the rear panel of the modem to the Ethernet port on your computer.
3. Check to see if the modem's **ETHERNET** LED is solid green. Solid green indicates that the Ethernet connection is functioning properly. Check the **ETHERNET** LED for each Ethernet jack to which you are connected.

Congratulations! You have completed the connection. Now, go to section 7, "Accessing Your Modem," to access your modem's Web pages.

5.1.2 Connecting USB Devices to Your Modem

It is recommended that you connect your modem via Ethernet connections. However, if you choose to connect your computer via USB, please follow the instructions in this section.

IMPORTANT: The USB installation will not function for Macintosh computers. Macintosh users will need to install the modem via Ethernet connection. Refer to section 5.1.1, "Connecting Ethernet Devices to Your Modem," for Ethernet installation instructions.

To network a computer in your home or office to your modem using a USB connection, please follow these steps:

1. Ensure that you have connected your modem to your broadband service using one the installation method explained earlier in section 5.1, "Connecting Your Modem to a DSL Network."
2. Insert the CD-ROM provided with your kit into the CD-ROM drive of the PC that will connect via USB.
3. Use the Y-cable provided with your kit. At the "Y" end of the cable, plug the USB jack (labeled PC/USB, blue) into the USB port on your computer. Then, at the other end of the Y-cable, plug the Ethernet jack (labeled PC/ETHERNET, yellow) into the Ethernet connector marked **DATA** on the rear panel of the modem.
4. Plug the small end of the power supply cord into the connector marked **12VDC** on the rear panel of the modem. Plug the other end of the power supply into an AC wall socket.
5. Complete the instructions outlined in section 6, "Installing the USB Drivers." Then, return to this section to complete the remaining step.
6. After the USB drivers have been installed, check to see if the **USB** LED is solid green. Solid green indicates that the USB connection is functioning properly.

Congratulations! You have completed the USB hardware installation. Now, go to section 7, "Accessing Your Modem," to access your modem's Web pages.

6. INSTALLING THE USB DRIVERS

This section explains how to install the USB drivers for your modem. If you are using only an Ethernet connection, USB driver installation is not necessary. The Microsoft Plug and Play (PnP) auto-detect feature recognizes when new hardware has been installed. After you connect the modem to the PC, the modem will be detected automatically.

IMPORTANT: Make sure that the CD-ROM provided with your kit is inserted into the PC's CD-ROM drive before connecting the USB jack, as explained in section 5.1.2, "Connecting USB Devices to Your Modem."

Determine which operating system is installed on your PC, and then follow the USB driver instructions that match your operating system. The following table provides a reference to the USB driver installation instructions. After you have completed the USB driver installation, return to section 5.1.2, "Connecting USB Devices to Your Modem," to complete the USB hardware installation instructions.

Your Operating System	Refer to this section for USB driver instructions
Windows 2000	6.1. Installing the USB Driver for Windows 2000
Windows XP	6.2. Installing the USB Driver for Windows XP
Windows Vista™	6.3. Installing the USB Driver for Windows Vista™

6.1 Installing the USB Driver for Windows 2000

To install the USB driver for Windows 2000, please follow these steps:

IMPORTANT: Confirm that the CD-ROM provided with the modem kit is inserted into the PC's CD-ROM drive before beginning this installation.

1. **Windows 2000:** After you connect the modem to your PC, the **Found New Hardware** window will appear (Figure 1). After a brief delay, the **Found New Hardware Wizard** will appear (Figure 2). Click **Next**.

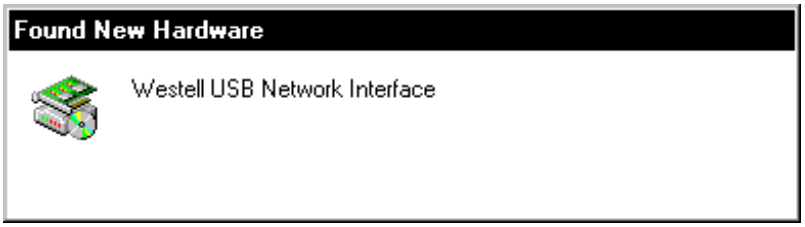


Figure 1. Windows 2000

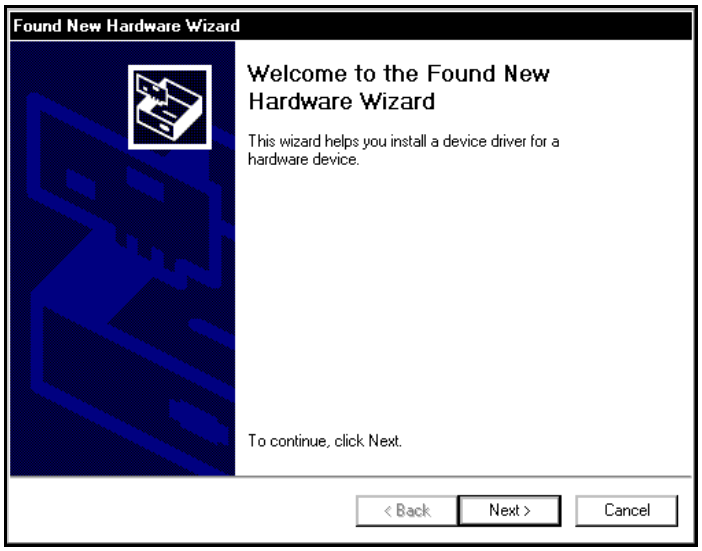


Figure 2. Windows 2000

2. **Windows 2000:** The **Install Hardware Device Drivers** window will appear (Figure 3). Select **Search for a suitable driver for my device (recommended)**. Click **Next**.

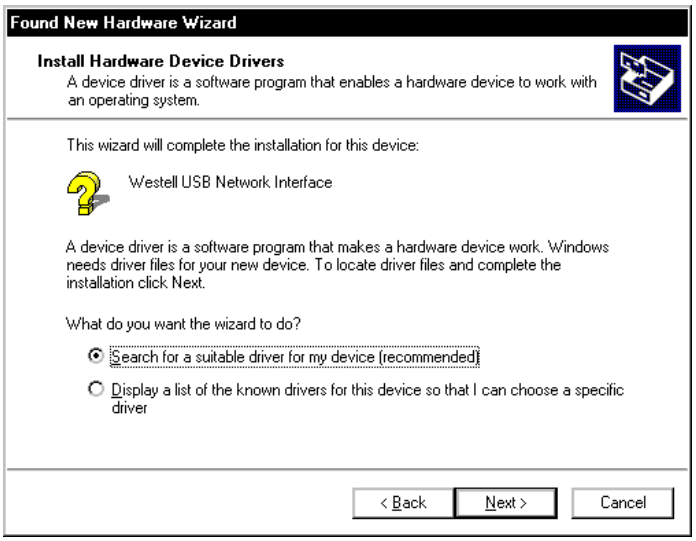


Figure 3. Windows 2000

3. **Windows 2000:** The **Locate Driver Files** window will appear. Select **CD-ROM drives** (Figure 4). Click **Next**.

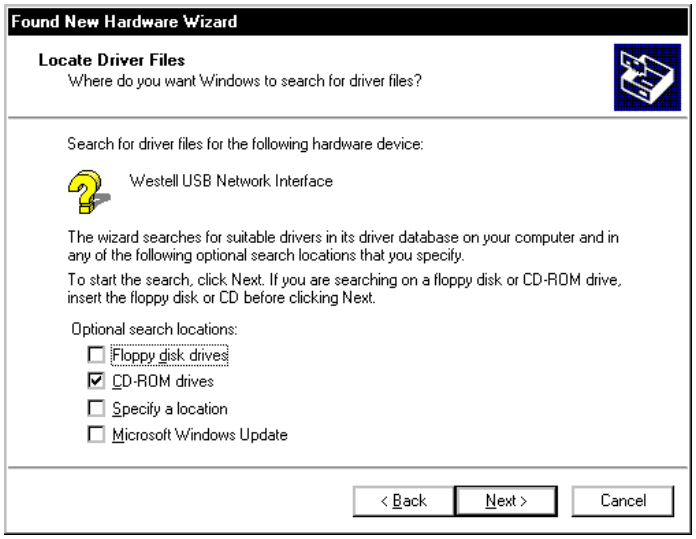


Figure 4. Windows 2000

4. **Windows 2000:** The **Driver Files Search Results** window will appear (Figure 5). Note the drive "letter" may vary. Click **Next**.

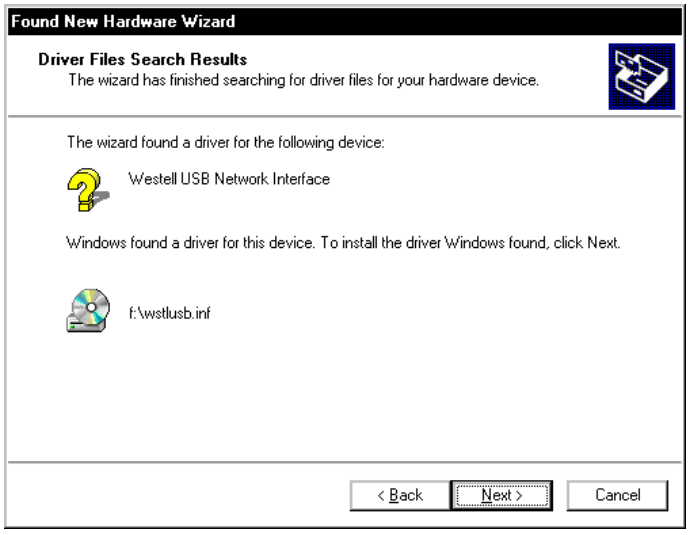


Figure 5. Windows 2000

5. **Windows 2000:** The window below confirms that the PC has finished loading the drivers (Figure 6). Click **Finish**.

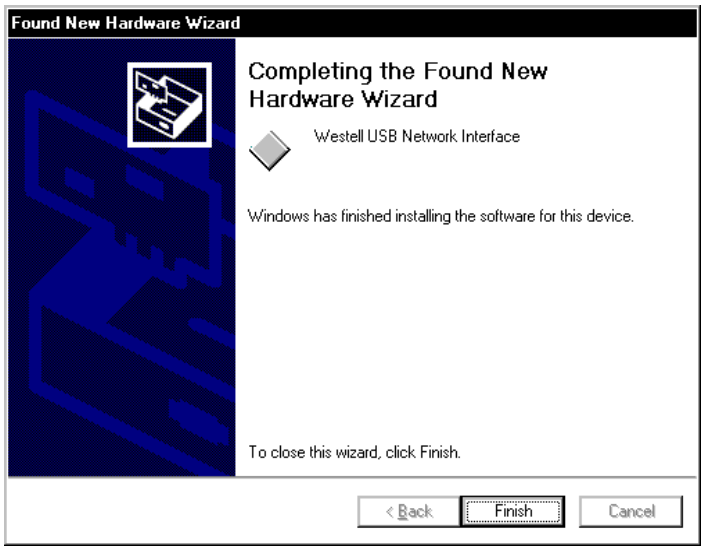


Figure 6. Windows 2000

6. **Windows 2000**: When the **System Settings Change** screen appears, the USB drivers are installed properly (Figure 7). Click **Yes** to restart your computer**.**

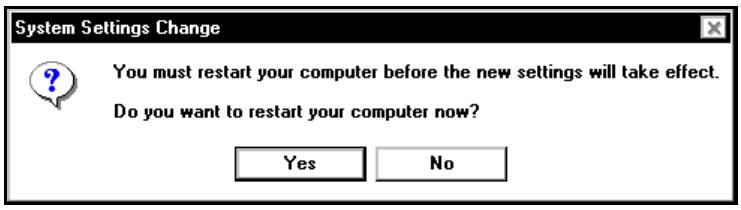


Figure 7. Windows 2000

Congratulations! You have completed the software installation for the USB drivers. Now, return to section 5.1.2, "Connecting USB Devices to Your Modem," to complete the hardware installation instructions.

6.2 Installing the USB Driver for Windows XP

To install the USB driver for Windows XP, please follow these steps:

IMPORTANT: Confirm that the CD-ROM provided with the modem kit is inserted into the PC's CD-ROM drive before beginning this installation.

1. **Windows XP:** After you connect the modem to your PC, the following screen will appear (Figure 8). Select **Install the software automatically (Recommended)**. Click **Next**.

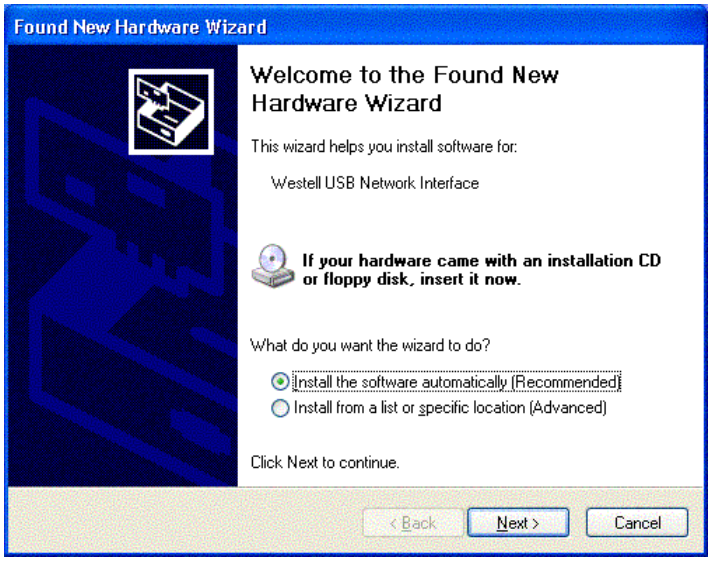


Figure 8. Windows XP

2. **Windows XP**: The window below confirms that the PC has finished loading the drivers (Figure 9). Click **Finish**.

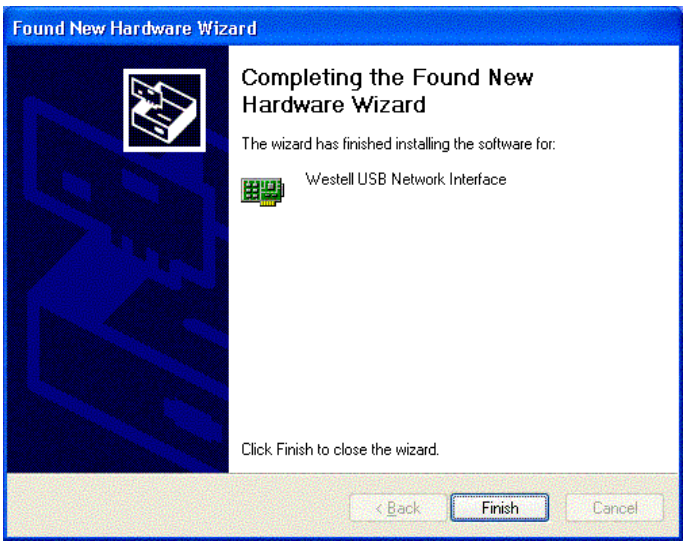


Figure 9. Windows XP

Congratulations! You have completed the software installation for the USB drivers. Now return to section 5.1.2, "Connecting USB Devices to Your Modem," to complete the hardware installation instructions.

6.3 Installing the USB Driver for Windows Vista™

To install the USB driver for Windows Vista™, please follow these steps:

IMPORTANT: Confirm that the CD-ROM provided with the modem kit is inserted into the PC's CD-ROM drive before beginning this installation.

1. **Windows Vista™:** After you connect the modem to your PC, the following **Found New Hardware** screen will appear (Figure 10). Click **Next**.

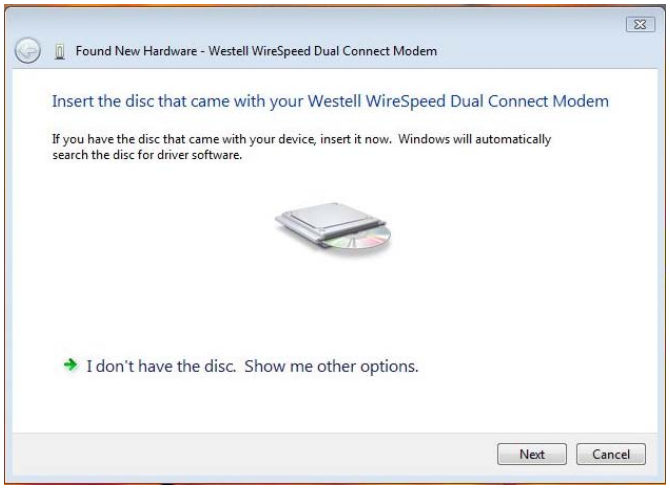


Figure 10. Windows Vista

2. **Windows Vista™**: The window below confirms that the PC has finished loading the drivers (Figure 11). Click **Close**.

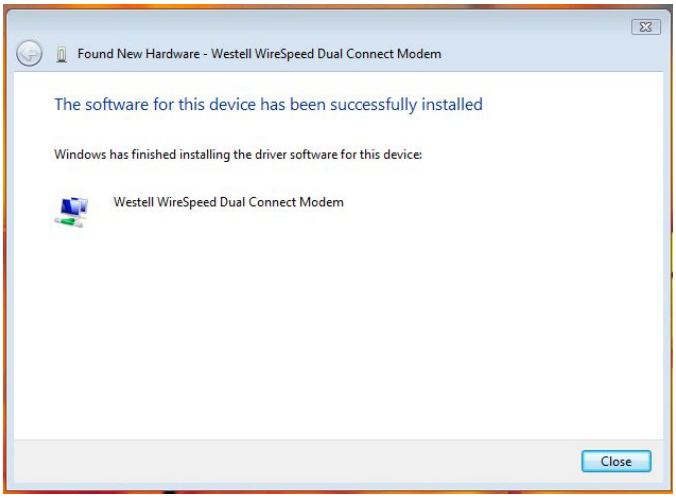


Figure 11. Windows Vista

Congratulations! You have completed the software installation for the USB drivers. Now return to section 5.1.2, "Connecting USB Devices to Your Modem," to complete the hardware installation instructions.

7. ACCESSING YOUR MODEM

7.1 Logging on to Your Modem

This section explains the logon procedures for your modem. These procedures should be used any time you want to access or make changes to your modem's configurations or firewall settings.

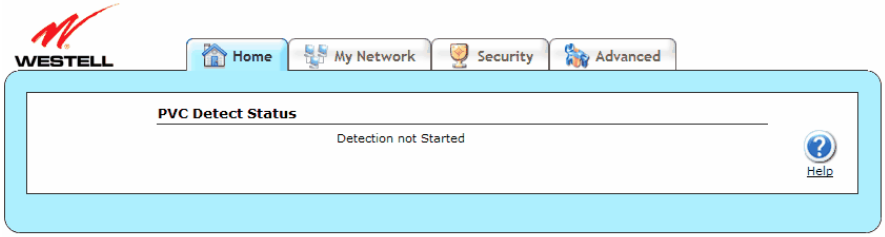
IMPORTANT: Your modem is capable of automatically sensing protocol type (DHCP or PPPoE). This process is designed to start after you have connected your modem to your network. To access your modem's Web pages, your PC must be configured for DHCP. Refer to your Windows help screen for information on configuring your computer for DHCP. At your PC, click **Start**, then **Help** to access the Windows help screen.

Your ISP determines the type of protocol you will use to connect to the Internet. Routed IP allows you to connect to your ISP equipment without first having to identify yourself (authenticate) with your ISP. PPPoE requires that you authenticate (type an account ID and password) before obtaining an Internet connection. After automatic protocol detection starts, the modem will determine which protocol you will use for your Internet connection.

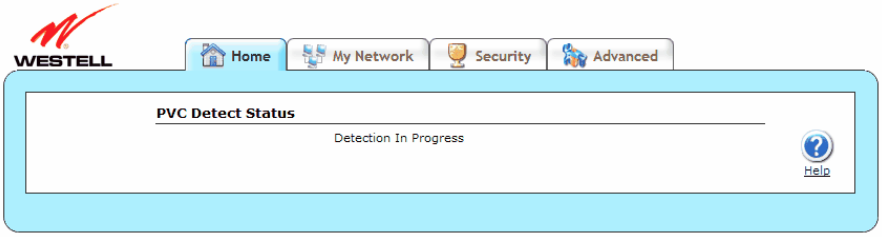
To log on to your modem, start your Web browser, and type the following IP address in the browser's address bar:

http://192.168.1.1

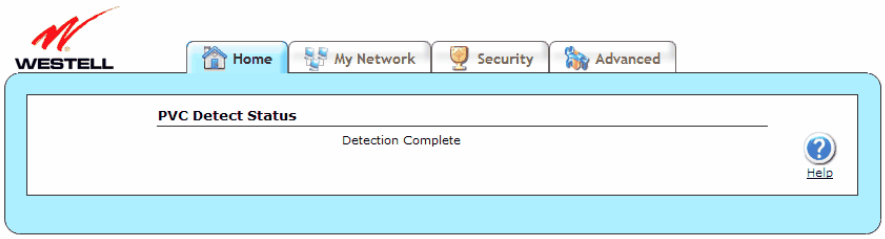
After you have typed the URL address, press **Enter** on your keyboard. If your modem has the Automatic PVC Detection feature enabled (optional), you will see this screen while the modem detects and configures the WAN connection.



The detection process will then begin as shown in the following screen.



Once the detection process is complete, you will see the following screen.



7.1.1 Connecting to the Internet via Routed IP Protocol

If Automatic WAN Protocol Detection finds that your ISP's server is DHCP, the ISP's DHCP server will send your modem a WAN IP address. A WAN IP address indicates that you have established a connection with your ISP. Routed IP allows you to connect to your ISP equipment without first having to identify yourself (authenticate) with your ISP. Once your modem has obtained a WAN IP address, you do not need to configure any additional settings

Congratulations! You have completed the modem's Automatic WAN Protocol Detection process. Now, go to section 7.4, "Confirming Your Internet Connection," to confirm your Internet connection.

7.1.2 Connecting to the Internet via PPPoE Protocol

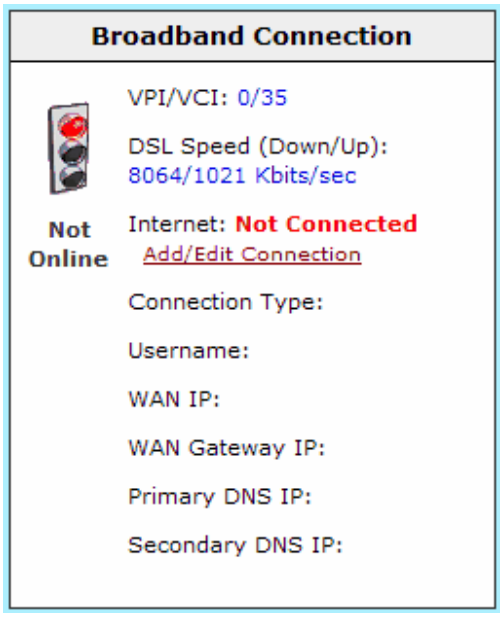
Some ISPs require that you identify yourself using PPP (Point-to-Point Protocol) authentication before obtaining an Internet connection. To connect to the Internet for the first time via PPP, go to one of the following sections:

- Section 7.2, "Configuring Your Internet Connection Using the Installation Wizard," for details on connecting to the Internet using the modem's built-in Installation Wizard. Use this method for simple, less-detailed configuration process.
- Section 7.3, "Configuring Your Internet Connection Manually," for details on connecting to the Internet using a manually set up connection. Use this method for a more detailed configuration process.

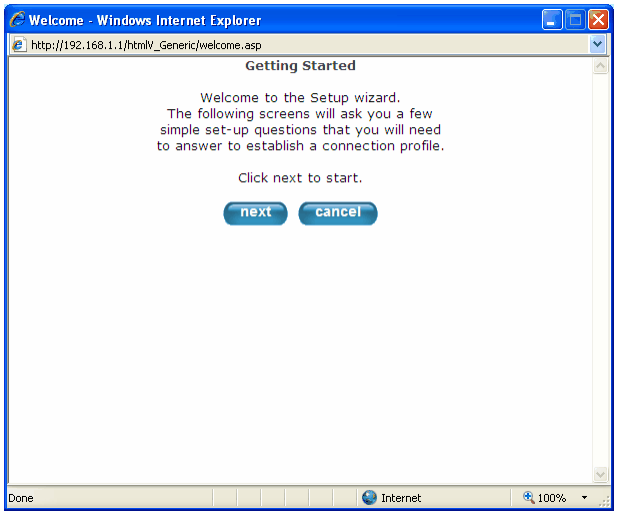
7.2 Configuring Your Internet Connection Using the Installation Wizard

To connect to the Internet using the modem's built-in Installation Wizard, please follow these steps:

1. Click the **Add/Edit Connection** link in the **Broadband Connection** panel of the **Home** screen. The **Getting Started** window will appear.

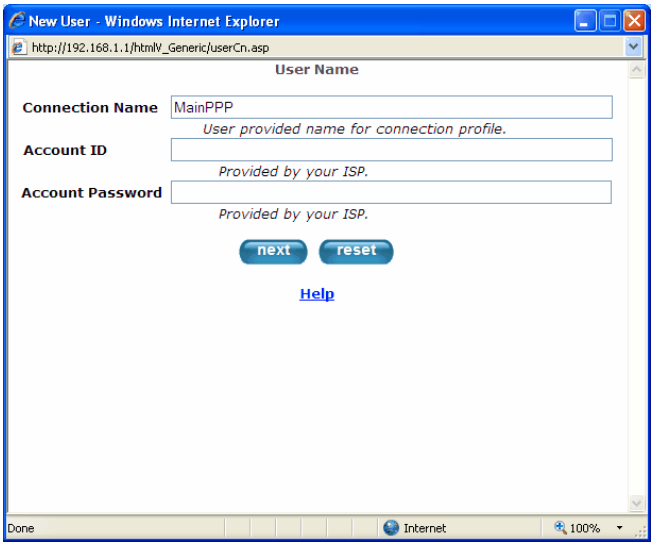


2. Click **next**. The **User Name** window will appear, requesting information that will allow the modem to make a connection to your ISP. This information is stored in your modem.

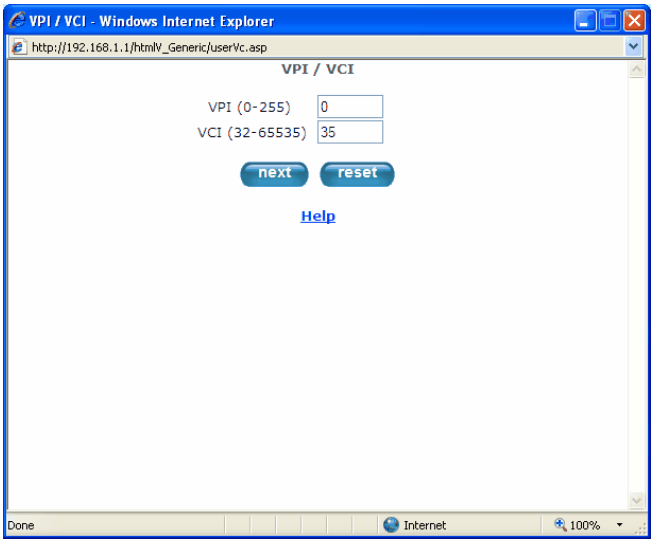


3. Type in the following information in the fields provided:

- Connection Name: This is a description of the default connection profile that your modem will use. You may use the default or assign a new description.
- Account ID: This is supplied by your ISP. This is a text string which uniquely identifies you with your ISP.
- Account Password: This is supplied by your ISP. This is a key phrase or text string that verifies your identity to the ISP.



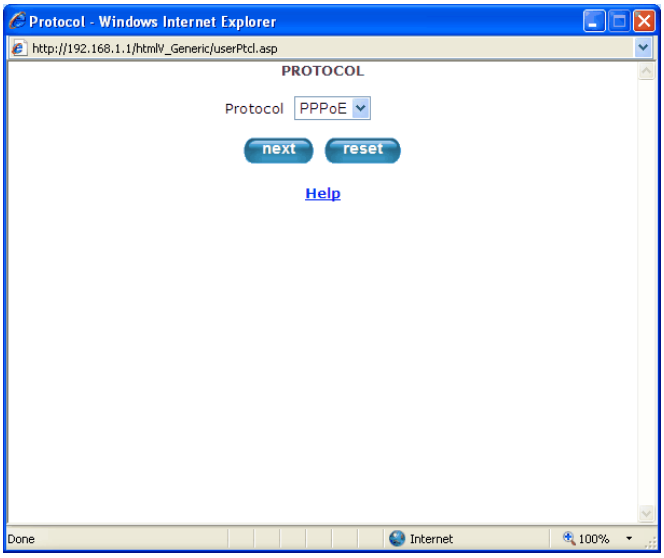
4. Click **next**. The **VPI/VCI** window will appear, requesting information that will allow the modem to establish a communications channel to the ISP.



5. Type in the following information in the fields provided:

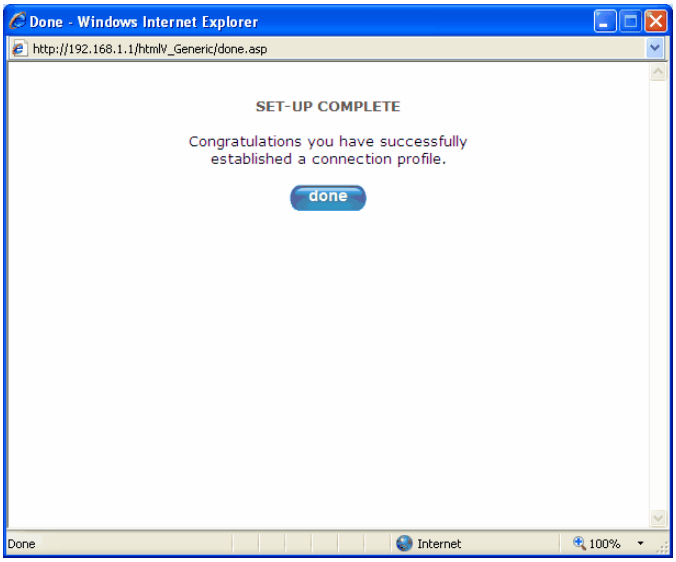
   - VPI (0-255): This is Virtual Path Indicator. This value is supplied by your ISP.
   - VCI (32-65535): This is the Virtual Channel Indicator. This value is supplied by your ISP.

6. Click **next**. The **PROTOCOL** window appears, requesting a networking protocol to use when communicating with the ISP.

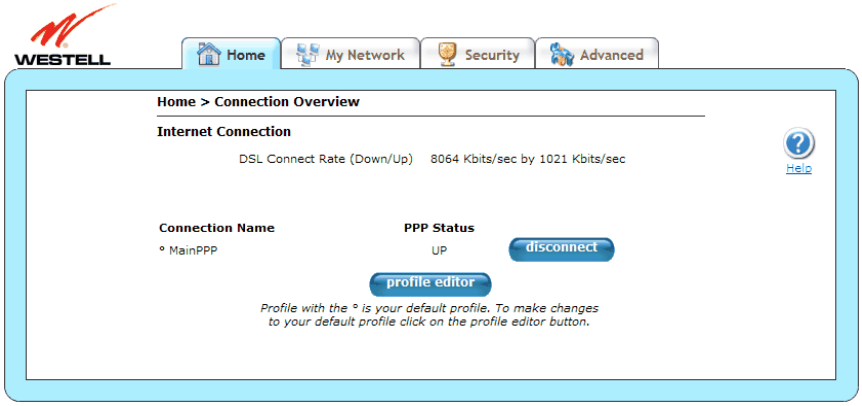


7. Click the drop-down menu to select a protocol: **PPPoA**, **PPoE**, or **Bridge**. This information is provided by your ISP.

8. Click the **next** button. The **SET-UP COMPLETE** window will appear, signifying that you have successfully established a connection profile.



9. Click the **done** button. The **Connection Overview** screen appears. The Installation Wizard is now done.



10. Click **Home** in the main menu to exit the process completely.

Congratulations! You have completed configuring your Internet connection using the Installation Wizard. Now, go to section 7.4, “Confirming Your Internet Connection,” to confirm your Internet connection.

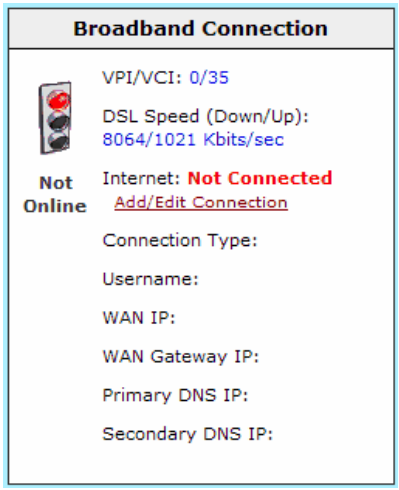
7.3 Configuring Your Internet Connection Manually

Your modem allows you to set up connection profiles for PPP authentication with your ISP. A connection profile contains your account ID and password (provided by your ISP), and several connection options that you can specify for your profile. The account ID and password are used for each connection profile that you set up. Connection profiles can be associated with specific service settings, such as firewall settings or NAT services, enabling you to customize your modem for specific users.

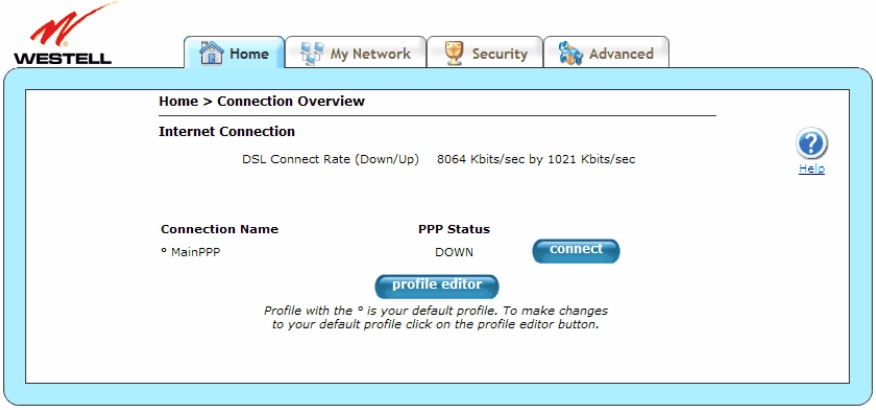
IMPORTANT: Before setting up a connection profile, confirm that you have an Account ID and Account Password from your ISP.

To connect to the Internet manually by setting up a PPPoE connection profile, please follow these steps:

1. Go to the **Home** page, and click the **Add/Edit Connection** link in the **Broadband Connection** to go to the **Connection Overview** screen. The **Connection Overview** screen displays the status of your Internet connection. In the screen below, the status displays **DOWN.** This means that you do not have an Internet connection.

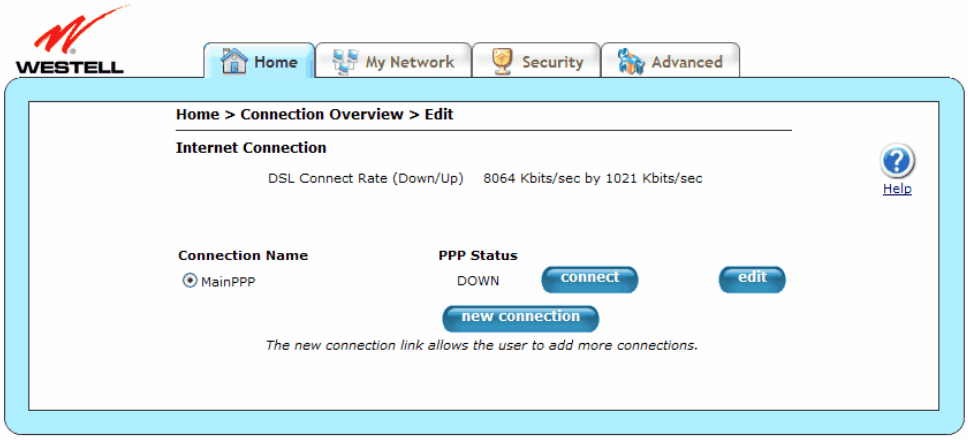


2. Click **profile editor** to set up your connection profile. The **Edit** screen (**Home > Connection Overview**) will appear.



3. Click **edit**. The **Edit Connection** window will appear. This window allows you to change the connection profile settings defined in the modem.

> **NOTE:** To create an entirely new connection profile, rather than edit an existing one, click **new connection** instead of **edit**.



4. Type in the following information in the fields provided and select from the following options:

- Connection Name: This is description for the connection profile that your modem will use. This name is supplied by your ISP.
- Account ID: This is your account ID. This ID is supplied by your ISP.
- Account Password: This is your account's password. This password is provided by your ISP.
- Service Profile: This drop-down menu lists pre-defined Service Profiles.
- Manual/On Demand/Always On: These are options for specifying how this particular connection profile is used.
- Time Out Enable: This check box enables/disables an automatic modem inactivity timeout.
- Save Password: This check box to enables/disables automatic password entry.
- Minutes for Connection Time Out: This is the number of minutes specified before the Time Out Enable feature disconnects the modem from the ISP.

Refer to the following table for detailed information on each of the Edit/New Connection window fields.

Connection Name	Displays the description for the connection profile that your modem will use. This field allows you to type in the desired name that you want to use for each profile that you set up. You can create and store up to eight unique connection profiles in your modem, which you can use once you establish a PPP session with your ISP. This field allows a maximum of 64 characters. Remember, use MainPPP as the connection name if you are connecting for the first time. Note: When you establish a PPPoE session for the first time, you must use the factory default Connection Name "MainPPP" to connect to your ISP. Then, if you want set up additional profiles, you can use connection names of your choice. The Connection Name is the name associated each connection profile.
Account ID	Displays your Account ID as supplied by your ISP. The Account ID field allows a maximum of 255 characters.
Account Password	Displays your Account Password as provided by your ISP. The Account Password is masked for extra security. This field allows a maximum of 255 characters.
Service Profile	Click this drop-down menu to select a pre-defined Service Profile. A service profile is a collection of settings for the built-in firewall and NAT. These settings control which applications are enabled to communicate through the modem. This selection specifies which service profile is used with this connection.
Manual/On Demand/Always On	Select the option to specify how this connection profile is used. By default, the modem's connection setting is set to **Always On**. • Manual: Select this option to manually establish your PPP session. • On Demand: Select this option to automatically reestablish your PPP session on demand anytime your PC requests Internet activity (for example, browsing the Internet, email, etc.). Please note that when you have Internet traffic, this setting may cause a delay. • Always On: Select this option to automatically establish a PPP session when you log on or if the PPP session goes down.
Time Out Enable	Click this check box to enable disconnect timeout. If enabled, the modem will monitor the ISP connection for activity. If there is no activity for the time out period, the modem will disconnect from the ISP. Note: The timeout option will be dimmed if you select **Always On** as your connection setting.
Save Password	Click this check box to enable automatic password entry. If enabled, the modem will automatically insert your Account Password. By default, this feature is enabled (checked).
Minutes for Connection Time Out	Displays the number of minutes of inactivity before your modem will disconnect from the ISP.

5. Click **save** and then **OK** to save the connection settings.

Congratulations! You have completed setting up your PPPoE connection profile. Now, go to section 7.4, "Confirming Your Internet Connection," to confirm your Internet connection.

7.4 Confirming Your Internet Connection

If you clicked the **Save** button in the **Edit** or **New Connection** window, the following screen will appear.

Click the **Connect** button, and wait a brief moment while the modem connects to the Internet. The **Status** field will display UP once an Internet connection has been established.

NOTE: If your modem's connection setting is set to Always On or On Demand, after a brief delay, the Internet connection will be established automatically; however, if the connection setting is set to Manual, you must click the **Connect** button in the **Connection** screen to establish an Internet connection.

Additional ways to confirm your Internet connection are:

- In the **Broadband Connection** panel of the **Home** page, view the **Internet** field. If the status reads **Not Connected**, you do not have a DSL link. However, if the **Internet** field displays **Connected** and the **Speed (Down/Up)** field displays numeric values, a DSL link has been established. The values displayed represent the transmission rates of your DSL signal (downstream and upstream). You may need to wait a brief moment for the modem to report these values.
- At the top of the modem, check to see if the **DSL** LED is solid green. Solid green indicates that the modem's DSL connection has been established. (The **DSL** LED may flash while the connection is being established.) Please wait a brief moment for the modem to connect.

If you do not have a DSL sync, first check your physical connections. (Refer to section 5, “Hardware Installations,” if needed.) If the problem persists, contact your ISP for further instructions.

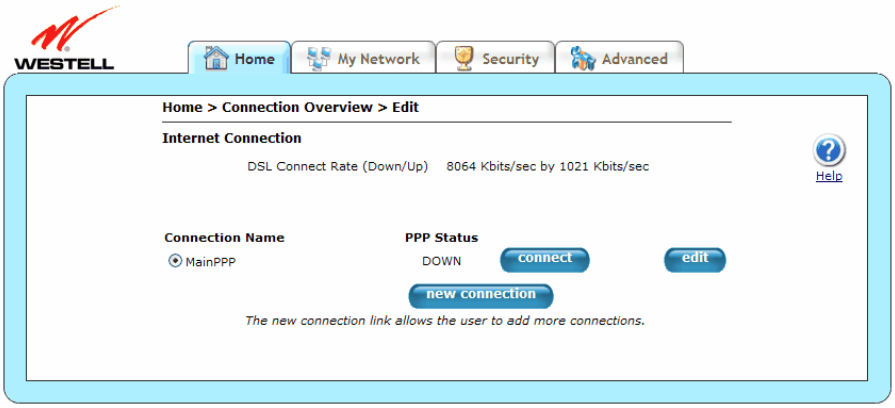
Congratulations! You have established an Internet connection. You can now **Go!** browse the Internet. For example, to visit Westell’s home page, type **http://www.westell.com** in your Internet browser’s address bar, and then press **Enter** on your keyboard.

7.5 Disconnecting from an Internet Session

If you have finished browsing the Internet and want to disconnect from your ISP, click the **Add/Edit Connection** link from the **Broadband Connection** panel. The following **Home > Connection Overview** screen will appear. Click **disconnect** and then **OK**.

IMPORTANT: If you disconnect the PPP session, this will disconnect the modem from the Internet, and Internet access for all users connected to the modem will be down until the PPP session is re-established.

If you clicked the **disconnect** button in the **Home > Connection Overview** screen, after a brief moment, **PPP Status** should display DOWN. This means that you no longer have a PPP session. However, your DSL session will not be affected. When you are ready to end your DSL session, simply unplug the modem from its power source.



When you are ready to establish a PPP session again, click the **connect** button in the **Home > Connection Overview** screen. If you have previously unplugged the modem, first plug in the modem, and then log on to your account profile to establish a PPP session.

NOTE: When you are ready to exit the modem's interface, click on the **X** (close) in the upper-right corner of the browser window. This will not affect your PPP Status; i.e., your PPP session will not be disconnected. You must click the **disconnect** button to disconnect your PPP session. To restore this interface, open your Internet browser window, type **http://192.168.1.1/** in the browser's address bar, and then press **Enter** on your keyboard. Type your **User name** and **Password** in the pop-up screen as needed.

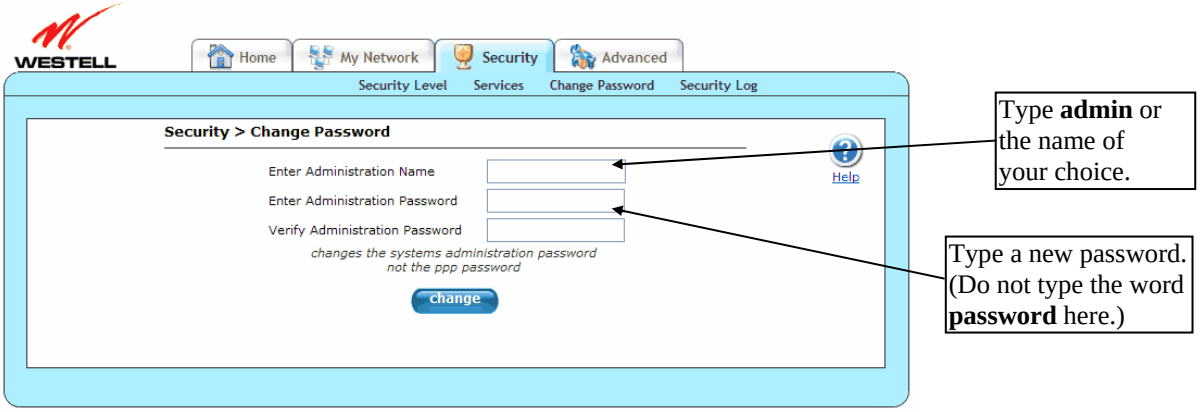
7.6 Changing the Administration Password

It is recommended that you change the administration password of your modem after completing initial installation and setup. You can accomplish this through the **Change Password** screen (**Security > Change Password**). This screen allows you to change the default administration name and password to values of your choice.

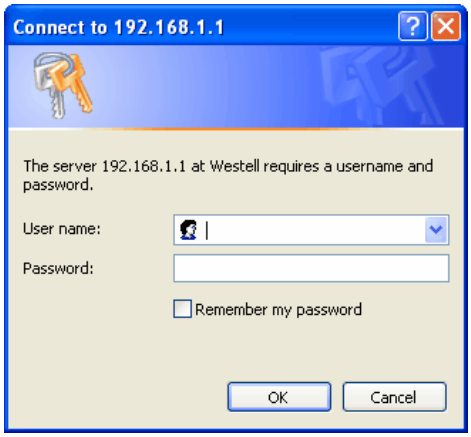
IMPORTANT:

1. The **Security > Change Password** screen allows you to use **admin** as your **administrator name** (your administrator name can match your user name). However, you may not use **password** as your **administrator password**. The values in these fields are case sensitive. Once you decide on an administrator name and password, please record them for future reference.
2. This feature changes the Administrator's password, not the PPP password.

Type your **Administration Name** and your **Administration Password** in the fields provided, and then click **change** and **OK.** The password fields will be masked for security purposes.



If you clicked **OK** after clicking **change**, the following screen will appear. Type in your new **User name** and **Password** in the fields provided, and then click **OK**.



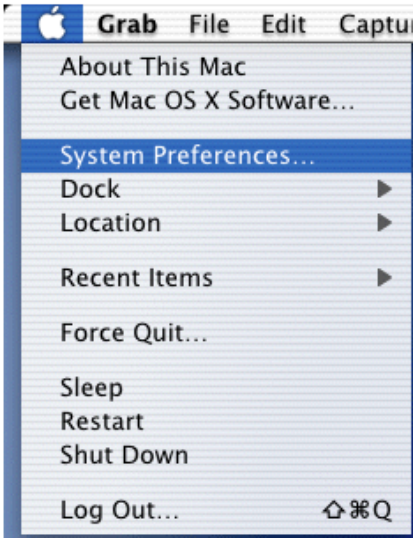
8. SETTING UP MACINTOSH OS X

This section provides instructions on how to use Macintosh Operating System 10 with the modem. Follow the instructions in this section to create a new network configuration for Macintosh OS X.

NOTE: Macintosh computers must use the modem's Ethernet installation. Refer to section 5, "Hardware Installations," for details.

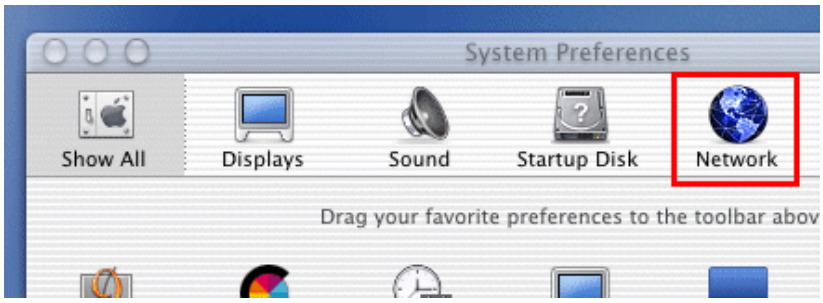
8.1 Opening the System Preference Screen

After you have connected the modem to the Ethernet port of your Macintosh, the screen below will appear. Click the **Apple** icon in the upper-left corner of the screen, and select **System Preferences**.



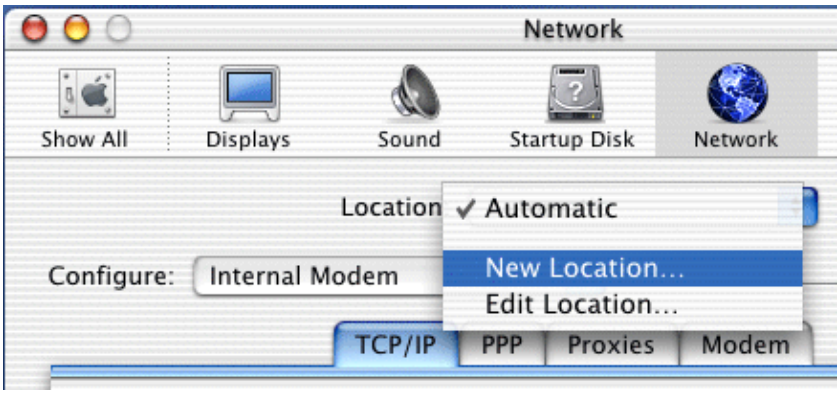
8.2 Choosing the Network Preferences

After selecting **System Preferences** from the previous screen, the following screen will appear. Click the **Network** icon.



8.3 Creating a New Location

After clicking the **Network** icon, the following screen will appear. Select **New Location** from the **Location** field.



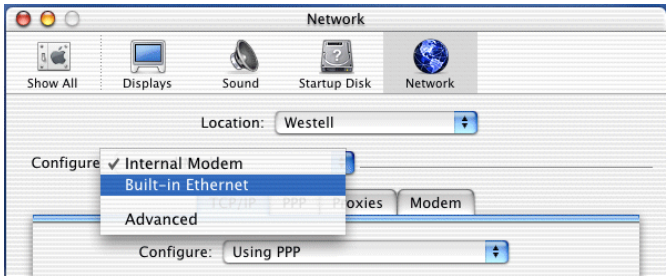
8.4 Naming the New Location

After selecting **New Location** in the **Network** screen, the following screen will appear. In the field labeled **Name your new location:**, change the text from **Untitled** to **Westell**. Click **OK**.

8.5 Selecting the Ethernet Configuration

After clicking **OK** in the **Name your new location:** screen, the **Network** screen will appear. The **Network** screen displays the settings for the newly created location. From the **Configure** field in the **Network** screen, select **Built-in Ethernet**. Click **Save** to save the settings.

NOTE: Default settings for the Built-in Ethernet configuration are sufficient to operate the modem.



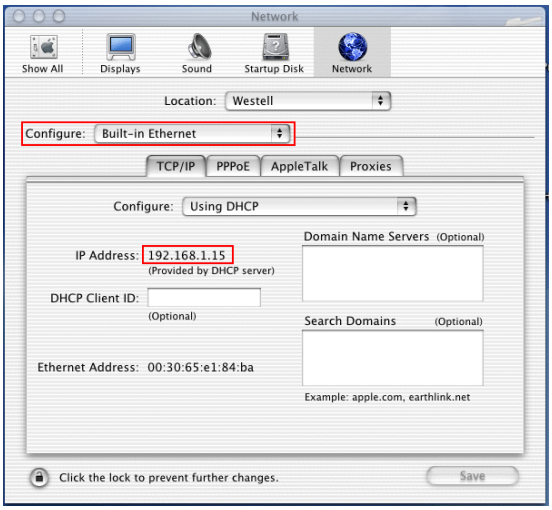
8.6 Checking the IP Connection

To verify that the computer is communicating with the modem, please follow these steps:

1. Go to the **Apple** icon in the upper-left corner of the screen, and select **System Preferences**.
2. In the **System Preferences** screen, click the **Network** icon. The **Network** screen will appear.
3. In the **Configure** field in the **Network** screen, select **Built-in Ethernet**.
4. View the **IP address** field. An IP address that begins with **192.168.1** should appear.

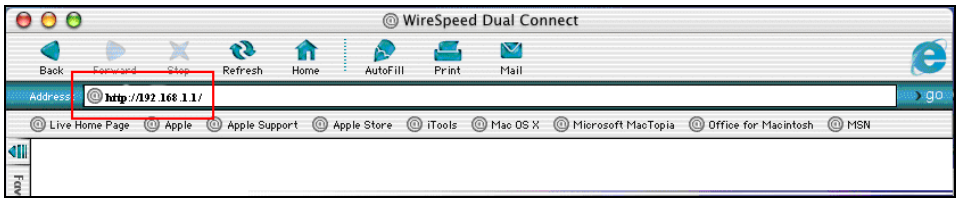
Congratulations! You have successfully verified communication between the computer and modem. Now, go to section 8.7, "Accessing Your Modem," to access your modem's Web pages.

NOTE: The modem's DHCP server provides this IP address. If this IP address is not displayed, check the modem's wiring connection to the PC. If necessary, refer to section 5, "Hardware Installations," for instructions.



8.7 Accessing Your Modem

In your Internet Explorer Web browser address bar, type **http://192.168.1.1/**. Next, press **Enter** on your keyboard.



The **Modem Secure** screen will appear. Go to the **Modem Secure** screen in section 7.1, “Logging on to Your ,” for logon instructions.

9. BASIC CONFIGURATION

IMPORTANT: The following sections assume that you have active DSL and Internet service.

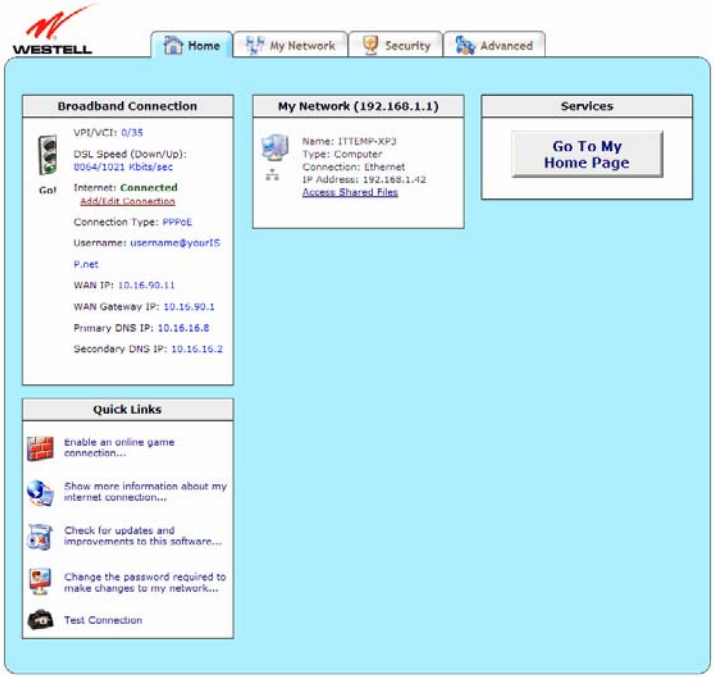
Your modem allows you to make changes to the configurable features of your modem, such as account profiles, network configurations, and security settings. The following sections explain each feature and show you how to make changes to the modem's settings. The main menu, displayed at the top of each page, allows you to navigate to the various configuration screens of your modem. Whenever you change the configurable settings of your modem, you must click **save** (or **apply** where applicable) to allow the changes to take effect in the modem.

To configure the settings in your modem, follow the instructions provided in sections 10 through 13.

10. HOME

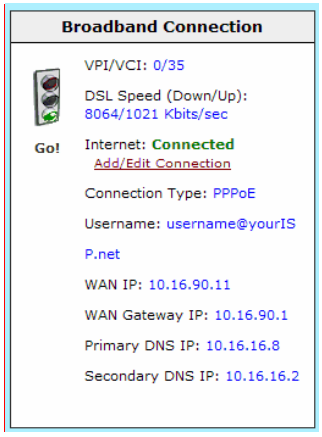
This section explains the initial screen of your modem and guides you through the configurable settings.

After you have logged on to your modem and established a PPP session with your Internet service provider (ISP), click **Home** in the top navigational menu (also referred to as the "main menu"), and the following screen will appear. The **Home** screen allows you to view connection information reported by your modem and to quickly access Internet services provided by your ISP. The following sections discuss each panel in the **Home** screen.



10.1 Broadband Connection Panel

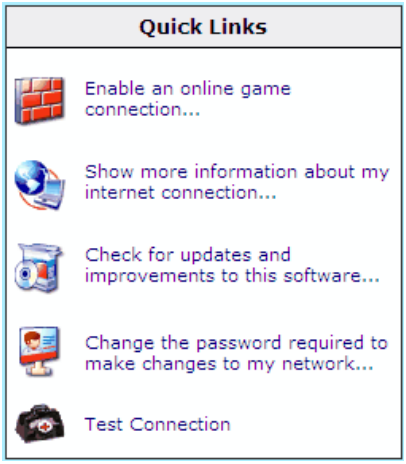
The **Broadband Connection** panel of the **Home** screen allows you to view details about your modem's connections. By clicking the **Add/Edit Internet Connection** link, you can access the screens that allow you to set up new account profiles, edit existing account profiles, and connect or disconnect from your ISP. After you have connected to your ISP, this panel will display the connection details. Additional information about your modem's broadband connection can be found in section 7, "Accessing Your Modem."



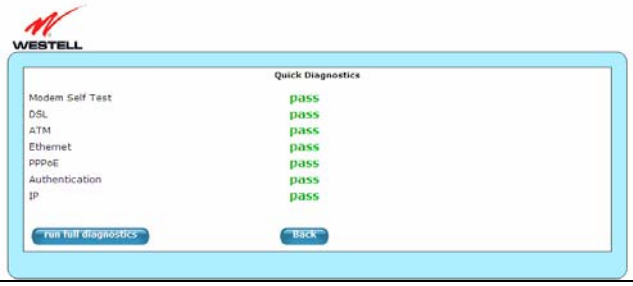
VPI/VCI	Displays VPI (Virtual Path Indicator) value and VCI (Virtual Channel Indicator) for a particular VC, which is defined by your ISP.
DSL Speed (Down/Up)	Displays the transmission rates (in Kbits/sec) of your DSL signal. **Down** is the rate at which data is transmitted downstream (from the Internet to your computer). **Up** is the rate at which data is transmitted upstream (from your computer to the Internet).
Internet	Displays status of your Internet connection: Connected or Not Connected.
Add/Edit Connection	Click this link to open the **Home > Connection Overview** screen, which provides a quick summary of your modem's Internet connection settings. Refer to section 7, "Accessing Your Modem."
Connection Type	Displays the protocol used for your Internet connection, which is provided by your ISP.
Username	Displays the username that you used to connect to your ISP. The username and password are provided by your ISP.
WAN IP	Displays a WAN IP address that has been assigned to your modem by your ISP. You will receive a WAN IP address only after your modem has established an Internet connection with your ISP. (The IP address "192.168.1.1" is your modem's LAN IP address, which is assigned to your modem by factory default.)
WAN Gateway IP	Displays the WAN IP address of the "upstream" connection point.
Primary DNS IP	Displays primary DNS IP provided by your ISP.
Secondary DNS IP	Displays secondary DNS IP provided by your ISP.

10.2 Quick Links Panel

The **Quick Links** panel of the **Home** screen allows you to quickly access certain features of your modem by clicking on the icon.

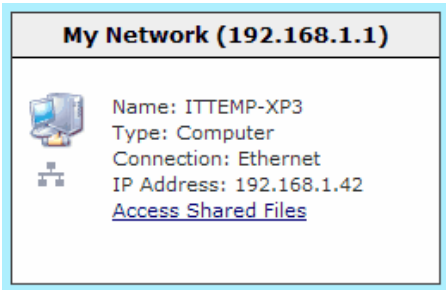


Enable an online game connection…	Click this link to set up a service profile and attach VPN, Gaming, or other NAT services to the profile. Refer to 12.2.2, "Port Forwarding" for additional information.
Show more information about my Internet connection…	Click this link to display a summary your modem's network statistics. Refer to section 13.2.3.1, "Summary," for additional information.
Check for updates and improvements for this software…	Click this link to update your modem's software, if available. Refer to section 13.2.8, "Update Device," for additional information.
Change the password required to make changes to my network…	Click this link to change your administrator password. Refer to section 12.3, "Change Password," for additional information.

Test Connection…	Click this link to test your modem's connection and run diagnostics as shown in the following screen. 

10.3 My Network Panel

The **My Network** panel of the **Home** screen allows you to view information about devices that are connected to your network.

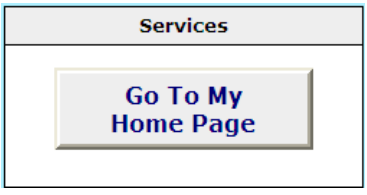


Name	Displays the ASCII (text) name of the device connected to the network
Type	Displays the type of device connected to your network.
Connection	Displays the physical connection used to interface with your modem.
IP Address	Displays the IP address assigned to your computer by your modem's DHCP server.
Access Shared Files	Click this link to access shared files from a device on your local network. (The device must have file sharing enabled.) Note: If the device has a firewall turned on, you will not be able to access shared files from the device.

10.4 Services Panel

The **Services** panel of the **Home** screen allows you to access features and services provided by your ISP.

NOTE: The links displayed in the **Services** panel will only be available after you have established a PPP session with your ISP and are specific to the services offered by your ISP.

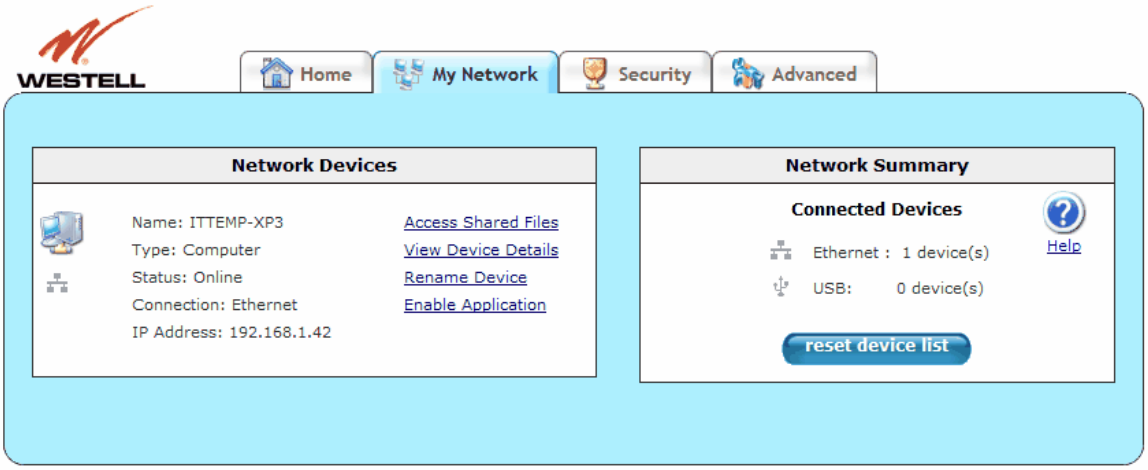


Go To My Home Page	Click this button to go to the default page of your Web browser; however, if your PPP session is down, you will not have Internet access. To browse the Internet, you must first establish a PPP session with your ISP. When you are ready to return to the modem's Web interface, type **http://192.168.1.1/** in your Internet browser's address bar, and press **Enter** on your keyboard.

11. MY NETWORK

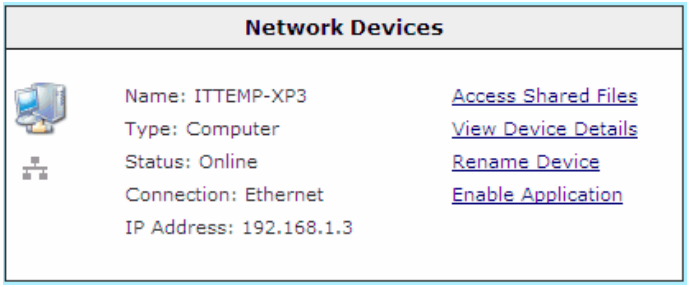
This section explains the network settings of your modem's local area network (LAN) and guides you through the configurable settings.

The following screen will appear if you select **My Network** from the main menu. This screen displays information about the devices connected to your local area network (LAN).

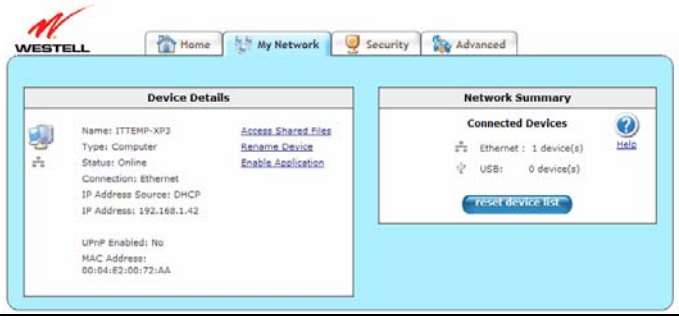
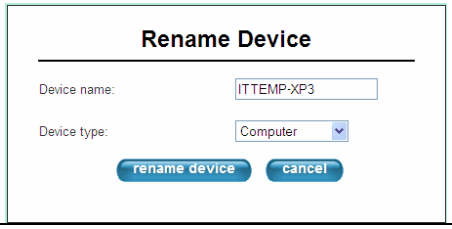
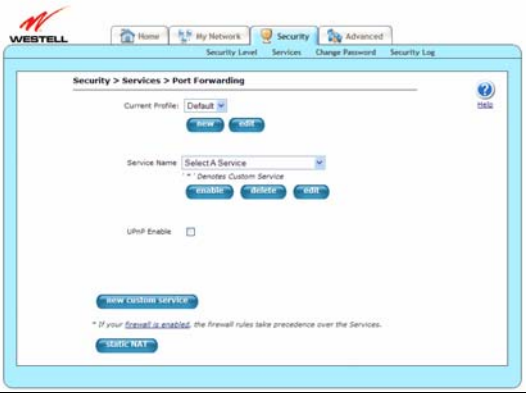


11.1 Network Devices

The **Network Devices** panel of the **My Network** screen displays details for each device connected to your LAN.



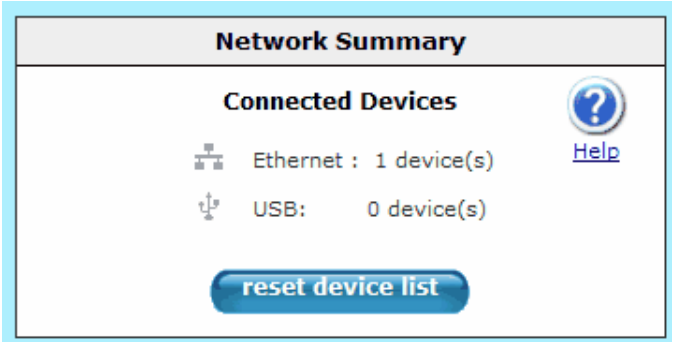
Name	Displays the ASCII (text) name of the device connected to the network
Type	Displays the type of device connected to your network.
Status	Displays the connection status for the device.
Connection	Displays the physical connection used to interface with your modem.
IP Address	Displays the IP address assigned to your computer by your modem's DHCP server.
Access Shared Files	Click this link to access shared files from a device on your local network. (The device must have file sharing enabled.) Note: If the device has a firewall turned on, you will not be able to access shared files from the device.

View Device Details	Click this link to view information about devices connected to your LAN as shown in the following screen. 
Rename Device	Click this link to change the names of devices connected to your LAN. In the following **Rename Device** screen, type the desired name in the **Device Name** field, and then select an option from the **Device type** drop-down menu. Click the **rename device** button to allow the changes to take affect; or click **cancel** to return to the **Device Details** screen. 
Enable Application	Click this link to set up applications for your service profile, such as port forwarding and port triggering services as shown in the following screen. This feature enables applications (Games, Webcams, IM, and others) by opening a tunnel between remote (Internet) computers and a specific device port inside your LAN. Refer to section 12.2.2, “Port Forwarding,” for additional information on this screen. 

11.2 Network Summary

The **Network Summary** panel of the **My Network** screen displays the number of Ethernet and USB devices connected to your LAN.

IMPORTANT: If you have PCs on your network that are not being displayed, check the firewall setting on the PCs to ensure that the firewall is disabled.



Connected Devices	Displays the interfaces that can be used to connect to your modem. Note: If you have computers on your network that are not being displayed, check the firewall setting on the PCs to ensure that the firewall is disabled.
Ethernet	Displys the number of devices that are connected to the modem via Ethernet 10/100 Base-T connection.
USB	Displys the number of devices that are connected to the modem via USB connection.
reset device list	Click this button to update the list of connected devices if, for example, devices have been recently added or removed and you want to update the list.

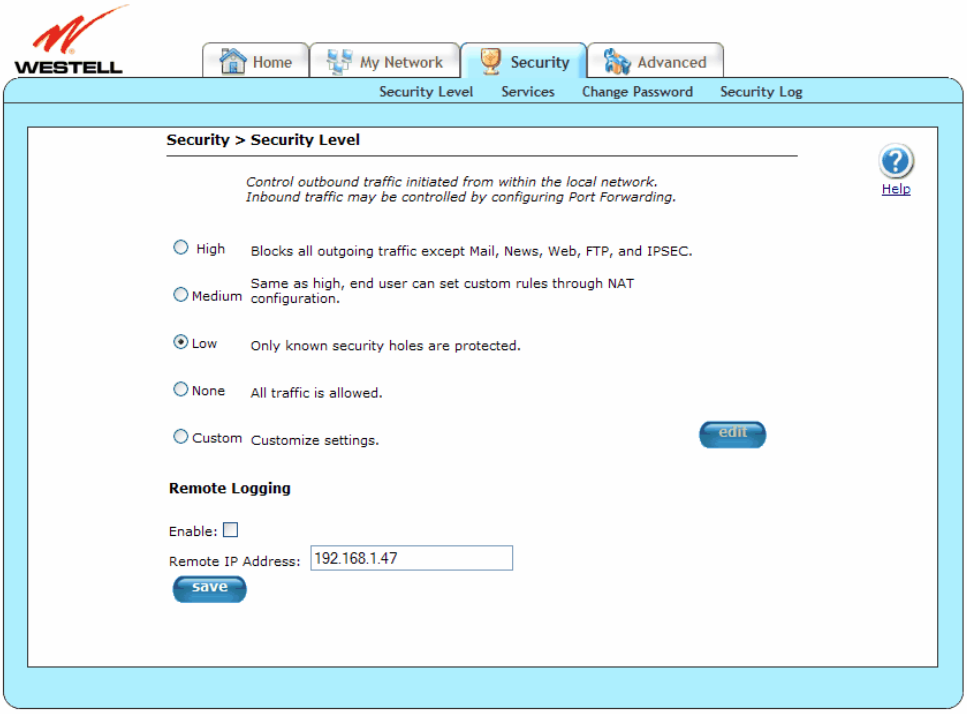
12. SECURITY

This section explains the security features of your modem and guides you through the configurable settings.

12.1 Security Level

The following screen will appear if you select **Security > Security Level** from the main menu. This screen allows you to change your firewall security levels by selecting from the available options. If you change the settings in this screen, click **save** and then **OK**. If you click **Cancel**, the screen will return to its previous settings.

IMPORTANT: It is recommended that you do not change the settings in the **Custom Rules** screen. If you need to reset your modem to factory default settings, follow the instructions in section 13.2.1, "Backup/Restore," to restore the modem to default settings.



Security Level	Select these options to control outbound traffic initiated within the local network. By default, the Security Level is set to None. Note: Only the most advanced users should select the **Custom** option. • High: Select this option to allow only basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. All other traffic is prohibited. • Medium: Select this option to allow only basic Internet functionality by default; however, Medium security allows customization through NAT configuration so that you can enable the traffic that you want to pass. • Low: Select this option to allow all traffic except for known attacks. With Low security, your modem is visible to other computers on the Internet. • None: Select this option to disable security and allow all traffic. (All traffic is passed.)

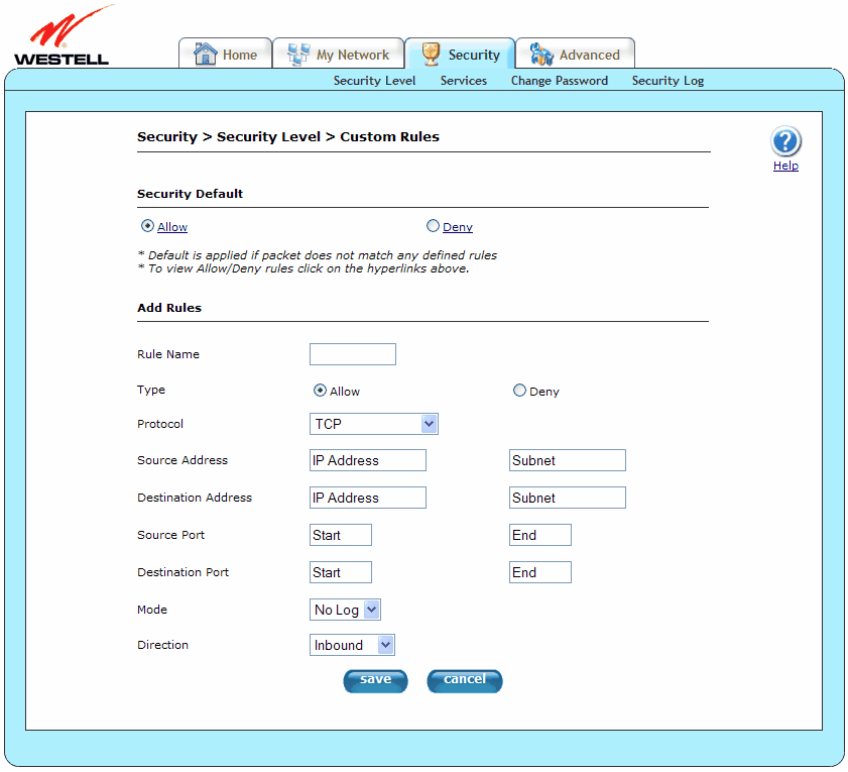
	• Custom: Select this option to edit the firewall configuration directly. When Custom is selected, the **edit** button will be clickable. Clicking **edit** will open the **Custom Rules** screen, which allows for user customization of modem security settings.
Remote Logging Note: The syslog server must be configured to listen on udp port 514, which is usually the default port. In order for the logs to be saved to the syslog server, the server should be configured to save the logs to a file. Some of the free syslog servers available on the Internet are kiwisyslog, MT_syslog and 3Csyslog.	
Enable	Click this check box to enable the modem to send firewall logs to a syslog server. By default, remote logging is disabled (unchecked).
Remote IP Address	Displays the IP address of the syslog server machine to which the diagnostics logs to be sent.

12.1.1 Custom Rules

The following screen will appear if you select **Custom** and then **OK** from the **Security Level** screen and click the **edit** button (**Security > Security Level > Custom Rules**). The **Custom Rules** screen allows you to configure the security parameters on your Inbound and Outbound traffic. Inbound rules will restrict inbound traffic from the WAN to the LAN. Outbound rules will restrict outbound traffic from the LAN to WAN. If you change the settings in this screen, click **save**. If you click **cancel**, the screen will return to its previous settings.

IMPORTANT: Custom security is an advanced configuration option that allows you to edit the firewall configuration directly. Only expert users should attempt this. It is recommended that you do not change the settings in this screen. If you need to reset your modem to factory default settings, follow the instructions in section 13.2.1, "Backup/Restore," to restore the modem to default settings.

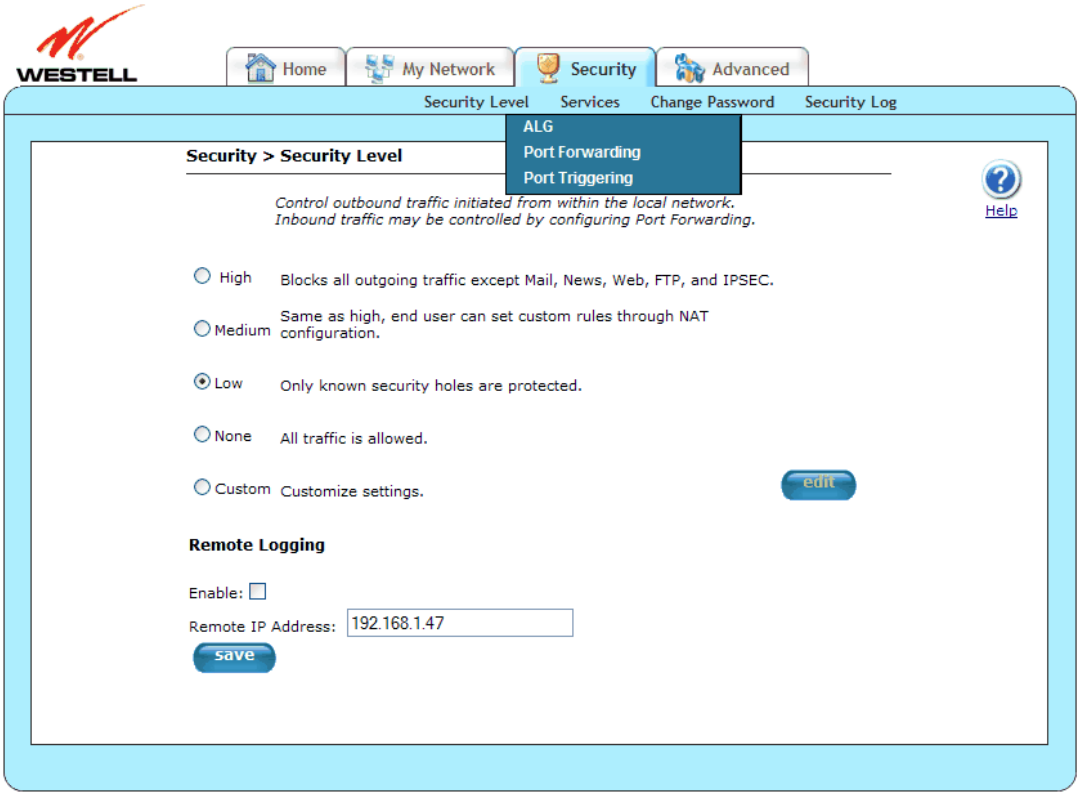
NOTE: The default security setting is applied if a packet does not match any defines rules. Clicking **Save** allows the firewall rules to be saved to flash (a temporary storage area in your modem).



Security Default	Select the option to allow or deny default action to be taken if no rule is found to match the given packet. • Allow: Allow the packet if no rule matches it. • Deny: Block the packet if no rule matches it.
Rule Name	Displays the name of the new rule.
Type	Select the option to allow or deny the packet matching this rule. • Allow: Allow the packet matching this rule. • Deny: Block the packet matching this rule.
Protocol	Click this drop-down menu to select the protocol for the new rule: TCP, UDP, Protocol Number, ICMP Type, or All.
Source Address	Displays the source address of the packet to check the rule against.
Destination Address	Displays the destination address of the packet to check the rule against.
Source Port	Displays the source port of the packet to check the rule against.
Destination Port	Displays the destination port of the packet to check the rule against.
Mode	Click this drop-down menu to specify whether or not packets need to be logged: Log or No Log.
Direction	Click this drop-down menu to select the traffic direction for which the rule is applied: Inbound, Outbound, or Both.

12.2 Security Services

This section discusses the **Security Services** screens (ALG, Port Forwarding, and Port Triggering) of your modem and guides you through the configurable settings.

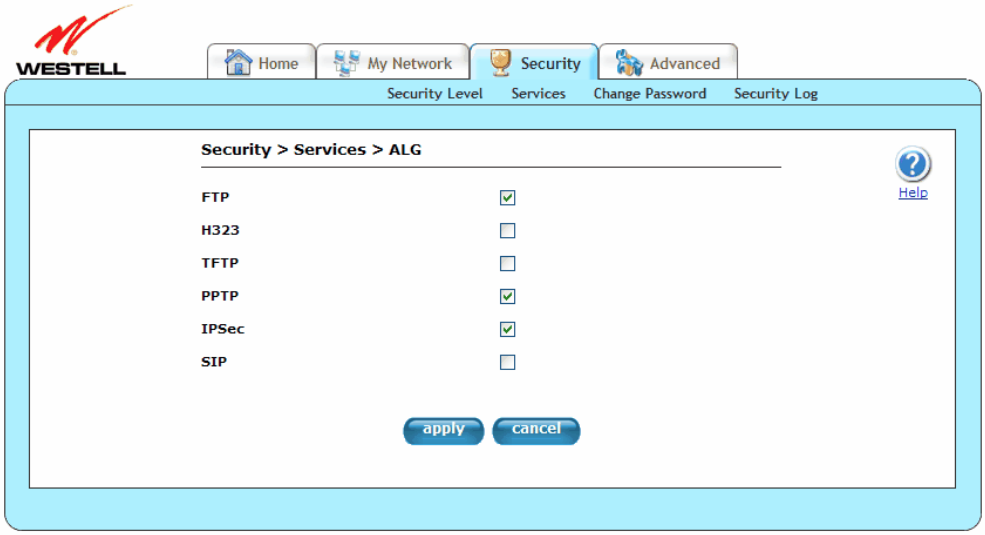


12.2.1 ALG

The following screen will appear if you select **Security > Services > ALG** from the main menu. This screen enables you to configure application-layer modem (ALG) services for your modem by clicking on the check box of each service that you want to enable (a check mark will appear in the box). If you change the settings in this screen, click **apply** and then **OK**. If you click **Cancel**, the screen will return to its previous settings.

Enabling an ALG service opens the IP ports associated with the corresponding service. For example, if you have an IPSec client running on a LAN-side PC attached to the modem, it is necessary to enable the IPSec ALG. Enabling IPSec opens the default ports used by IPSec, 500 and 1500, so that traffic to and from the IPSec client may pass through.

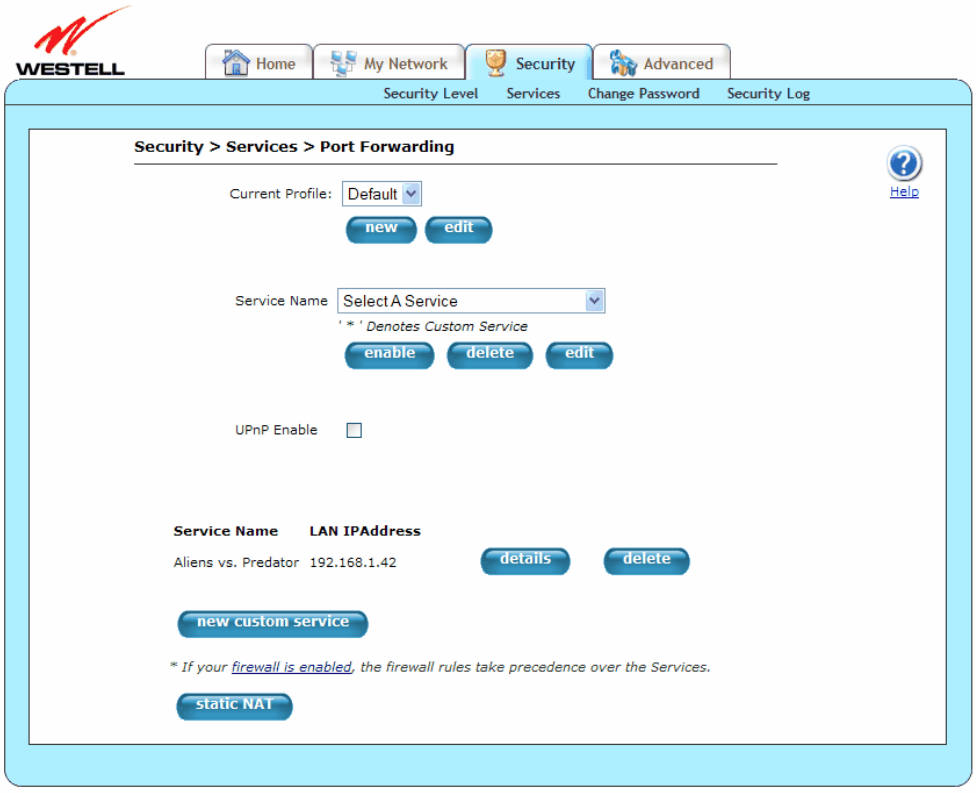
NOTE: When the firewall level is set to "High," some services may not be configurable.



FTP	Click this check box to enable the FTP ALG.
H323	Click this check box to enable the H323 ALG.
TFTP	Click this check box to enable the TFTP ALG.
PPTP	Click this check box to enable the PPTP ALG.
IPSec	Click this check box to enable the IPSec ALG.
SIP	Click this check box to enable the SIP ALG.

12.2.2 Port Forwarding

The following screen will appear if you select **Security > Services > Port Forwarding** from the main menu. This screen allows you to forward incoming traffic from the outside network to a range of WAN ports on an IP address on the LAN. You can also enable traffic from a local network (to a specified port range) to be allowed to go outside of the network in medium firewall settings. Displayed are currently active port forwarding services. You can add more pre-defined services (or create your own services) by selecting the appropriate entry in the **Service Name** drop-down menu.

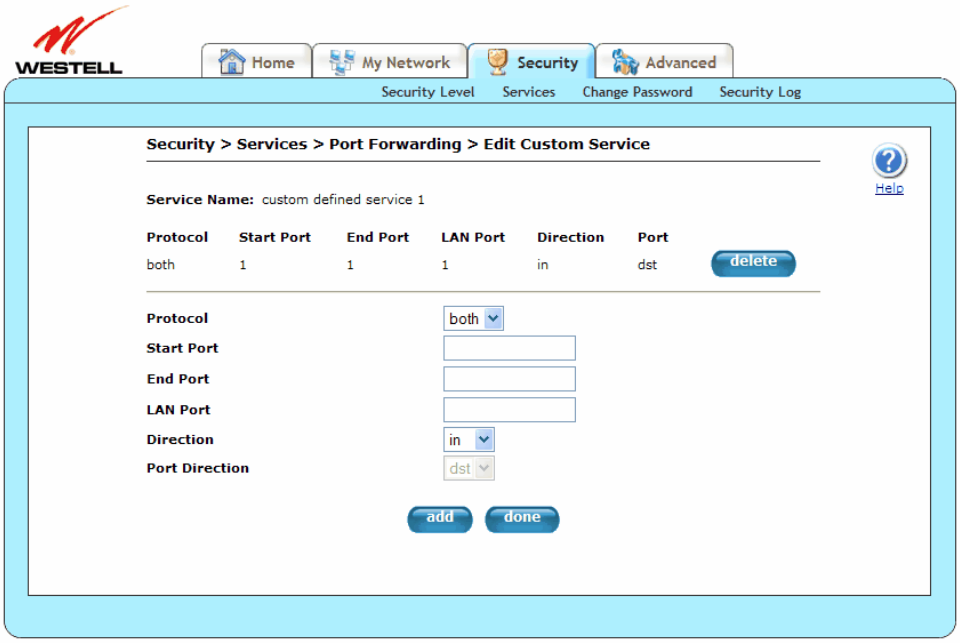


Current Profile	Click this drop-down menu to display the NAT (Network Address Translation) services available. All of the settings on this screen are associated with a Service Profile. The service profile is selected from the **Current Profile** drop-down menu. If no profile has been created, the settings chosen are applied to the default profile. The **Service Profile** drop-down menu located in the **Home > Connection Overview > Edit** screen (on the **Home** screen, click the **Add/Edit Connection** link) associates a service profile with one or more of your "Connection Profiles." This means different connections can allow different services to be associated with them. Use the **Current Profile** drop-down menu to select a profile to edit. However the profile will be activated from the **Home > Connection Overview > Edit** screen. • To create a new service profile, click the **new** button. • To remove a service profile, click the **delete** button (not available for the Default profile). • To change the name of a service profile, click the **edit** button.

Service Name	Click this drop-down menu to select the NAT (Network Address Translation) service for configuring your modem. **Service Name** lists all of the configured services available for the selected Service Profile. To enable a predefined or custom service, select it from the drop-down menu, and click the **enable** button. The **Enable PreDefined Service** window will open, showing a detailed description of that service and will step you through the process of enabling a service. The modem will then configure the port(s) to enable the service. Refer to section 12.2.2.2, "Enable PreDefined Service." • To delete the selected service from the **Service Name** listing, click the **delete** button. • To edit a Custom Defined Service, including allowing you to delete an existing rule from the service or add new rule to the service, click the **edit** button. Refer to section 12.2.2.1, "Edit Custom Service."
UPnP Enable	Click this check box to enable UPnP (Universal Plug and Play), allowing the modem to seamlessly connect and communicate with other UPnP-enabled devices, without the need for user configuration, centralized servers, or product-specific device drivers. When enabled, UPnP advertises the presence of your modem on the LAN. Click **OK** to restart the modem and save the changes. The modem will then configure itself to respond to UPnP messages. By default, **UPnP Enable** is disabled.
Service Name	Displays the Service Name of a previously enabled NAT service.
LAN IP Address	Displays the LAN IP Address of a previously enabled NAT service.
details	Click this button to open the **Service Details** screen (**Security > Services > Port Forwarding > Service Details**). This allows you to view details of the selected enabled port forwarding service.
delete	Click this button to delete an enabled NAT service.
new custom service	Click this button to open the **New Custom Service** screen (**Security > Services > Port Forwarding > New Custom Service**), which will step you through the process of creating a custom service entry.
Firewall is enabled	Click this link to open the **Security Level** screen (**Security > Security Level**), allowing you to modify your firewall settings as needed. Refer to section
Static NAT	Click this button to open the Static NAT pop-up window. Use this window to map a private IP address to a public IP address, where the public address is WAN IP address of the modem. This allows an internal host to have an unregistered (private) IP address and still be reachable over the Internet. • To enable a Static NAT device, click the drop-down menu to select a **Static NAT Device**, type the IP Address of the device that will function as the default NAT destination in the provided field, and click the **enable** button. • To disable a static NAT device, click the drop-down menu to select a **Static NAT Device**, and click the **disable** button. • Click **cancel** to return to the **Port Forwarding** screen without implementing any changes.

12.2.2.1 Edit Custom Service

The following screen will appear if you click the **edit** button after selecting a custom-defined service from the **Service Name** drop-down menu of the **Port Forwarding** screen (**Security > Services > Port Forwarding > Edit Custom Service**). This screen allows you to edit a custom-defined service selected from the **Port Forwarding Service Name** drop-down menu. If you change the settings in this screen, click **add** and then **done**.



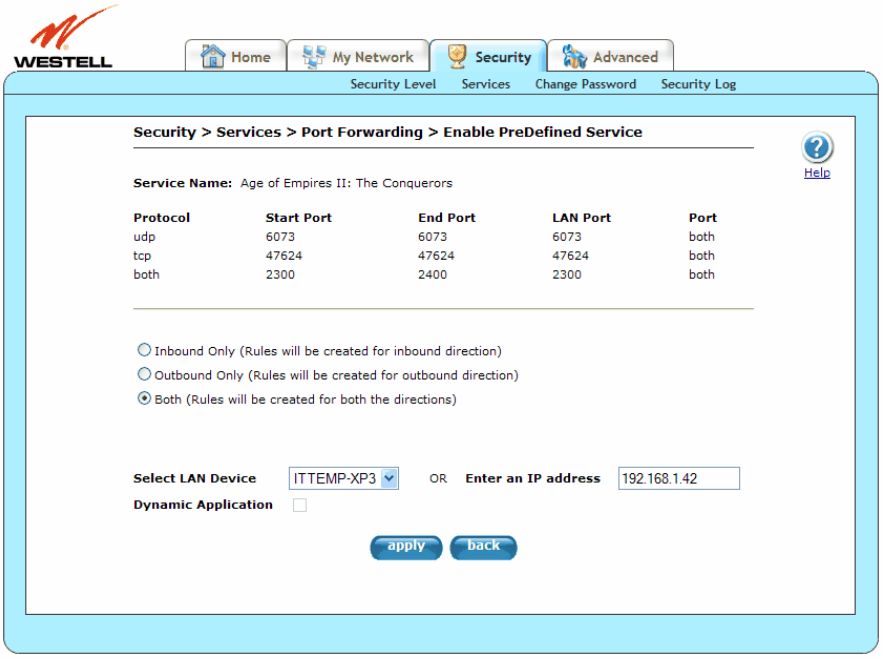
Service Name	Displays the name of the selected service.
Protocol	Displays the IP Protocol type. • TCP: Transmission Control Protocol. • UDP: User Datagram Protocol. • BOTH: Both Transmission Control Protocol and User Datagram Protocol.
Start Point	Displays the starting Port number for Incoming/Outgoing Packets.
End Point	Displays the ending Port number for Incoming/Outgoing Packets.
LAN Port	Displays the port number to map the Incoming WAN Packets to.
Direction	Displays the direction of the packet. • in: Incoming WAN packets. • out: Outgoing WAN packets. • BOTH: both incoming WAN packets and outgoing WAN packets.
Port	Displays the port that needs to be checked. • dst: Rule will be created for destination port. • src: Rule will be created for source port. • BOTH: Rule will be created for both the destination and source ports.
delete	Click this button to delete the currently selected rule from the custom service.
Protocol	Click this drop-down menu to select the IP Protocol type. • both: BOTH Transmission Control Protocol and User Datagram Protocol. • tcp: Transmission Control Protocol. • udp: User Datagram Protocol.

Start Port	Displays the start Port number for Incoming/Outgoing Packets.
End Port	Displays the end Port number for Incoming/Outgoing Packets.
LAN Port	Displays the Port number to map the Incoming WAN Packets to. This will not be required for outgoing packets.
Direction	Click this drop-down menu to select the direction of the packet. • in: Incoming WAN packets. • out: Outgoing WAN packets. • BOTH: both incoming WAN packets and outgoing WAN packets.
Port Direction	Click this drop-down menu to select the port that needs to be checked: • dst: Rule will be created for destination port. • src: Rule will be created for source port.
add	Click this button to create/add a rule to the custom service.
done	Click this button to return to the **Port Forwarding** screen.

12.2.2.2 Enable PreDefined Service

The following screen will appear if you click the **enable** button after selecting a service from the **Service Name** drop-down menu of the **Port Forwarding** screen (**Security > Services > Port Forwarding > Enable PreDefined Service**). This screen allows you to add predefined and custom-defined applications to your **Port Forwarding Service Name** drop-down menu. You can enable the selected service as a host service or a dynamic service. If you change the settings in this screen, click **apply** and then **OK**. If you click **back** or **Cancel**, the screen will return to its previous settings.

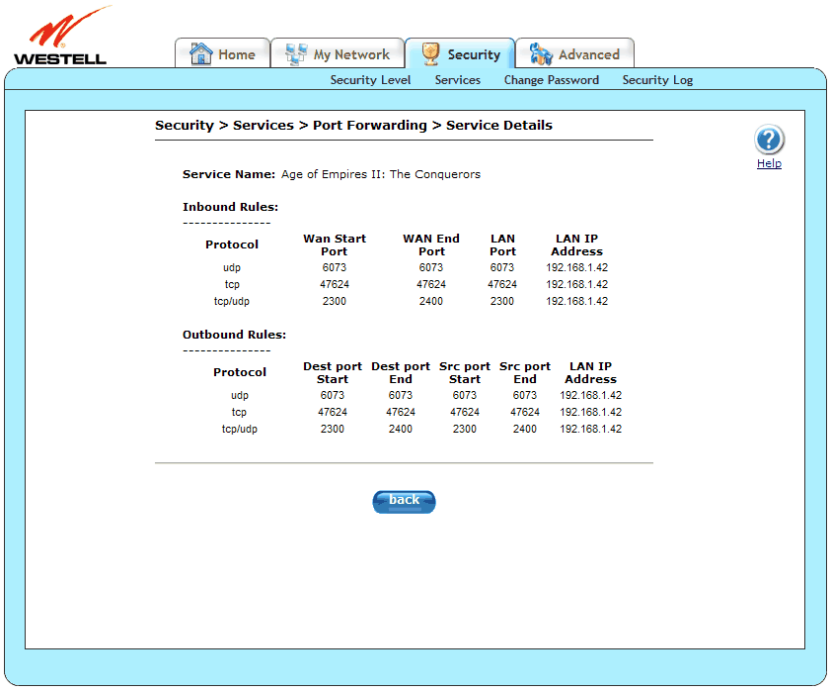
For host services, all the rules of the selected service are applicable only for the selected host connected to the modem. Dynamic service will enable all the rules in the service as dynamic rules; that is, rules are applicable for all devices connected to the modem. Traffic from the outside network coming to the modem needs to be directed to a particular host connected to the modem; therefore, any service that contains a rule for inbound traffic (such as having direction as “in”) cannot be enabled as a dynamic service. A predefined service can be enabled in any direction with the proper mode selected (host service or dynamic service). Dynamic application is not applicable for services having direction as “Inbound Only” or “Both.”



Service Name	Displays the name of the selected service.
Protocol	Displays the IP Protocol type. • TCP: Transmission Control Protocol. • UDP: User Datagram Protocol. • BOTH: Both Transmission Control Protocol and User Datagram Protocol.
Start Point	Displays the starting Port number for Incoming/Outgoing Packets.
End Point	Displays the ending Port number for Incoming/Outgoing Packets.
LAN Port	Displays the port number to map the Incoming WAN Packets to.
Port	Displays the port that needs to be checked. • Dst: Rule will be created for destination port. • Src: Rule will be created for source port. • BOTH: Rule will be created for both the destination and source ports.
Packet Direction	Select these options to set the direction for the rules in the predefined service. These options will only be shown for pre-defined services. • Inbound Only: All the rules of the service will be applicable for the incoming traffic from the outside network. • Outbound Only: All the rules of the service will be applicable for the outgoing traffic from the local network. • Both: All the rules of the service will be applicable for the incoming as well as outgoing traffic to and from the modem.
Select LAN Device OR Enter an IP address	Click this drop-down menu to select the IP Address of the LAN computer for this service; or, you can select the "name" of the computer from the drop-down menu. If you enable the **Dynamic Application** check box, then the IP Address field will be disabled and contain the IP address of 0.0.0.0.
Dynamic Application	Click this check box to enable Dynamic Application, which will only allow outgoing connections from any local PC. If the **Dynamic Application** check box is not checked, then the service will be applied as a host service.

12.2.2.3 Service Details

The following screen will appear if you click the **details** button for a **Service Name** on the **Port Forwarding** screen (**Security > Services > Port Forwarding > Service Details**). This screen displays the details of the selected enabled port forwarding service, including applied rules for the selected enabled service having direction as "in" (rules destined for incoming traffic from outside network).



Service Name	Displays the name of the selected service.
Inbound Rules Displays the applied rules for the selected enabled service having direction as "in" (rules destined for incoming traffic from outside network).	
Protocol	Displays the IP Protocol type. • TCP: Transmission Control Protocol. • UDP: User Datagram Protocol. • BOTH: Both Transmission Control Protocol and User Datagram Protocol.
Wan Start Point	Displays the starting Port number for incoming WAN packets.
Wan End Point	Displays the ending Port number for incoming WAN packets.
LAN Port	Displays the port number to map the incoming WAN packets to.
LAN IP Address	Displays the IP address of the LAN computer to map the packets to.
Outbound Rules Displays the applied rules for the selected enabled service having direction as "out" (rules destined for outgoing traffic from local network).	
Protocol	Displays the IP Protocol type. • TCP: Transmission Control Protocol. • UDP: User Datagram Protocol. • BOTH: Both Transmission Control Protocol and User Datagram Protocol.
Dest port Start	Displays the destination starting port number for outgoing packets.
Dest port End	Displays the destination ending port number for outgoing packets.
Src port Start	Displays the source starting port number for outgoing packets.

Src port End	Displays the source ending port number for outgoing packets.
LAN IP Address	Displays the IP address of the LAN computer to map the packets to.
back	Click this button to return to the **Port Forwarding** screen.

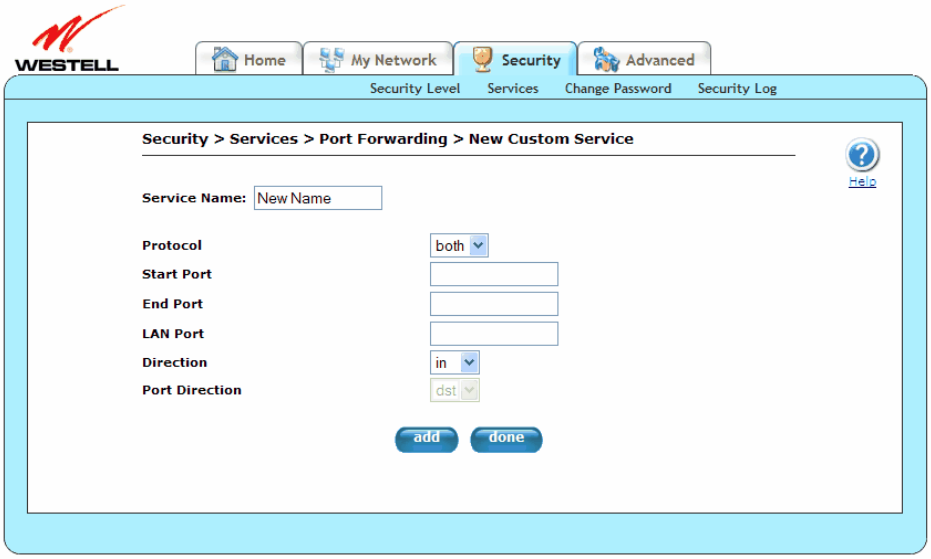
12.2.2.4 New Custom Service

The following screen will appear if you click the **new custom service** button from the **Port Forwarding** screen (**Security > Services > Port Forwarding > New Custom Service**). This screen allows you to add predefined and custom-defined applications to your **Port Forwarding Service Name** drop-down menu. You can enable the selected service as a host service or a dynamic service.

To create a service rule for outgoing traffic from the local network, select the desired protocol, and specify the port range from which you want to allow traffic in medium firewall settings, direction as out, and port direction as “dst” (if you want to check for destination port in outgoing traffic) or “src” (if you want to check for source port in outgoing traffic).

If you want to allow incoming traffic from outside the network to the local network, create an “in” direction rule, and select the port range on which you want to allow incoming traffic. Select LAN port on which this traffic needs to be directed and the desired protocol.

These rules can be applied by enabling the service from the **Service Name** drop-down menu on the **Port Forwarding** screen.

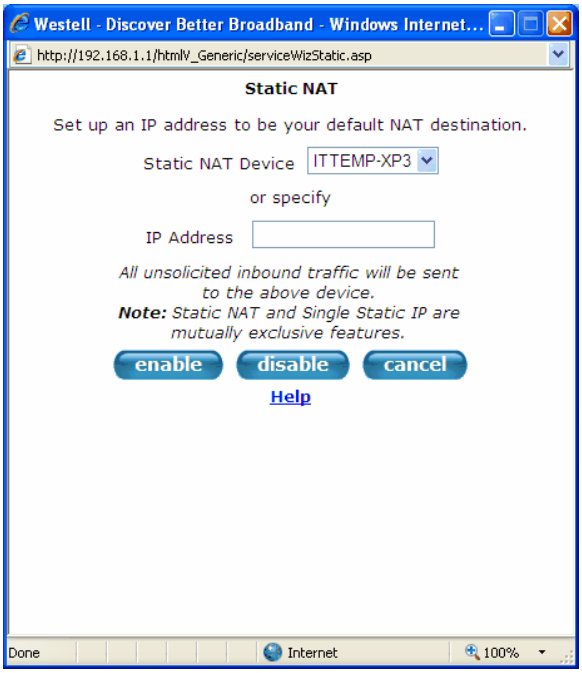


Service Name	Displays the name for the “new” service being created.
Protocol	Click this drop-down menu to select the IP Protocol type. • both: BOTH Transmission Control Protocol and User Datagram Protocol. • tcp: Transmission Control Protocol. • udp: User Datagram Protocol.
Start Port	Displays the start Port number for Incoming/Outgoing Packets.
End Port	Displays the end Port number for Incoming/Outgoing Packets.
LAN Port	Displays the Port number to map the Incoming WAN Packets to. This will not be required for outgoing packets.
Direction	Click this drop-down menu to select the direction of the packet. • in: Incoming WAN Packets. • out: Outgoing WAN Packets.

Port Direction	Click this drop-down menu to select the port that needs to be checked. • dst: Rule will be created for destination port. • src: Rule will be created for source port.
add	Click this button to create/adds a rule to the custom service.
done	Click this button to return to the **Port Forwarding** screen.

12.2.2.5 Static NAT

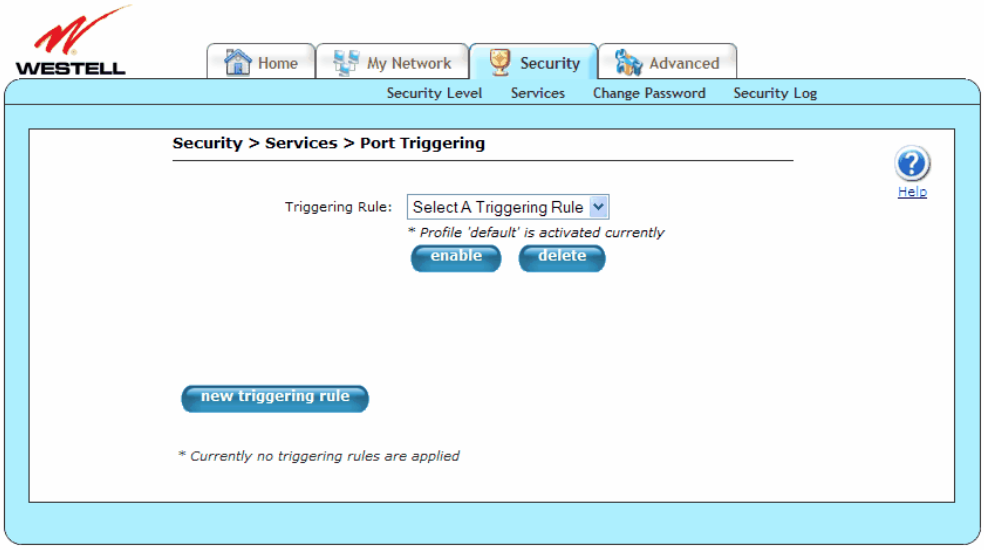
The following screen will appear if you click the **static NAT** button from the **Port Forwarding** screen (**Security > Services > Port Forwarding**). This screen allows you to set up an IP address to be your default NAT destination, mapping a private IP address to a public IP address, where the public address is the WAN IP address of the modem. This allows an internal host to have an unregistered (private) IP address and still be reachable over the Internet. If you change the settings in this screen, click **enable**. If you click **cancel**, the screen will return to its previous settings. Click **disable** to disable Static NAT.



Static NAT Device	Click this drop-down menu to select name of the device that will function as the default NAT destination.
IP Address	Displays the IP address of the device that will function as the default NAT destination.

12.2.3 Port Triggering

The following screen will appear if you select **Security > Services > Port Triggering** from the main menu. This screen allows you to configure port triggering. In port triggering, outbound traffic on predetermined ports ("triggering ports") causes inbound traffic to specific incoming ports to be dynamically forwarded to the initiating host while the outbound ports are in use. This screen contains the Port Triggering Rule Configuration, which allows you to forward a range of ports to the LAN only after outbound traffic has been sent to a specified range of ports. Currently active port triggering ranges are displayed and can be removed by clicking the **delete** button.



Triggering Rule	Click this drop-down menu to select an active Port Triggering Rule.
enable	Click this button to open the **Apply Rule** screen (**Security > Services > Port Triggering > Apply Rule**), which will show the details of the rule and allow you to apply the selected rule. Refer to section 12.2.3.1, "Apply Rule."
delete	Click this button to delete an existing Port Triggering rule.
Rule Name	Displays name of the Triggering Rule enabled from the drop-down menu.
Outgoing Protocol	Displays the protocol for outgoing connection from the local network.
Port Start	Displays the LAN side TCP/UDP start port.
Port End	Displays the LAN side TCP/UDP end port.
Incoming Protocol	Displays the incoming protocol for the triggered ports.
Port Start	Displays the WAN side TCP/UDP start port.
Port End	Displays the WAN side TCP/UDP end port.
New triggering rule	Click this button to add a new Port Triggering rule using the **New Triggering Rule** screen (**Security > Services > Port Triggering > New Triggering Rule**). Refer to section 12.2.3.2, "New Triggering Rule."

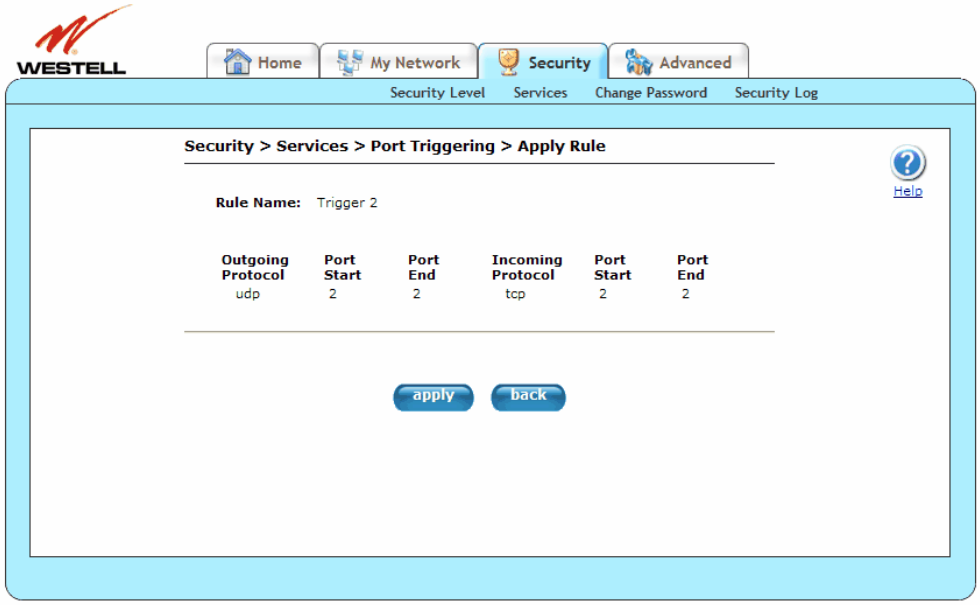
NOTE: Not all of the options are available on every screen.

The following screen appears when you select a **Triggering Rule** from the drop-down menu, and click the **enable** button.

To apply the triggering rule, click the **apply** button and then **OK**. The **Port Triggering** screen will now display the newly applied triggering rule.

12.2.3.1 Apply Rule

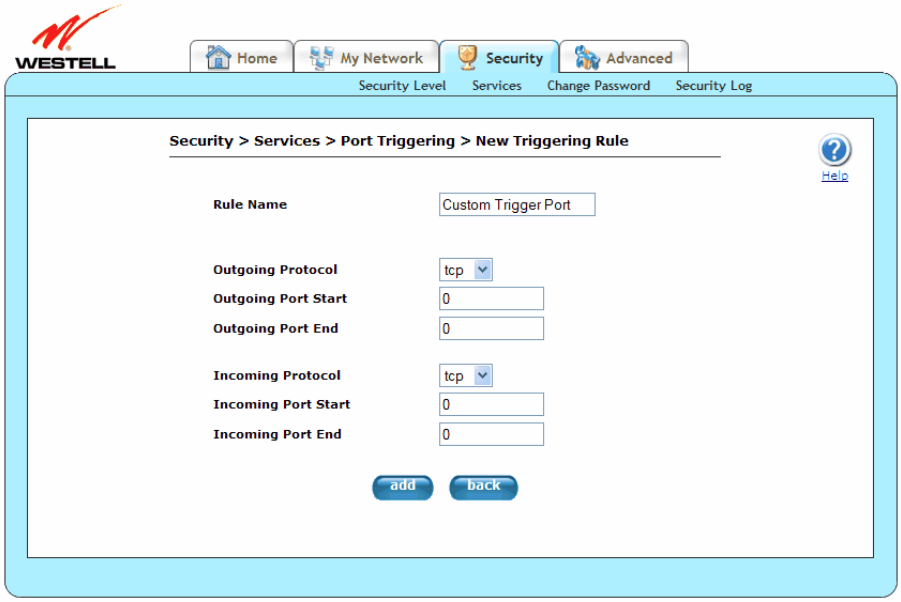
The following screen will appear if you click the **enable** button from the **Port Triggering** screen (**Security > Services > Port Triggering > Apply Rule**). This screen allows you to apply a rule previously selected from the **Triggering Rule** drop-down menu.



Rule Name	Displays the name for the new port triggering rule being created.
Outgoing Protocol	Click this drop-down menu to select an outgoing connection from the local network on a predetermined port or range of ports: • Tcp: Transmission Control Protocol. • Udp: User Datagram Protocol.
Port Start	Displays the local LAN side TCP/UDP start port.
Port End	Displays the local LAN side TCP/UDP end port.
Incoming Protocol	Click this drop-down menu to select the incoming protocol for the triggered ports: • Tcp: Transmission Control Protocol. • Udp: User Datagram Protocol.
Port Start	The WAN side TCP/UDP start port.
Port End	The WAN side TCP/UDP end port.
apply	Click this button to create a port triggering rule that can be enabled from the **Port Triggering** screen's **Triggering Rule** drop-down menu.
back	Click this button to return to the **Port Triggering** screen.

12.2.3.2 New Triggering Rule

The following screen will appear if you click the **new custom service** button from the **Port Triggering** screen (**Security > Services > Port Triggering > New Triggering Rule**). This screen allows you to create a "new" port triggering rule that will then be added to the **Triggering Rule** drop-down menu.



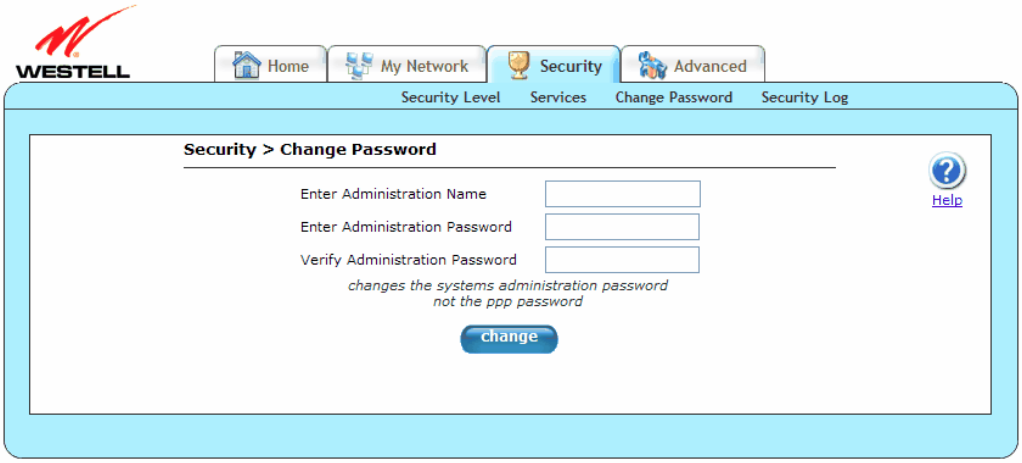
Rule Name	Displays the name for the new port triggering rule being created.
Outgoing Protocol	Click this drop-down menu to select an outgoing connection from the local network on a predetermined port or range of ports: • Tcp: Transmission Control Protocol. • Udp: User Datagram Protocol.
Outgoing Port Start	Displays the local LAN side TCP/UDP start port.
Outgoing Port End	Displays the local LAN side TCP/UDP end port.
Incoming Protocol	Click this drop-down menu to select the incoming protocol for the triggered ports: • Tcp: Transmission Control Protocol. • Udp: User Datagram Protocol.
Incoming Port Start	The WAN side TCP/UDP start port.
Incoming Port End	The WAN side TCP/UDP end port.
add	Click this button to create a port triggering rule that can be enabled from the **Port Triggering** screen's **Triggering Rule** drop-down menu.
back	Click this button to return to the **Port Triggering** screen.

12.3 Change Password

The following screen will appear if you select **Security > Change Password** from the main menu. This screen allows you to change your Administration Name and Administration Password, protecting the modem from any unauthorized modifications to the configuration settings. The values typed in the password fields will be masked for security purposes. If you change the settings in this screen, click **change** and then **OK**. If you click **Cancel**, the screen will return to its previous settings.

NOTE: If the modem is password protected and you are not an authorized user, you will not be able to change the value in this screen. (The modem cannot be configured unless an authorized user is logged in.) Contact your network administrator for further instructions.

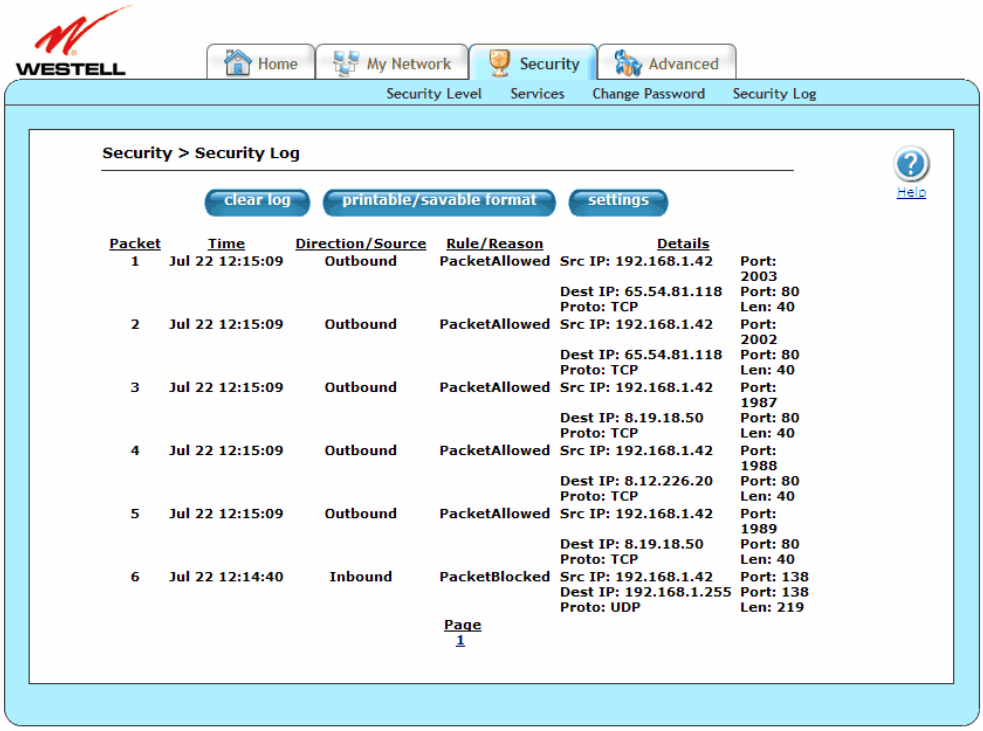
IMPORTANT: The **Security > Change Password** screen allows you to use **admin** as your **administration name** (your administration name can match your user name). However, this screen does not allow you to use **"password"** as your **administration password**. You must type a different password in order for this screen to take effect. If you type **password** in the fields labeled **Enter Administration Password** and **Verify Administration Password**, this screen will not continue the logon. Once you decide on an **administration name** and **password**, please record them for future reference.



Enter Administrative Name Note: This changes the Systems Administrator password, not the PPP password.	Type the name of your network administrator.
Enter Administrative Password	Type your network administrator's password in this field.
Verify Administrative Password	Retype your network administrator's password in this field.

12.4 Security Log

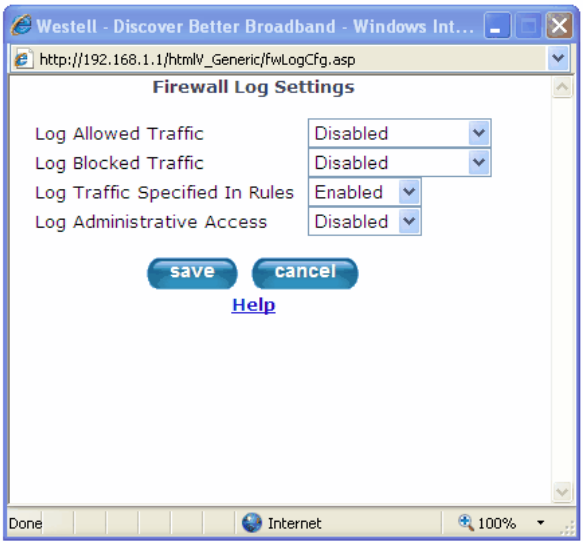
The following screen will appear if you select **Security > Security Log** from the main menu. This screen is an advanced diagnostics screen and will alert you of noteworthy information sent to your modem from the Internet. It may also contain entries that indicate Local Administrative Access and/or Remote Access logins or failures. Up to 1000 entries can be made, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for new entries as they occur.



Clear log	Click this button to remove all entries from the log.
printable/savable format	Click this button to open a new window that contains a list of all the logged packets that can be saved to file or sent to a local printer.
Settings	Click this button to select the information that you want logged via the F**irewall Log Settings** window. Click **OK** on the pop-screen that follows. Refer to section 12.4.1, "Firewall Log Settings."
Packet	Displays the packet number.
Time	Displays the time that the packet was sent.
Direction/Source	Displays the direction of transmission.
Rule/Reason	Displays the internal rule that caused the logged event. The internal rule is set up under Firewall rules.
Details	Displays a description of the logged event.
Page	Clicking a number link at the bottom of the page navigates you to the corresponding range of entries. The most recent entries are always on the highest numbered page.

12.4.1 Firewall Log Settings

The following screen will appear if you click the **settings** button from the **Security Log** screen (**Security > Security Log > Firewall Log Settings**). This screen allows you to configure firewall logging. Remote logging allows the firewall logs to be sent to a machine running a syslog server.



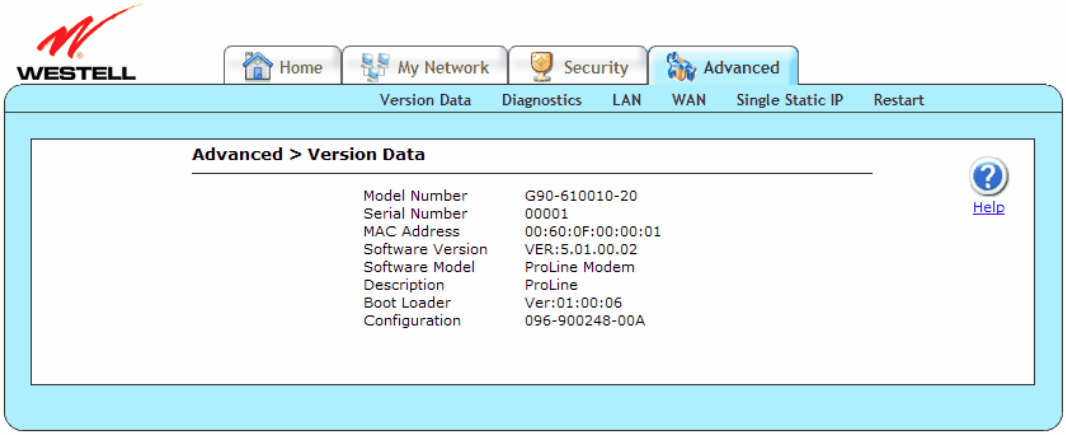
Log Allowed Traffic	Click this drop-down menu to choose from the log allowed traffic options. • Disabled: System will not log allowed traffic. • Inbound Packets: System will log inbound packets only. • Outbound Packets: System will log outbound packets only. • All Packets: System will log both inbound and outbound packets.
Log Blocked Traffic	Click this drop-down menu to choose from the log blocked traffic options. • Disabled: System will not log blocked traffic. • Inbound Packets: System will log inbound packets only. • Outbound Packets: System will log outbound packets only. • All Packets: System will log both inbound and outbound packets.
Log Traffic Specified In Rules	Click this drop-down menu to enable or disable logging traffic specified in rules.
Log Administrative Access	Click this drop-down menu to enable or disable logging administrative access.
save	Click this button to save the changes made on this screen.
cancel	Click this button to cancel the changes made on this screen.

13. ADVANCED

This section explains the advanced features of your modem and guides you through the configurable settings. It provides instructions on backing up and restoring your modem's configuration settings, gives details about the statistic screens of your modem, and allows you to configure your modem's LAN, WAN, and Static IP features.

13.1 Version Data

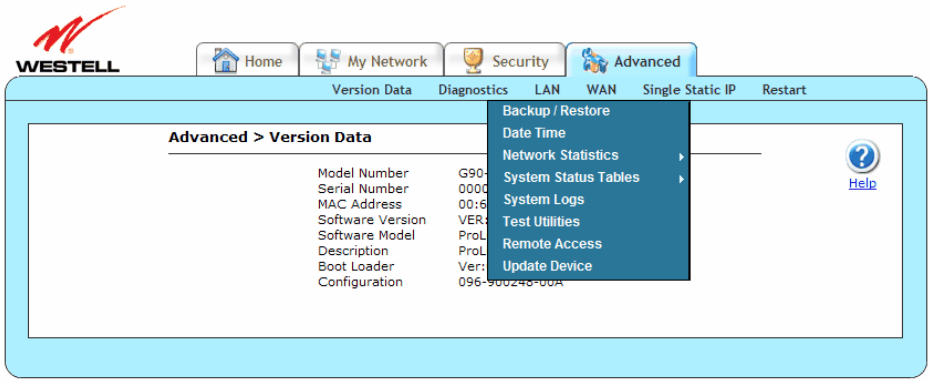
The following screen will appear if you select **Advanced > Version Data** from the main menu. This screen displays general information about your modem.



Model Number	Displays your modem manufacturer's model number.
Serial Number	Displays your modem manufacturer's serial number.
MAC Address	Displays your modem Media Access Controller (MAC); i.e., hardware address of this device.
Software Version	Displays your modem's version of application software.
Software Model	Displays your modem's application type.
Description	Displays your modem's product description.
Boot Loader	Displays your modem's version of boot loader software
Configuration	Displays your modem's proprietary configuration number.

13.2 Diagnostics

This section discusses the **Diagnostics** screens (Backup/Restore, Date Time, Network Statistics, System Status Tables, System Logs, Test Utilities, Remote Access, and Update Device) of your modem and guides you through the configurable settings.

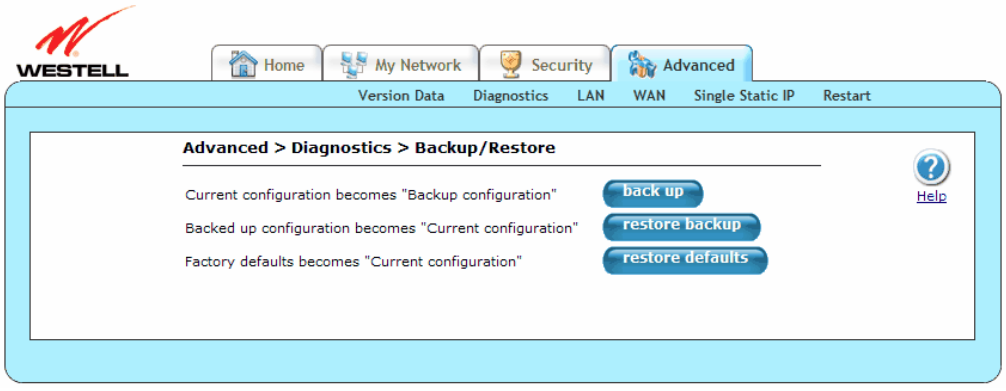


13.2.1 Backup/Restore

The following screen will appear if you select **Advanced > Diagnostics > Backup/Restore** from the main menu. This screen allows you to configure backup and restore settings for your modem.

NOTE: Backup settings are stored in a separate area of flash memory in the modem, not to an external backup source.

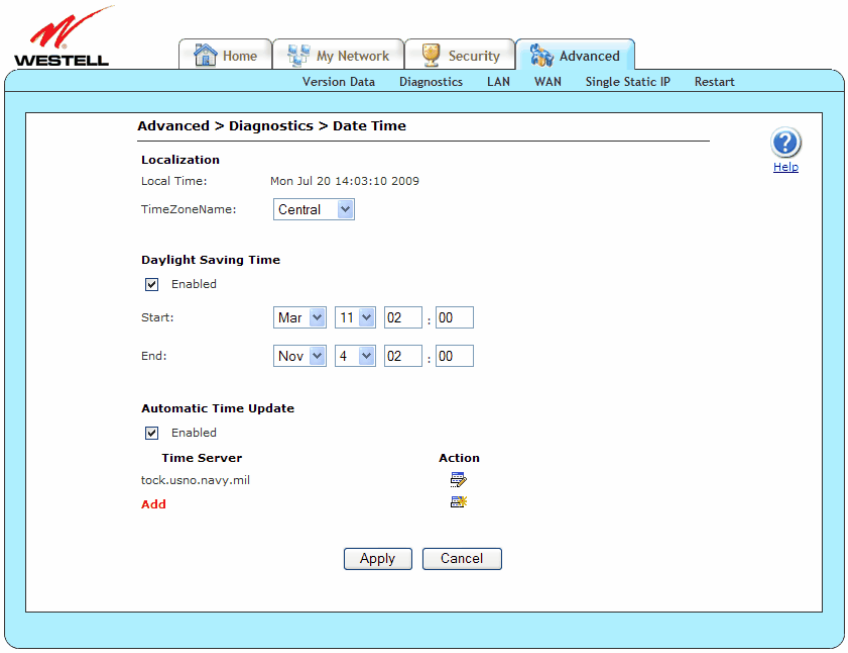
CAUTION: If you restore the modem to factory default settings, any data that the modem has reported will be lost.



Current configuration becomes Backup Configuration	Click this button to store the current configuration of your modem so that it can be recalled later.
Backed up configuration becomes current configuration	Click this button to retrieve the last back up copy of all configuration parameters and make these values current.
Factory default becomes Current configuration	Click this button to set all user configurable parameters back to the factory default settings.

13.2.2 Date Time

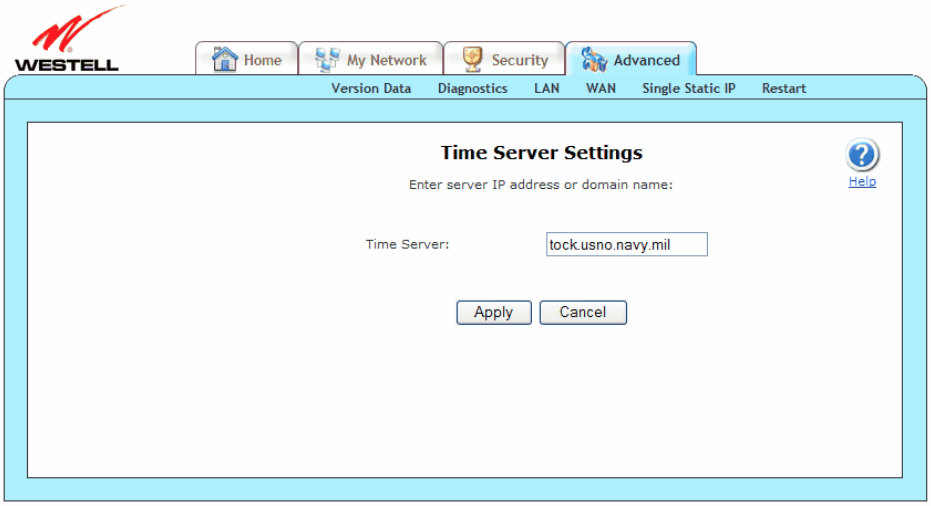
The following screen will appear if you select **Advanced > Diagnostics > Date Time** from the main menu. This feature allows you to set the date and time values of your modem. If you change the settings in this screen, click **apply** and then **OK**. If you click **Cancel**, the screen will return to its previous settings.



Local Time	Displays the local time after applying the daylight savings settings.
TimeZoneName	Click this drop-down menu to select your Time Zone values: Eastern, Central, Mountain, or Pacific.
Daylight Saving Time Enabled/Disabled	Click this check box to enable daylight savings feature.
Daylight Saving Time Start	Click these drop-down menus and type data into fields to set daylight savings start date and time.
Daylight Saving Time End	Click these drop-down menus and type data into fields to set daylight savings end date and time.
Automatic Time Update Enabled/Disabled	Click this check box to enable or disable the Automatic Time Update feature. This feature contains the entry for the time server that is contacted for obtaining the time settings. Enabling or disabling the NTP server allows you to edit the first NTP server entry or add/remove/edit a second NTP server.
Time Server	Displays the Time Server used for updating the modem.
Action Edit	Click this icon to open the **Time Server Settings** screen (**Advanced > Diagnostics > Date Time > Time Server Settings**). Refer to section 13.2.2.1, "Time Server Settings."
Action New	Click this icon to open the **Time Server Settings** screen (**Advanced > Diagnostics > Date Time > Time Server Settings**). Refer to section 13.2.2.1, "Time Server Settings."
Add	Click this icon to open the **Time Server Settings** screen (**Advanced > Diagnostics > Date Time > Time Server Settings**). Refer to section 13.2.2.1, "Time Server Settings."

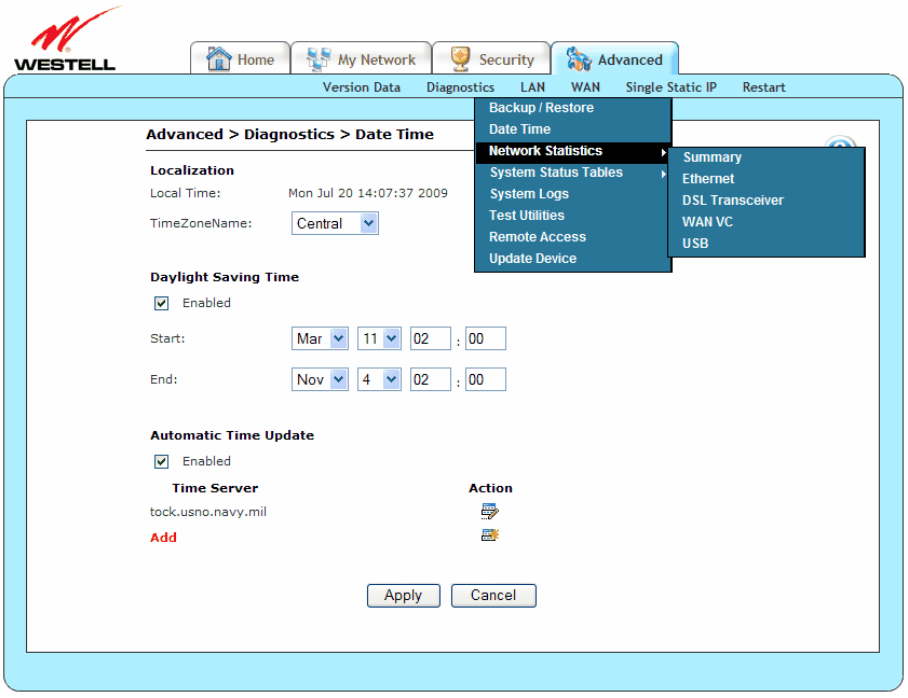
13.2.2.1 Time Server Settings

The following screen will appear if you click the **Action Edit** ( ), **Action New** ( ), or **Add** icons/link on the **Date Time** screen (**Advanced > Diagnostics > Date Time > Time Server Settings**). This screen allows you to edit NTP server domain name or IP address. If you change the settings in this screen, click **apply** and then **OK**. If you click **Cancel**, the screen will return to its previous settings.



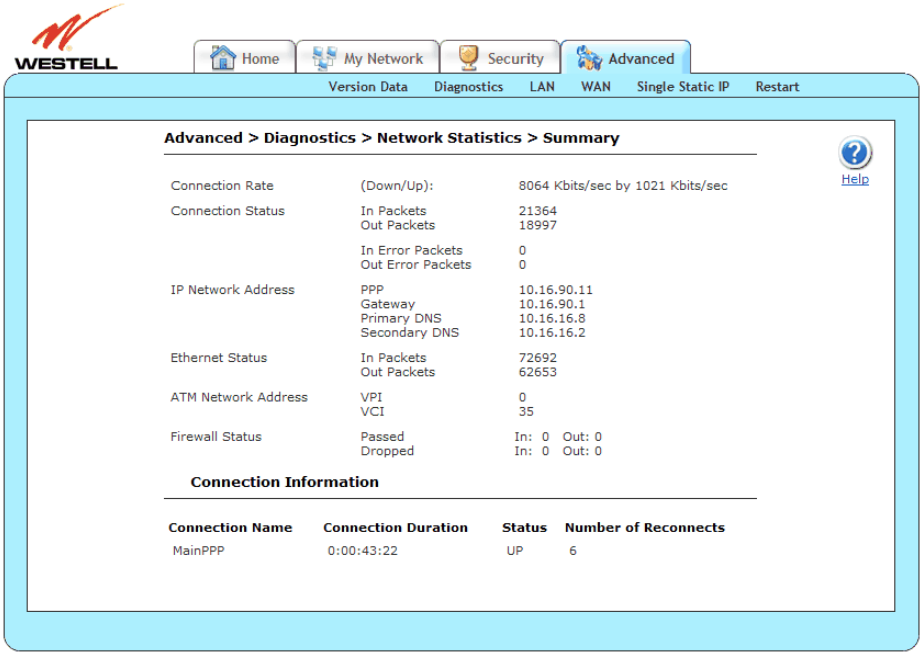
13.2.3 Network Statistics

This section discusses the **Network Statistics** screens (Summary, Ethernet, DSL Transceiver, WAN VC, and USB) of your modem and guides you through the configurable settings.



13.2.3.1 Summary

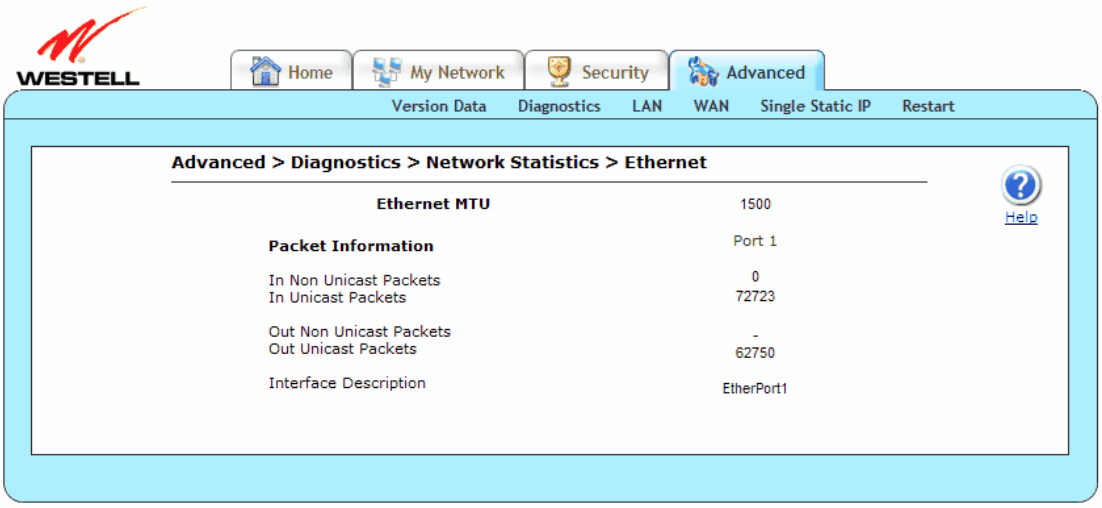
The following screen will appear if you select **Advanced > Diagnostics > Network Statistics > Summary** from the main menu. This screen displays summary information about your modem. The DSL connection state is shown along with the amount of traffic that has passed through the modem. Each connection profile is listed with its associated usage information.



Connection Rate	Displays status of DSL signal and rate of your connection.
Connection Status	Displays the number of packets received (IN) or sent (OUT) in packets via DSL as well as corresponding error packets.
IP Network Address	Displays IP Network Address data. • PPP: An IP address identifies your device on the Internet. • Gateway: IP address of your modem. • Primary DNS: Provided by your ISP. • Secondary DNS: Provided by ISP.
Ethernet Status	Displays the number of packets received (IN) or sent (OUT) in packets via Ethernet.
ATM Network Address	Displays your VPI and VCI values, which are provided by your ISP.
Firewall Status	Displays your firewall traffic in packets. • Passed: Monitors information traffic that was successfully received (IN) or transmitted (OUT) in packets. • Dropped: Monitors information traffic that was not successfully received (IN) or transmitted (OUT) due to your firewall settings.
Connection Information	
Connection Name	Displays the connection profile established previously in section 7, “Accessing Your Modem.”
Connection Duration	Displays how long your PPP session has been connected.
Status	Displays the status of your PPP session as either UP (connected) or DOWN (disconnected).
Number of Reconnects	Displays the number of attempts that were made to establish a PPP session.

13.2.3.2 Ethernet

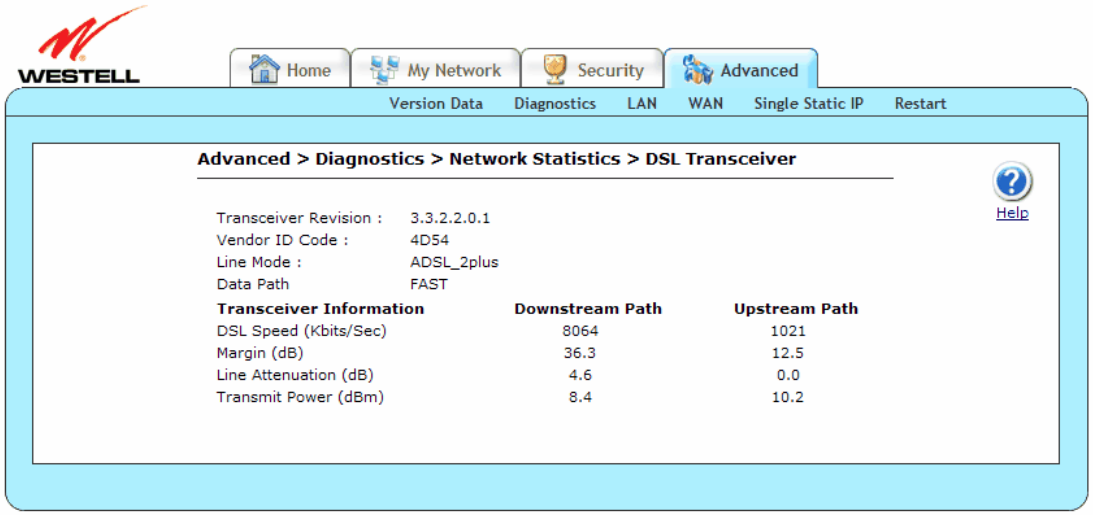
The following screen will appear if you select **Advanced > Diagnostics > Network Statistics > Ethernet** from the main menu. This screen displays information about your modem's Ethernet connections.



Ethernet MTU	Displays the maximum transmission unit (MTU): the number of data bytes contained in the Ethernet frame.
Packet Information	Displays packet information reported for ports 1-4.
In Non Unicast Packets	Displays the number of non-Unicast packets received on the Ethernet interface. "In" is from the PC to the modem.
In Unicast Packets	Displays the number of Unicast packets received on the Ethernet interface. "In" is from the PC to the modem.
Out Non Unicast Packets	Displays the number of non-Unicast packets transmitted on the Ethernet interface. "Out" is from the modem to the PC.
Out Unicast Packets	Displays the number of Unicast packets transmitted on the Ethernet interface. "Out" is from the modem to the PC.
Interface Description	Displays the modem's interface type.

13.2.3.3 DSL Transceiver

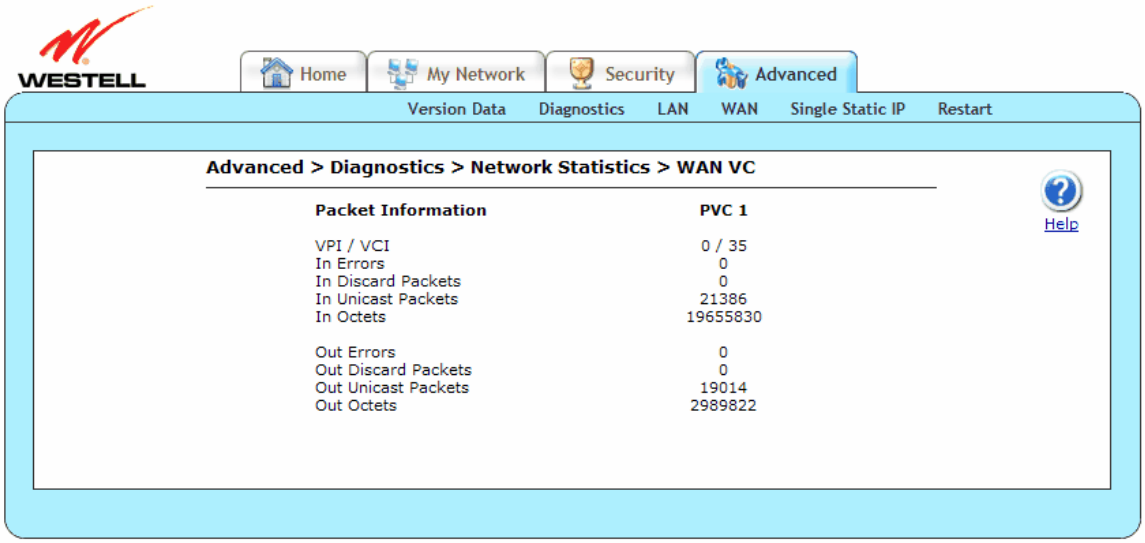
The following screen will appear if you select **Advanced > Diagnostics > Network Statistics > DSL Transceiver** from the main menu. This screen displays information about your modem's DSL transceiver.



Transceiver Revision	Displays the transceiver software version number.
Vendor ID Code	Displays the CPE vendor's chipset ID code.
Line Mode	Displays the operational mode: ADSL2, Annexl, ADSL_ANSI_T1.413, ADSL_G.dmt, ADSL_G.lite, ADSL_2plus, and ADSL_re-adsl.
Data Path	Displays the data path used (either Fast or Interleaved).
Transceiver Information-Downstream Path/Upstream Path	
DSL Speed (Kbits/Sec)	Displays the transmission rate provided by your ISP.
Margin (db)	Displays the Signal-to-Noise Ratio (S/N), where 0 db = $1x10^{-7}$, which inhibits your DSL speed.
Line Attenuation (dB)	Displays DSL line loss.
Transmit Power (db/Hz)	Displays transmitted signal strength.

13.2.3.4 WAN VC

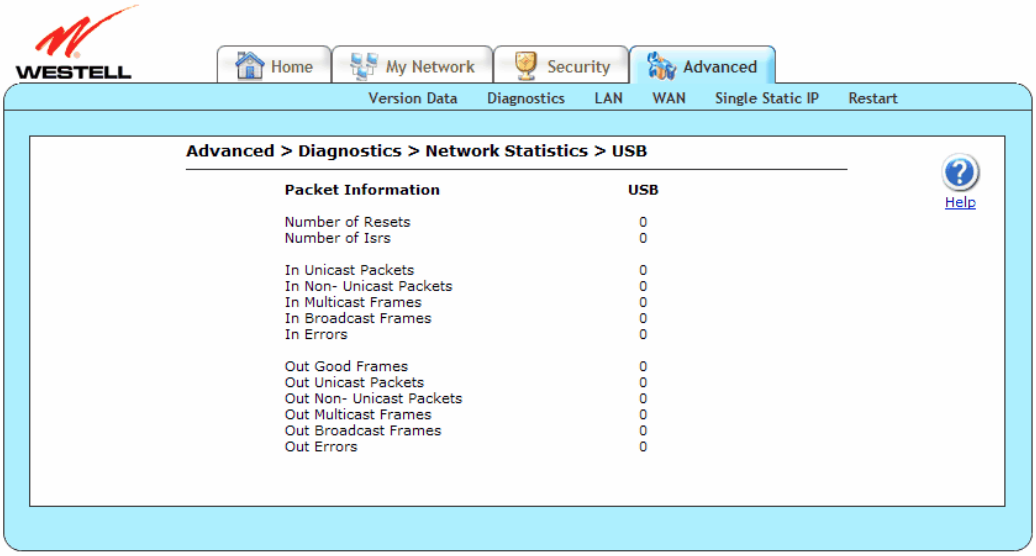
The following screen will appear if you select **Advanced > Diagnostics > Network Statistics > WAN VC** from the main menu. This screen displays information about your modem's WAN virtual connection (VC) settings.



VPI/VCI	Displays the VPI/VCI values obtained from your ISP.
In Errors	Displays the number of error packets received on the ATM port. "In" is from the PC to the remote.
In Discard Packets	Displays the number of discarded packets received. "In" is from the PC to the remote.
In Unicast Packets	Displays the number of Unicast packets received on the ATM port. "In" is from the PC to the remote.
In Octets	Displays the number of bytes received on the ATM port. "In" is from the PC to the remote.
Out Errors	Displays the number of outbound packets that could not be transmitted due to errors. "Out" is from the remote to the PC.
Out Discard Packets	Displays the number of outbound packet discarded. "Out" is from the remote to the PC.
Out Unicast Packets	Displays the number of Unicast packets transmitted on the ATM port. "Out" is from the remote to the PC.
Out Octets	Displays the number of bytes transmitted on the ATM port. "Out" is from the remote to the PC.

13.2.3.5 USB

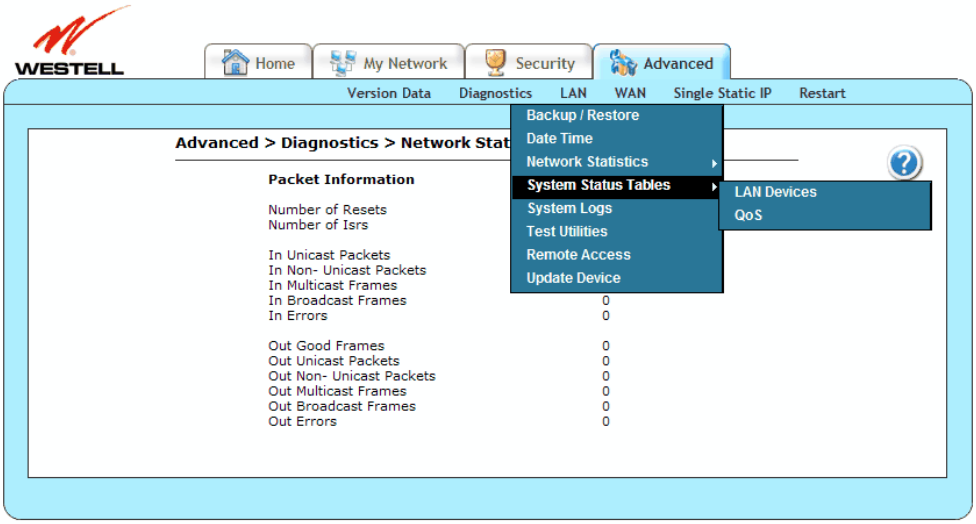
The following screen will appear if you select **Advanced > Diagnostics > Network Statistics > USB** from the main menu. This screen displays information about your modem's USB connection.



Number of Resets	Displays the number of times the Host PC reset the USB Interface.
Number of Isrs	Displays the number of times the Host PC requested communication with the modem.
In Unicast Packets	Displays the number of packets received that did not have a Multicast or Broadcast class destination IP address. "In" is from the host PC to the modem.
In Non-Unicast Packets	Displays the number of packets received that had a Multicast or Broadcast class destination IP address. "In" is from the host PC to the modem.
In Multicast Frames	Displays the number of frames received that had a Multicast class destination IP address. "In" is from the host PC to the modem.
In Broadcast Frames	Displays the number of frames received that had a Broadcast class destination IP address. "In" is from the host PC to the modem.
In Errors	Displays the number of packets received with an invalid format. "In" is from the host PC to the modem.
Out Good Frames	Displays the number of frames sent to the Host PC. "Out" is from the modem to the host PC.
Out Unicast Packets	Displays the number of packets sent that did not have a Multicast or Broadcast class destination IP address. "Out" is from the modem to the host PC.
Out Non-Unicast Packets	Displays the number of packets sent that had a Multicast or Broadcast class destination IP address. "Out" is from the modem to the host PC.
Out Multicast Frames	Displays the number of frames sent that had a Multicast class destination IP address. "Out" is from the modem to the host PC.
Out Broadcast Frames	Displays the number of frames sent that had a Broadcast class destination IP address. "Out" is from the modem to the host PC.
Out Errors	Displays the number of packets received by the modem but not sent to PC due to an Error condition. "Out" is from the modem to the host PC.

13.2.4 System Status Tables

This section discusses the **System Status Tables** screens (LAN Devices and QoS) of your modem and guides you through the configurable settings.



13.2.4.1 LAN Devices

The following screen will appear if you select **Advanced > Diagnostics > System Status Tables > LAN Devices** from the main menu. The modem scans the network for devices that are connected to your LAN. If you want to disable this feature in the modem, click **disable scanning**.

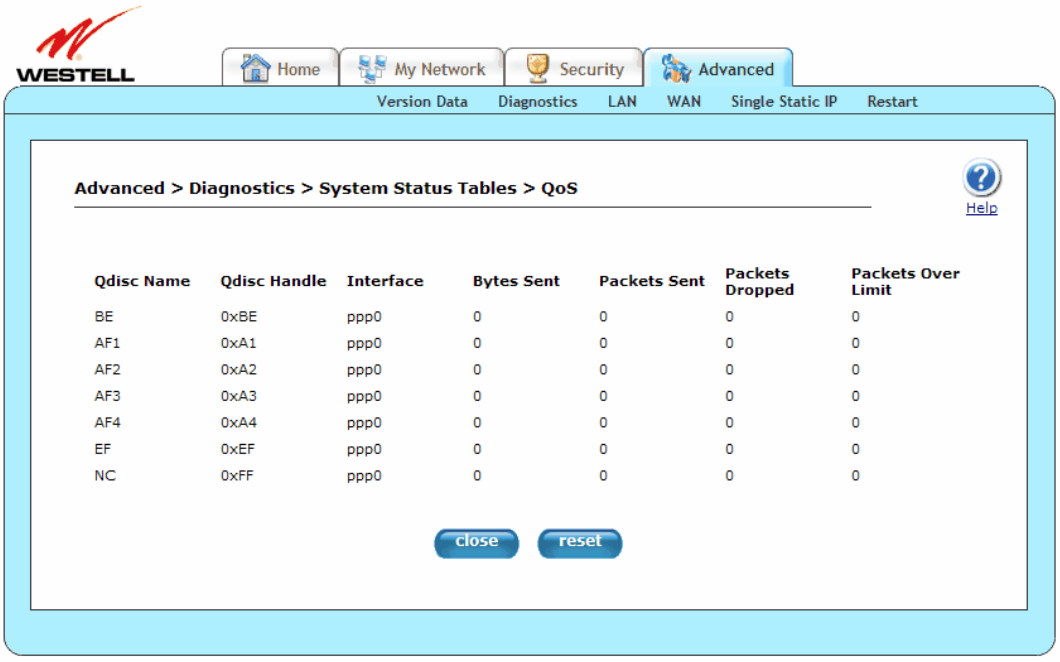
IP Address	Displays the IP network address that your modem is on.
MAC Address	Displays the Media Access Controller (MAC) address of this device.
Name	Displays the ASCII (text) name of the devices connected to the LAN.
Status	Displays the status of the devices connected to the LAN.
Enable/disable scanning	Click this button to enable or disable the scanning function.

13.2.4.2 QoS

The following screen will appear if you select **Advanced > Diagnostics > System Status Tables > QoS** from the main menu. This screen contains the Internet Protocol QoS Status.

Click **close** to return to the **Version Data** screen.

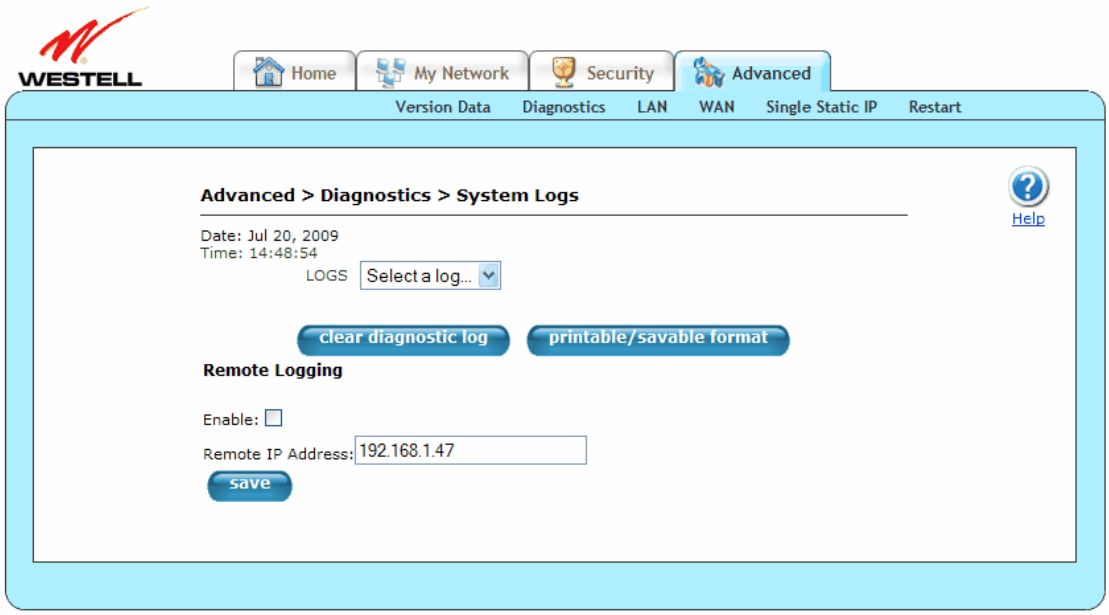
NOTE: QoS must be enabled for this table to be populated.



Qdisc Name	Displays the QoS Discipline Name.
Qdisc Handle	Displays the QoS Discipline Handle.
Interface	Displays the QoS Discipline Interface.
Bytes Sent	Displays the QoS Discipline Interface.
Packets Sent	Displays the number of bytes sent.
Packets Dropped	Displays the number of packets dropped.
Packets Over Limit	Displays the number of packets over the committed limit.
close	Click this button to exit out of the QoS screen.
reset	Click this button to reset the QoS statistics information to 0.

13.2.5 System Logs

The following screen will appear if you select **Advanced > Diagnostics > System Logs** from the main menu. This screen allows you to manage diagnostic log data. If you change the settings in this screen, click **save** and then **OK**. If you click **Cancel**, the screen will return to its previous settings.



Date	Displays the current date.
Time	Displays the current time.
LOGS	Click this drop-down menu to select a logging option. • All: Lists both Connection and System logs. • Connection: List all events related to connection activity (Any traffic on the USB, Ethernet, or DSL ports). • System: List all events related to system activity (Time, Errors, Boot Information, etc).
Clear diagnostic log	Click this button to clear diagnostic log data.
Printable/savable format	Click this button to open up a pop-up window detailing modem status and events that may be printed or saved to file.
Remote Logging Enable/Disable	Click this check box to enable/disable Remote Logging. Remote Logging contains the configuration for the diagnostics remote logging, allowing diagnostics logs to be sent to a machine running a syslog server. If saving the diagnostics logs is desired, remote diagnostics logging should be enabled, and the IP address of the syslog server must be configured. Note: The syslog server must be configured to listen on udp port 514, which is usually the default. In order for the logs to be saved to the syslog server, the server should be configured to save the logs to a file. Some of the free syslog servers available on the internet are kiwisyslog, MT_syslog and 3CSyslog.
Remote IP Address	Displays the IP address of the syslog server machine to which the diagnostics logs will be sent.
save	Click this button to save changes made to the **System Logs** screen.

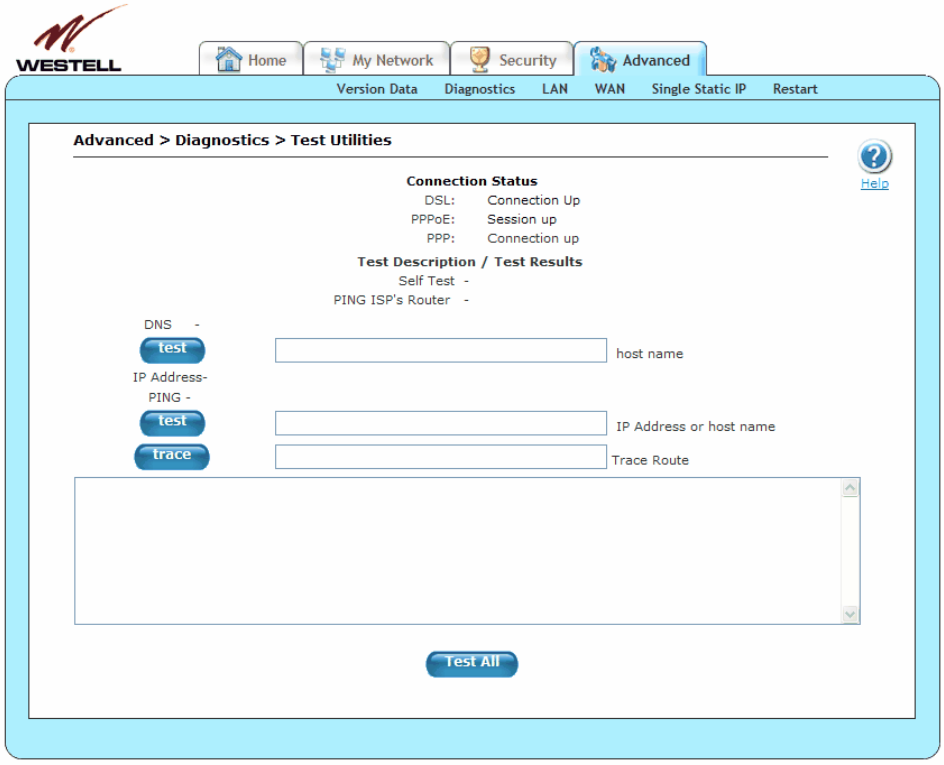
13.2.6 Test Utilities

The following screen will appear if you select **Advanced > Diagnostics > Test Utilities** from the main menu. This screen provides tools for diagnosing network connection problems. Some tests depend on the modem status and the capabilities exercised by previous tests, and, therefore, may not be run.

If you want to PING using the **Test Utilities** screen, type your **DNS** or **IP** address in the fields provided, and click the **test** button. The System Self Test will run a diagnostic test that executes independent of firewall security settings.

If you want to PING using the MS-DOS (shell) window on your PC or station, you will first need to check your firewall security setting. (If you PING via DOS shell you are susceptible to firewall rules, as this PING is dependent on your modem's firewall settings.) If your firewall is set to **Medium** or **High**, you will not be able to PING. You must set your firewall security setting to **Low** or **None**.

- To run a DNS test, type the appropriate host name in the field provided, and then click **test.**
- To run a PING test, type the appropriate IP address or host name in the field provided, and then click **test.**
- To run a Trace Route, type the appropriate IP address or host name in the field provided, and then click **trace.**
- To run a full diagnostic test on your modem, click **Test All.**



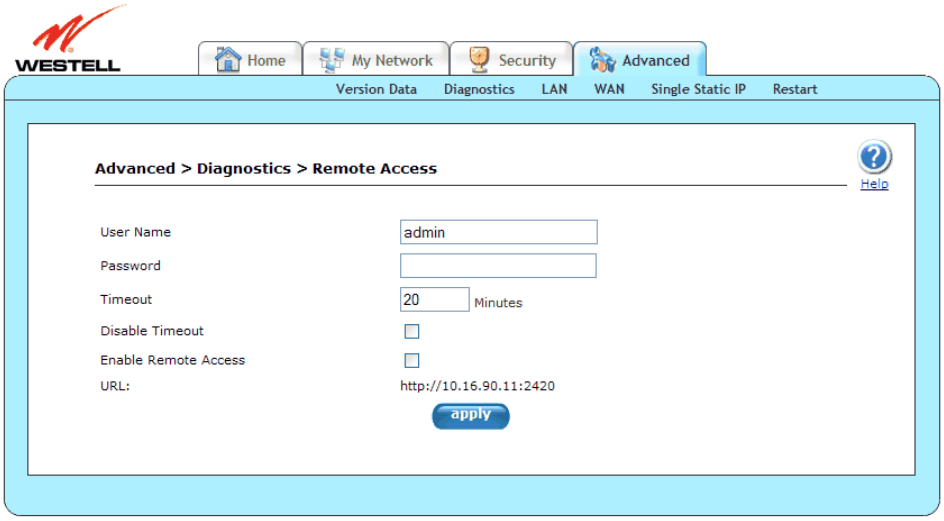
DSL	Displays the DSL connection status. If the status is DOWN, check to be sure the cable connecting your modem to the DSL wall jack is properly connected. (Also, ensure the plug is properly seated in the modem jack.) If this is ok, then try another phone cable. Next, wait for the modem to train (this may take up to two minutes). If it still hasn't come into sync, try power cycling the modem. If after trying these approaches the modem still will not sync, contact your ISP. • UP: Your modem is operating correctly and has obtained synchronization with the opposing network device. • DOWN: Your modem is operating correctly, but not synchronized with the opposing device.

PPPoE	Displays the PPPoE session status: • Session UP: A valid PPPoE session has been detected. • No Session: Currently, there is no active PPPoE session established. • Initiating Session: A PPP session must be connected from the homepage screen. • Connecting: The connection process for a PPPoE session has been initialized. Wait 10-15 seconds and try again. If discovery still cannot complete, there may be a configuration issue with your ISP's equipment. Verify your VPI/VCI settings (on the **Advanced > WAN > VCs screen**) and contact your provider. • Authenticating: The authentication process for a PPPoE session has been initialized. Wait 10-15 seconds and try again. If this fails, there may be a configuration issue with your provider's equipment. Verify your Username/Password settings (on the **Advanced > WAN > Connection Overview > profile editor > edit screen**), and contact your provider. • Idle: A PPPoE session was halted. WAN Cable must be connected and UP, then a PPP session must be connected from the **Home** screen. If the connection still cannot complete, there may be a configuration issue with your ISP's equipment. Verify your VPI/VCI settings (on the **Advanced > WAN > VCs** screen) and contact your ISP. • Disconnecting: The disconnection process for a PPPoE session has been initialized. Wait a few seconds for the PPPoE connection to come down.
PPP	Displays the PPP connection status. Note: A PPPoE session must already be established. • Connection UP: Modem has established a PPP connection • No Connection: There is no PPP connection. A PPP session must be connected from the **Home** screen.
Test Description / Test Results	
Self Test	Displays the results of an integrity check of certain internal components of the modem. • Success: The modem is operating correctly. • Flash Corrupt: The self test process has detected a problem with internal flash memory. Restart the modem. If the error persists, contact your ISP.
PING ISP's Router	Displays the results of an IP network check (an IP Ping) of the ISP's router. This test verifies that the modem can exchange IP traffic with an entity on the other side of the DSL line. • Success: Modem has detected an IP Remote Router connection. • No Response: The IP Remote Router does not answer the IP Ping. This test fails when the ISP's router does not give its IP address to the modem during session establishment. Try pinging another host, using the IP Address – PING **test** button. If you are able to ping any host, or even if you are able to find an IP address for a given host name (try "www.yahoo.com"), then the failure of the "IP Remote Router" test is moot because the success of the ping demonstrates that you are getting IP traffic across the DSL line. If the separate ping fails as well, contact your ISP.
DNS test	Type the **host name** in the provided field, and click the DNS **test** button to resolve the name of a particular host. • Success: Your modem has successfully obtained the resolved address. The IP address is shown below the **host name** field. • No Response: Your modem has failed to obtain the resolved address. Determine the IP addresses of your DNS servers (from the **Home** screen, click **Edit** > **Advanced**), and then ping test those addresses. This may provide useful information when you contact your ISP and speak with Technical Support. • Host not found: The DNS Server was unable to find an address for the given host name. • No data, enter host name: No host name is specified. • Could not test: The test could not be executed due to your modem's settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a ping.

IP Address PING test	Type the **IP Address or host name** in the provided field, and click the IP Address PING **test** button to perform an IP continuity check to a remote computer either within or beyond the ISP's network. If you ping by host name, DNS will be used to look up the appropriate IP address for that name. • Success: The Remote Host computer was detected. • No Response: Many IP hosts are configured to not respond to IP ping message. If you are successful with a DNS test using the same host name, your connection is probably fine whether you can ping the named host or not. • No name or address to PING: No host name or IP address was specified. • Could not test: The test could not be executed due to your modem's settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a ping.
IP Address PING trace	Type the IP Address or host name in the **Trace Route** field, and click the **trace** button to perform an IP traceroute to a remote computer either within or beyond the ISP's network. Trace Route is used to determine where the packet is stopped on the network. If you trace by name, DNS will be used to look up the appropriate IP address for that name. • Success: Trace will display its progress in the provided field. Trace will show three round trip times and the DNS name (if available) of each intermediate modem. • Failure: Trace will display "*" when it doesn't receive a response or can't determine the DNS name of an intermediate modem. This is not necessarily an error; some modems are configured to ignore trace route packets or don't have DNS names.
Test All	Click this button to run a full diagnostic test on your modem.

13.2.7 Remote Access

The following screen will appear if you select **Advanced > Diagnostics > Remote Access** from the main menu. This screen allows you to configure your modem so that it can be configured remotely. Once enabled, this feature can be manually disabled or will automatically disable after the configured period of inactivity. If you change the settings in this screen, click **apply** and then **OK**. If you click **Cancel**, the screen will return to its previous settings.



User Name	Displays your **User Name** in the provided field.
Password	Displays your **Password** in the provided field.
Timeout	Displays the **Timeout** minutes in the provided field. This is the number of minutes after which remote access will be deactivated (if it has been activated).

Disable Timeout	Click this check box (a checkmark will appear) to activate the Disable Timeout feature. Uncheck the check box to deactivate this feature.
Enable Remote Access	Click this check box (a checkmark will appear) to activate Enable Remote Access. Uncheck the check box to deactivate this feature.
URL	Displays the IP address of the remote management device (modem). This address must be placed in a remote PC's Web browser in order to communicate with your modem. If this field says "Not Connected," you are not currently connected to the Internet.

To enable remote access, please follow these steps:

1. Type the administrator's password in the field provided.

   NOTE: The password should be at least 4 characters long and should not exceed 32 characters. Do not type a blank space or asterisks in the **Password** field. The password is case sensitive.

2. Click the **Enable Remote Access** check box (a check mark will appear in the check box).
3. Click **apply** button to allow the settings to take effect.

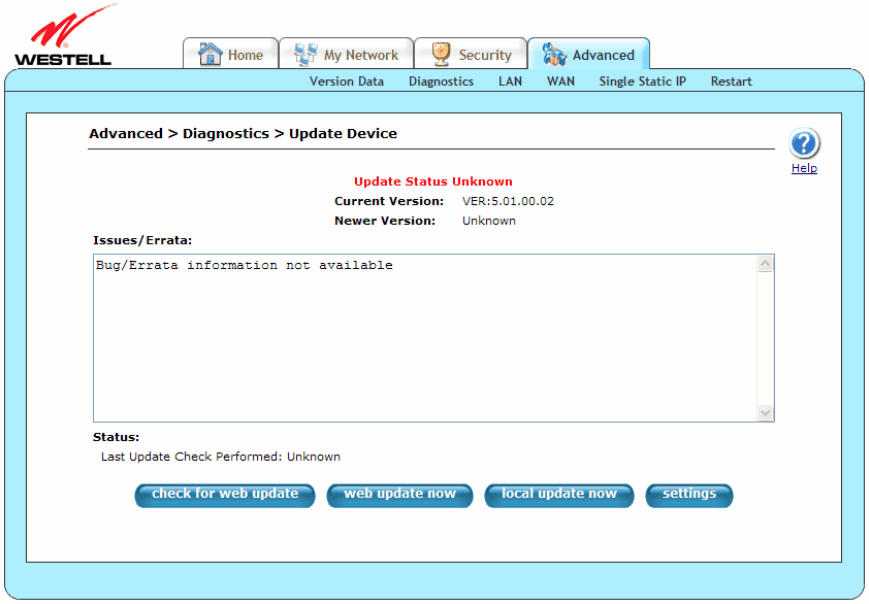
Congratulations! You have successfully enabled remote access.

13.2.8 Update Device

The following screen will appear if you select **Advanced > Diagnostics > Update Device** from the main menu. This screen is used to update the firmware that controls the operation of your modem. The updated firmware may be loaded either from a file that is located on a local hard drive or from update files stored on an Internet server.

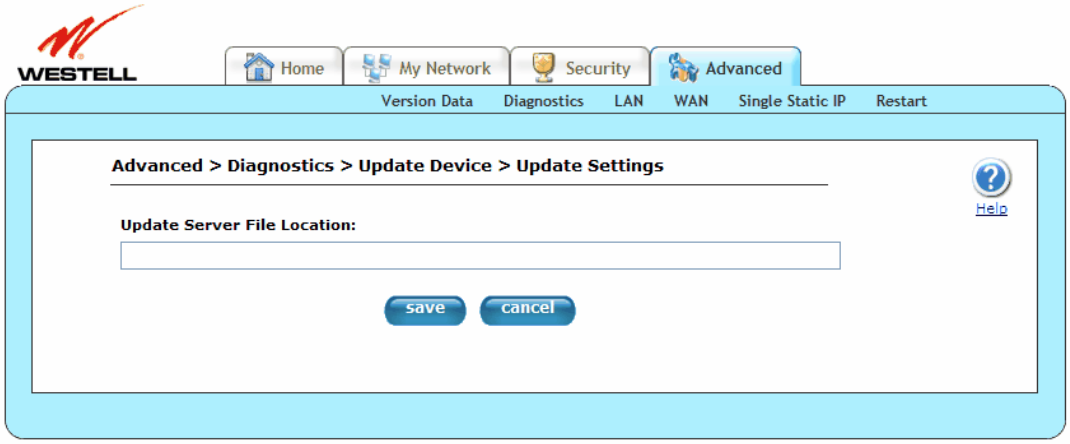
This maintenance screen enables users to check the Internet for modem software upgrades, using the **check for web update** button. (An Internet site must be specified that contains the proper update files and may or may not be specified by default.) A **local update now** button option allows users to update the software from a file stored locally.

CAUTION: The configurable settings of your modem may be erased during the update process.



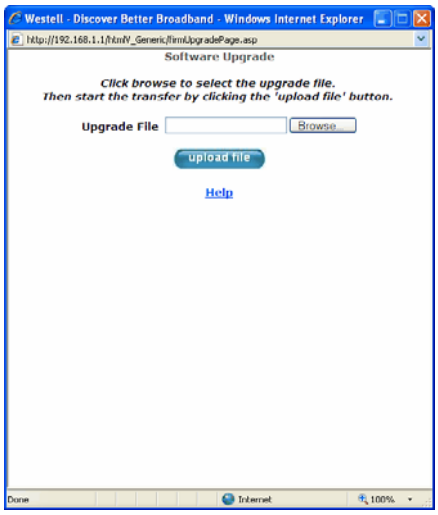
Current Version	Displays the current version of the modem software.
Available Version	Displays the version of software available for download. This field is only valid after the **check for web update** button is clicked and completed.
Issues/Errata	Displays issues/errata that have been addressed in the version to be downloaded and issues/errata that are known to exist. This field is only valid after the **check for web update** button is clicked and completed.
check for web update	Click this button to initiate your modem reading the Upgrade File from the Internet site specified in the settings and display the information in the **Available Version** and **Issues/Errata** fields. This command only provides information about the latest version. To actually perform the update, click the **web update now** button. Note: If you click **check for web update**, and the screen returns "bug information not available," this indicates that the software update file is not available.
web update now	Click this button to initiate your modem reading the update file from the Internet site specified in the settings, and if the update is applicable, download the update file and apply it to the modem.
local update now	Click this button to open the **Update Software** screen. This screen can be used to update the modem from a file stored locally.
settings	Click this button to open the **Update Settings** screen. This screen can be used to configure the FTP/HTTP site where the update information for this product is stored.

To display the location of the software update file, click the **settings** button in the **Advanced > Diagnostics > Update Device** screen (**Advanced > Diagnostics > Update Device > Update Settings**). The following screen will appear. Click **save** to save this file to the desired location.

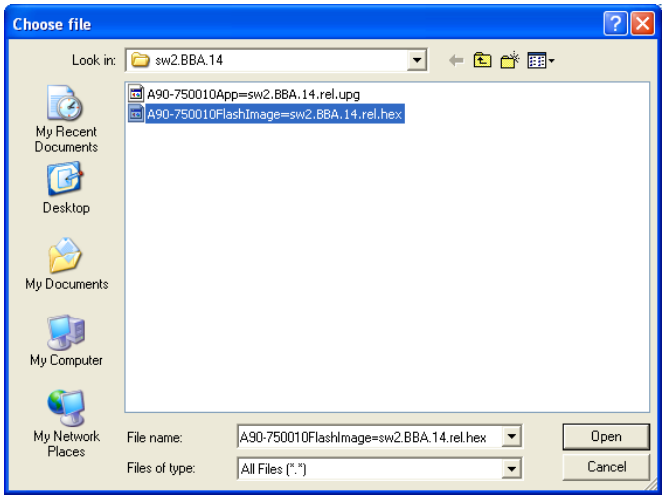


To update your modem's software using an upgrade file stored on a local hard drive, please follow these steps:

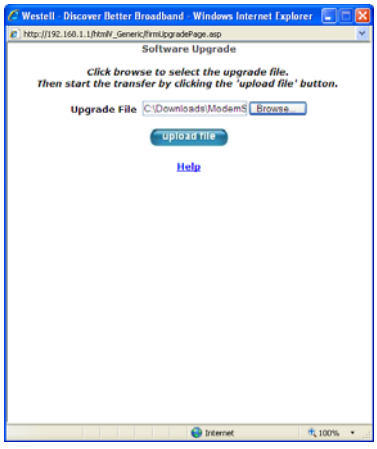
1. Click the **local update now** button in the **Advanced > Diagnostics > Update Device** screen. The following window will appear.

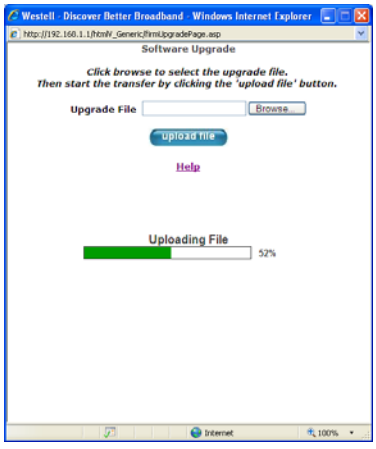


2. Click **Browse…** and navigate to the location where the upgrade file is stored.

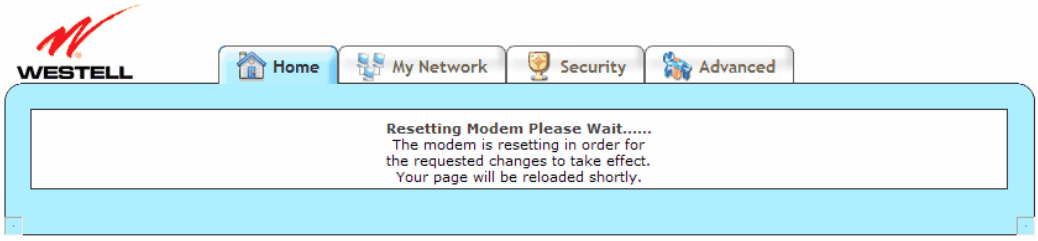


3. Select the appropriate upgrade file from your browser, and click **Open**. The file name will appear in the field labeled **Upgrade File**.
4. Click the **upload file** button from the **Software Upgrade** window, and the upload will begin.





Once the upload is complete, the following screen will appear, and your modem will reset.



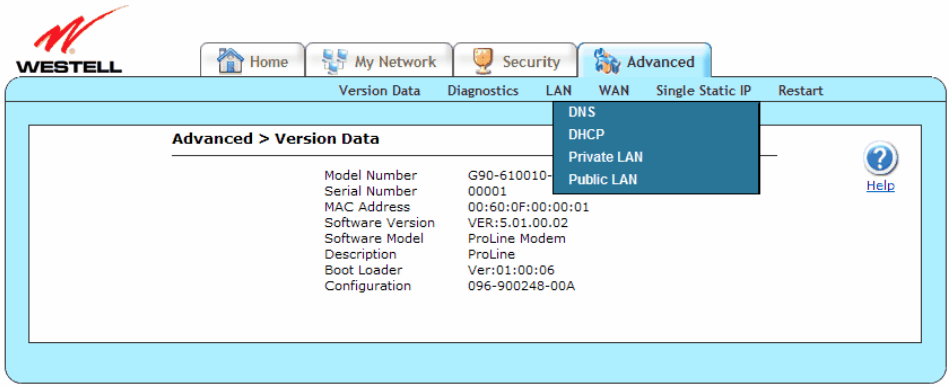
After a brief delay, the **Home** screen will appear.

5. Confirm that you have a DSL sync and that the PPP Status displays **UP**. (If necessary, click **connect** in the **Home > Connection Overview** screen to establish your PPP session.)

Congratulations! You have successfully updated your modem's software.

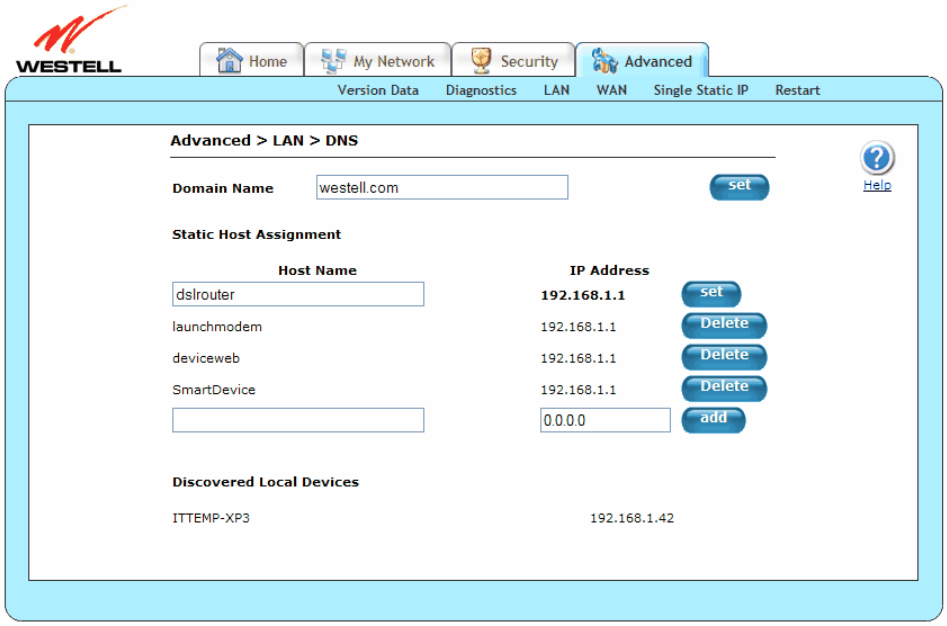
13.3 LAN (Local Area Network)

This section discusses the **LAN** (Local Area Network) screens (DNS, DHCP, Private LAN, and Public LAN) of your modem and guides you through the configurable settings.



13.3.1 DNS

The following screen will appear if you select **Advanced > LAN > DNS** from the main menu. Your modem has a built-in DNS server and a feature called Dynamic DNS. When an IP address is assigned, the modem will interrogate the new device for a machine name, using several well-known networking protocols. Any names learned will be added "dynamically" to the DNS server's table of local hosts. A static host assignment is only needed if the new device does not support any of the well-known protocols.



Domain Name	Type your **Domain Name** (name of your network) in the provided field. This name uses the Internet standard for delineating domain names. To add a Domain Name, type in your new domain name and click **Set.**
Static Host Assignment	
Host Name	Type a **Host Name** for your modem and **IP Address** in the fields provided, and click the **set** button. To add a new Host name, in the field under Static Host Assignment, type in the host name and IP address and click **set**. If you click **add**, the screen will show that the **Host Name** and **IP Address** have been added to the DNS server. If you want to delete a static host assignment, click the **delete** button adjacent to the **Host Name** and **IP Address** fields that you want to delete.
IP Address	Displays the IP address that is assigned to the Host Name.
Discovered Local Devices	Displays a list of local devices on the LAN that were assigned a DHCP Address. The DNS name and IP address entry of each discovered device is displayed. If "No Discovered Devices" is displayed, manually refresh the screen.

NOTE: Names may not contain spaces. Only letters, digits and the special characters dash (-), underscore (_) and dot (.) may be used. These special characters may not appear at the beginning or at the end of a name. The maximum length of a name can be is 63 characters.

To add a new DNS entry, please follow these steps:

1. Type the new **Domain Name** in the provided field, and then click **Set** to save the setting.
2. Type a **Host Name** and **IP Address** in the fields provided, and then click **Add.**

   NOTE: Adding or deleting a static host is immediate, and does not require you to save changes.

Congratulations! You have successfully added a new DNS entry.

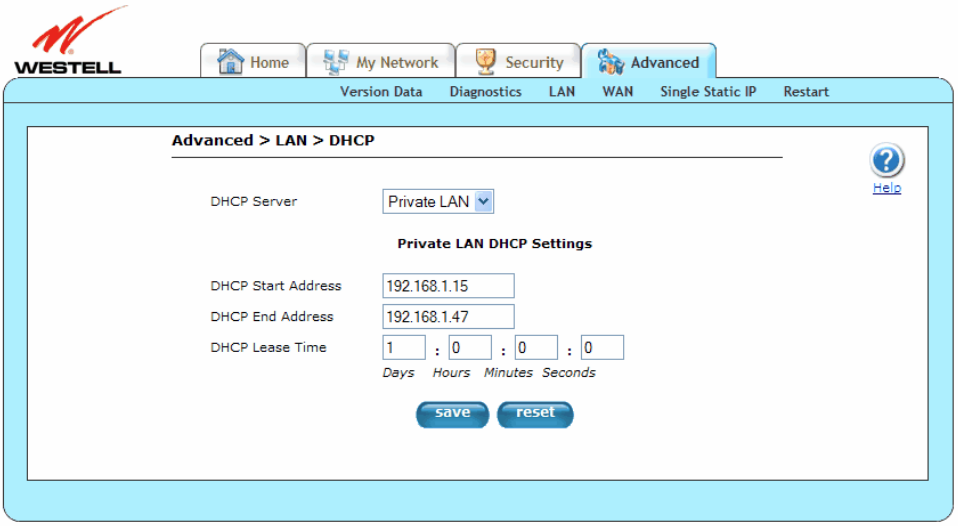
13.3.2 DHCP

The following screen will appear if you select **Advanced > LAN > DHCP** from the main menu. This screen contains the settings that control how your modem interacts with local devices connected to it. It is recommended that these settings not be changed. If you change the settings in this screen, click **save** and then **OK**. If you click **reset** or **Cancel**, the screen will return to its previous settings.

Your modem's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to DHCP clients. A client (host) is a device connected to a network.

A client sends out a broadcast message on the LAN requesting an IP address for itself. The modem's DHCP server then checks its list of available addresses and leases a local IP address to the client for a specific period of time. It simultaneously designates this IP address as "taken," and the client keeps this IP address for the duration of the lease.

NOTE: If you want to disable the DHCP server in the modem, uncheck the check box next to **Enable DHCP Server**. Westell recommends that you do not change these settings unless your ISP instructs you to do so.



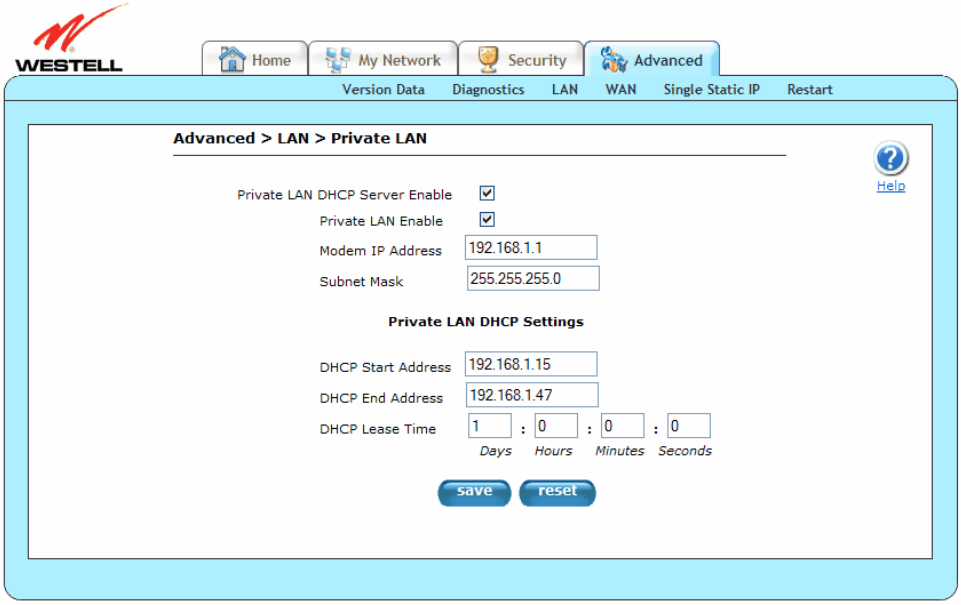
DHCP Server	Click this drop-down menu to select the DHCP (Dynamic Host Control Protocol) server. DHCP is an Internet standard that allows your modem to automatically assign IP addresses to devices connected on the LAN network. It is advised that this be enabled for **Private LAN**. • Off: DHCP Server is disabled. • Private LAN: DHCP addresses will be saved into the Private LAN configuration. • Public LAN: DHCP addresses will be saved into the Public LAN configuration. This option is only available when **Public LAN DHCP** server is enabled.
DHCP Start Address (if DHCP is enabled)	Displays the start of the IP address pool that the modem uses to assign IP addresses to local devices. Start Address must be within the IP address and lower than the DHCP End Address (any number from 0-254). By default, **DHCP Start Address** is set to **192.168.1.15**.
DHCP End Address (if DHCP is enabled)	Displays the end address of the IP address pool that the modem uses for automatic configuration of local devices. End Address must be within the IP address and higher than the DHCP Start Address (any number from 0-254). By default, **DHCP**

	End Address is set to **192.168.1.47**.
DHCP Lease Time (if DHCP is enabled)	Displays the DHCP lease time in days/hours/minutes/seconds. This is the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request. DHCP Lease Time must be greater than 10 seconds (seconds must be between 0 and 59; minutes must be between 0 and 59; and hours must be between 0 and 23). By default, **DHCP Lease Time** is set to **01:00:00:00**.

13.3.3 Private LAN

The following screen will appear if you select **Advanced > LAN > Private LAN** from the main menu. This screen contains the settings that allow you to control how your modem interacts with local devices connected to the modem. It is recommended that these settings not be changed. If you change the settings in this screen, click **save** and then **OK**. If you click **reset** or **Cancel**, the screen will return to its previous settings.

IMPORTANT: Whenever you change the Private LAN settings, the screen will display the changes; however, you must click **save** to allow the changes to take effect in the modem.



Private LAN DHCP Server Enable	Click this check box to enable the Private LAN DHCP Server feature. DHCP is an Internet standard that allows the modem to automatically assign IP addresses to devices connected on the LAN. It is recommended that you enable this for the private LAN. By default, **Private LAN DHCP Server Enable** is enabled (checked).
Private LAN Enable	Click this check box to enable the Private LAN feature. This setting enables the addresses from the Private LAN to use the NAT interface. Westell recommends that you leave this feature enabled. By default, **Private LAN Enable** is enabled (checked).
Modem IP Address	Displays your modem's IP address.
Subnet Mask	Displays the Subnet Mask, which determines what portion of an IP address is controlled by the local network and which portion is controlled by the host.
DHCP Start Address (if DHCP is enabled for Private LAN)	Displays the first IP address that the DHCP server will provide to assign IP addresses to local devices.
DHCP End Address (if DHCP is enabled for Private LAN)	Displays the last IP address that the DHCP server will provide for automatic configuration of local devices.

DHCP Lease Time (if DHCP is enabled for Private LAN)	Displays the DHCP lease time in days/hours/minutes/seconds. This is the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request. DHCP Lease Time must be greater than 10 seconds (seconds must be between 0 and 59; minutes must be between 0 and 59; and hours must be between 0 and 23). By default, the **DHCP Lease Time** is set to **01:00:00:00**.

If the settings typed in the **Private LAN Configuration** screen are incorrect, the following warning messages may be displayed in pop-up screens. If this occurs, check the settings in the **Private LAN Configuration** screen.

Warning Message	Check **Private LAN DHCP Settings** fields.
Start Address is not part of the Subnet	Check the value in the **DHCP Start Address** field.
End Address is not part of the Subnet	Check the value in the **DHCP End Address** field.
End Address is below the Start Address	Check the value in the **DHCP End Address** field.
Lease time must be greater than 10 seconds	Check the values in the **DHCP Lease Time** fields.
Seconds must be between 0 and 59	Check the **Seconds** value in the **DHCP Lease Time** field.
Minutes must be between 0 and 59	Check the **Minutes** value in the **DHCP Lease Time** field.
Hours must be between 0 and 23	Check the **Hours** value in the DHCP **Lease Time** field.

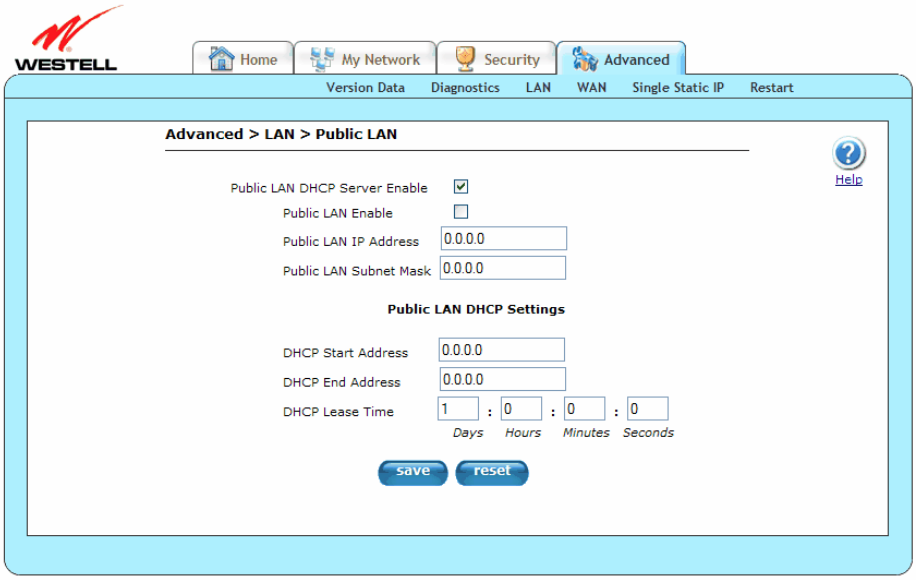
13.3.4 Public LAN

The following screen will appear if you select **Advanced > LAN > Public LAN** from the main menu. This screen contains the settings for determining how your modem will interact with the local devices connected to it. It is recommended that these settings not be changed. This feature is mutually exclusive with the VLAN feature. If you change the settings in this screen, click **apply** and then **OK**. If you click **reset** or **Cancel**, the screen will return to its previous settings.

Public LAN allows the modem to issue DHCP addresses from its Public LAN IP address pool. IP addresses served from the Public LAN pool bypass the NAT interface and are accessible from the WAN, allowing your computer to have global address ability. To use the Public LAN feature, your ISP must support Multiple IP Address Passthrough.

NOTE:

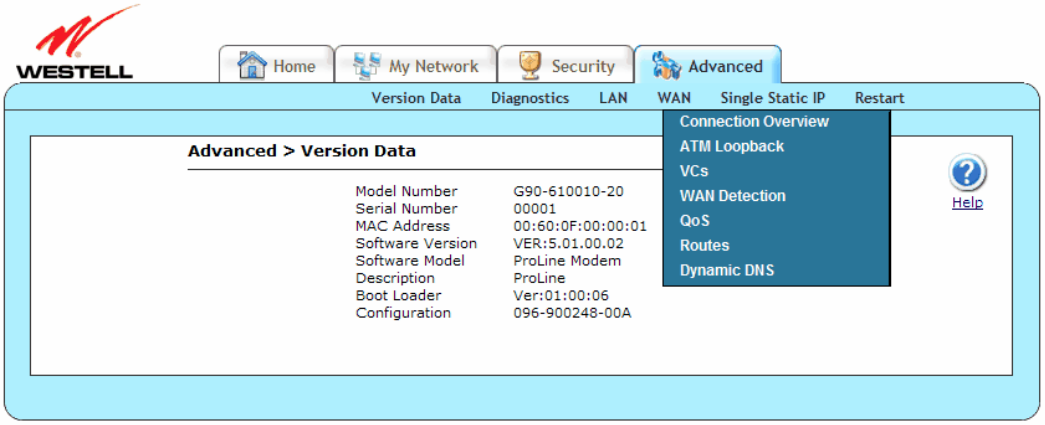
1. By enabling the DHCP server for Public LAN, you automatically disable the DHCP Server for Private LAN. By default, the modem's Public LAN DHCP server is disabled, and the Private LAN DHCP server is enabled. Whenever the Public LAN DHCP server is disabled, the modem will not issue public LAN IP addresses to devices on your network.
2. Public LAN IP addresses are provided by your ISP. If you have questions about this feature, contact your ISP for details.
3. By default, the Public LAN DHCP server is disabled. It is recommended that these settings not be changed unless you are instructed to do so by your ISP.



Public LAN DHCP Server Enable	Click this check box to enable the Public LAN DHCP Server feature. DHCP is an Internet standard that allows the modem to automatically assign IP addresses to devices connected on the LAN. It is recommended that you enable this for the public LAN. By default, **Public LAN DHCP Server Enable** is enabled (checked).
Public LAN Enable	Click this check box to enable the Public LAN feature. This setting enables the Public interface, which allows for a global subnet to exist behind your modem. Westell recommends that you leave this feature enabled. By default, **Public LAN Enable** is enabled (checked).
Public LAN IP Address	Displays your modem's IP address.
Public LAN Subnet Mask	Displays the Public LAN Subnet Mask that is used to determine if an IP address belongs to your local network.
DHCP Start Address (if DHCP is enabled for Public LAN)	Displays the first IP address that the DHCP server will provide to assign IP addresses to local devices.
DHCP End Address (if DHCP is enabled for Public LAN)	Displays the last IP address that the DHCP server will provide for automatic configuration of local devices.
DHCP Lease Time (if DHCP is enabled for Public LAN)	Displays the DHCP lease time in days/hours/minutes/seconds. This is the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request. DHCP Lease Time must be greater than 10 seconds (seconds must be between 0 and 59; minutes must be between 0 and 59; and hours must be between 0 and 23). By default, **DHCP Lease Time** is set to **01:00:00:00**.

13.4 WAN (Wide Area Network)

This section discusses the **WAN** (Wide Area Network) screens (Connection Overview, ATM Loopback, VCs, WAN Detection, QoS, Routes, and Dynamic DNS) of your modem and guides you through the configurable settings.

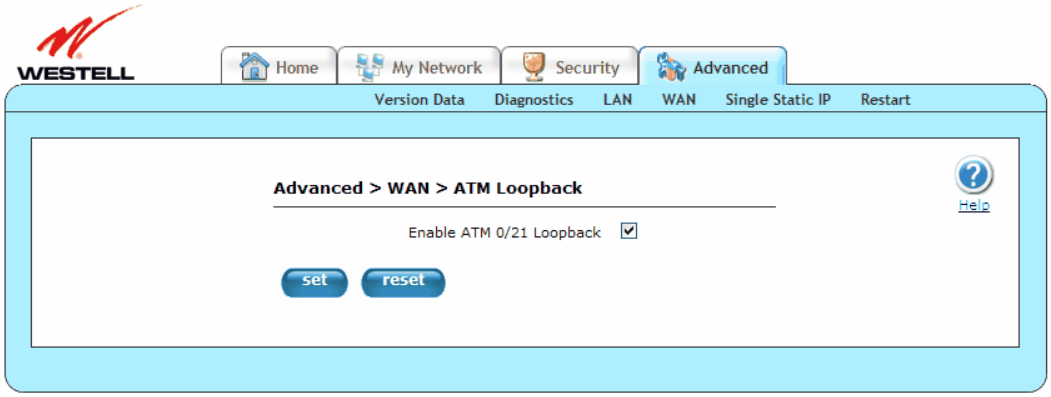


13.4.1 Connection Overview

The following screen will appear if you select **Advanced > WAN > Connection Setup** from the main menu. Please refer to section 7, "Accessing Your Modem," for detailed information on using this screen.

13.4.2 ATM Loopback

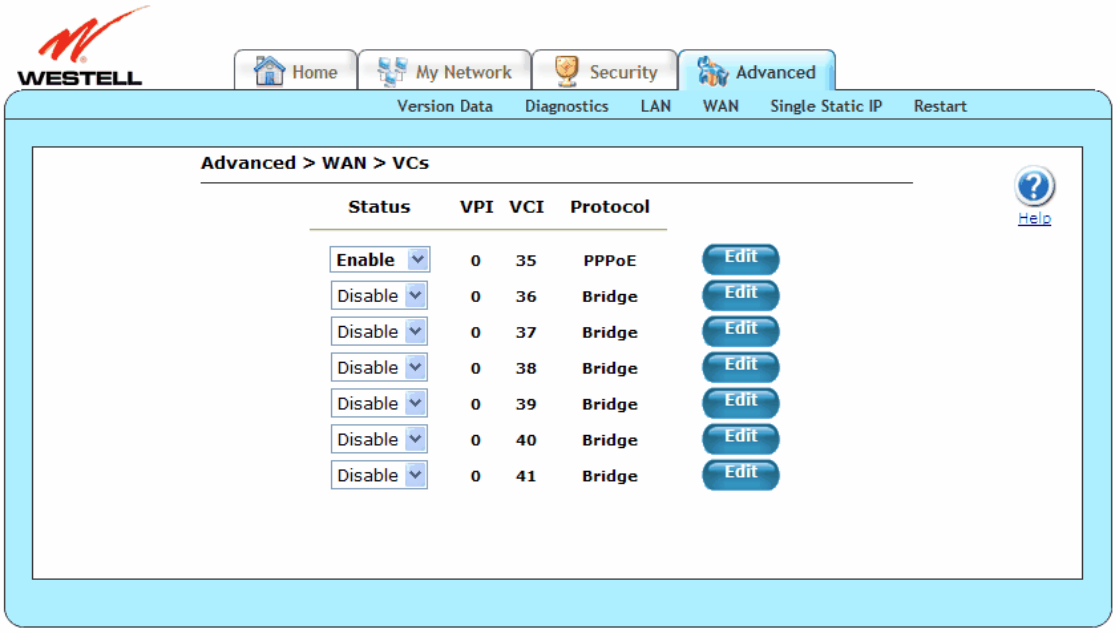
The following screen will appear if you select **Advanced > WAN > ATM Loopback** from the main menu. This setting enables an ATM cell loopback on VPI/VCI 0/21. It is recommended that this setting not be changed. If you change the settings in this screen, click **set** and then **OK**. If you click **reset** or **Cancel**, the screen will return to its previous settings.



Enable ATM 0/21 Loopback:	Click the **Enable ATM 0/21 Loopback** check box to enable this feature. By default, **Enable ATM 0/21 Loopback** is enabled (checked).

13.4.3 VCs

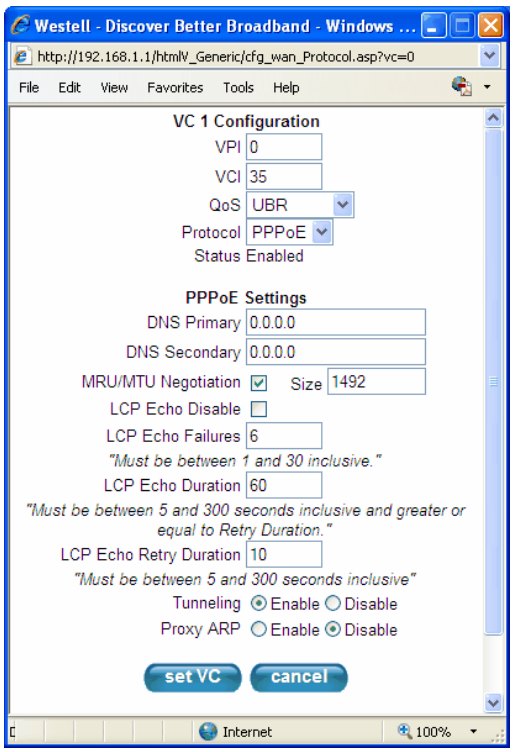
The following screen will appear if you select **Advanced > WAN > VCs** from the main menu. A VC (Virtual Connection) identifies a connection through the ISP's ATM network to your ISP. This screen is an advanced screen. Modifying parameters identified on this screen can cause severe disruption of your service. It is recommended that nothing be changed on this screen unless explicitly instructed by your ISP.



Status	Click this drop-down menu to enable or disable your VC (Virtual Connection). "Enable" must be displayed to edit VC settings.
VPI	Displays the VPI (Virtual Path Indicator) value for a particular VC, which is defined by your ISP.
VCI	Displays the VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your ISP.
Protocol Note: The configuration specified by your ISP will determine which Protocols are available to you.	Displays the Protocol for each VC, which is specified by your ISP. • PPPoA: Point to Point Protocol over ATM (Asynchronous Transfer Mode). • PPPoE: Point to Point Protocol over Ethernet. • Bridge: Bridge Protocol.
Edit	Click **Edit** button to edit the VC using the **VC 1 Configuration** window. Refer to section 13.4.3.1, "VC 1 Configuration."

13.4.3.1 VC 1 Configuration

The following screen will appear if you click the **Edit** button from the **VCs** screen (**Advanced > WAN > VCs > Edit**). This screen allows you to edit your VCs. If you change the settings in this screen, click **set VC** and then **OK**. If you click **Cancel**, the screen will return to its previous settings.



VC 1 Configuration	
VPI	Displays the VPI (Virtual Path Indicator) value for a particular VC, which is defined by your ISP.
VCI	Displays the VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your ISP.

PCR	Displays the Peak Cell Rate (PCR): The maximum rate at which cells can be transmitted across a virtual circuit, specified in cells per second and defined by the interval between the transmission of the last bit of one cell and the first bit of the next. This value is a percentage of the current data rate; for example: • 100 allows this VC to use 100% of the available bandwidth. • 80 allows this VC to use 80% of the available bandwidth. By default, **PCR** is 100.
QoS	Click this drop-down menu to select the Quality of Service (QoS). The selections available are determined by your ISP.
Protocol Note: The configuration specified by your ISP will determine which Protocols are available to you.	Click this drop-down menu to select the Protocol to be used. The selections available are determined by your ISP. • PPPoA: Point to Point Protocol over ATM (Asynchronous Transfer Mode) • PPPoE: Point to Point Protocol over Ethernet • Bridge: Bridge Protocol
Status	Displays the status of your VC (Virtual Connection). This field must display "Enable" in order to allow edits to the VC settings.
PPPoE Settings	
DNS Primary	Displays the DNS Primary address for resolving machine names, which is provided by your ISP.
DNS Secondary	Displays the DNS Secondary address for resolving machine names, which is provided by your ISP.
MRU/MTU Negotiation	Click this check box to enable or disable MRU/MTU Negotiation. If enabled, the Maximum Received Unit (MRU) would enforce MRU negotiations. By default, **MRU/MTU Negotiation** is disabled (unchecked). Note: Enable this option only at your ISP's request.
Size	Displays the size of the MRU.
LCP Echo Disable	Click this check box to enable or disable LCP Echo Disable. If checked, this option will disable the modem LCP Echo transmissions. By default, **LCP Echo Disable** is disabled (checked).
LCP Echo Failures	Displays the number of continuous LCP echo non-responses received before the PPP session is terminated. This number must be between 1 and 30 inclusive.
LCP Echo Duration	Displays the interval between LCP Echo transmissions with responses. This number must be between 5 and 300 seconds inclusive and greater or equal to **LCP Echo Retry Duration**.
LCP Echo Retry Duration	Displays the interval between LCP Echo after no response. This number must be between 5 and 300 seconds inclusive.
Tunneling	Click the option to enable or disable the Tunneling feature. If Enabled, this option allows PPP traffic to be bridged to the WAN. By default, **Tunneling** is enabled. Note: Tunneling is available in PPPoE mode only.
Proxy ARP	Click the option to enable or disable the Proxy ARP feature. When enabled, the modem replies to WAN ARPs for Public LAN Addresses. By default, **Proxy ARP** is disabled.
PPPoA Settings	
DNS Primary	Displays the DNS Primary address for resolving machine names, which is provided by your ISP.
DNS Secondary	Displays the DNS Secondary address for resolving machine names, which is provided by your ISP.
MRU/MTU Negotiation	Click this check box to enable or disable MRU/MTU Negotiation. If enabled, the Maximum Received Unit (MRU) would enforce MRU negotiations. By default, **MRU/MTU Negotiation** is disabled (unchecked). Note: Enable this option only at your ISP's request.
Size	Displays the size of the MRU.

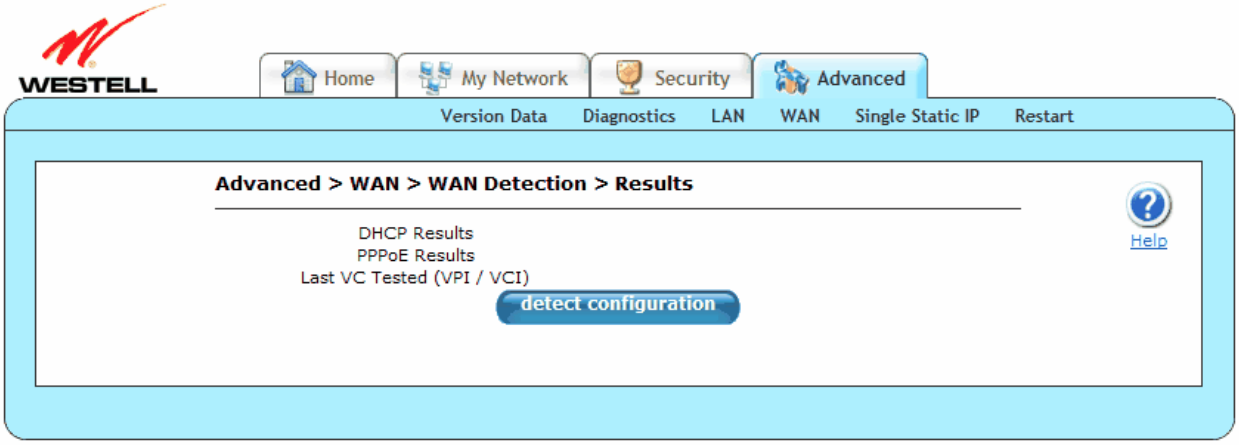
LCP Echo Disable	Click this check box to enable or disable LCP Echo Disable. If checked, this option will disable the modem LCP Echo transmissions. By default, **LCP Echo Disable** is disabled (checked).
LCP Echo Failures	Displays the number of continuous LCP echo non-responses received before the PPP session is terminated. This number must be between 1 and 30 inclusive.
LCP Echo Duration	Displays the interval between LCP Echo transmissions with responses. This number must be between 5 and 300 seconds inclusive and greater or equal to **LCP Echo Retry Duration**.
LCP Echo Retry Duration	Displays the interval between LCP Echo after no response. This number must be between 5 and 300 seconds inclusive.
Bridge Settings	
Mode	Click this drop-down menu to select the Bride Setting for the VC: Bridge or Routed Bridge.
RoutedBridge Settings	
Mode	Click this drop-down menu to select the Bride Setting for the VC: Bridge or Routed Bridge.
DHCP Client	Click the option to enable or disable the DHCP Client feature. Enabling this feature will obtain the IP address automatically. Disabling this feature will use the static IP address that you type in the provided field
IP Address	Displays the IP network address that your modem is on.
Subnet Mask	Displays the subnet mask, which determines if an IP address belongs to your local network.
Gateway	Displays the IP address of the network gateway, which is provided by your ISP.
DNS Primary	Displays DNS Primary address, which is provided by your ISP.
DNS Secondary	Displays DNS Secondary address, which is provided by your ISP.
Proxy ARP	Click the option to enable or disable the Proxy ARP feature.

13.4.4 WAN Detection

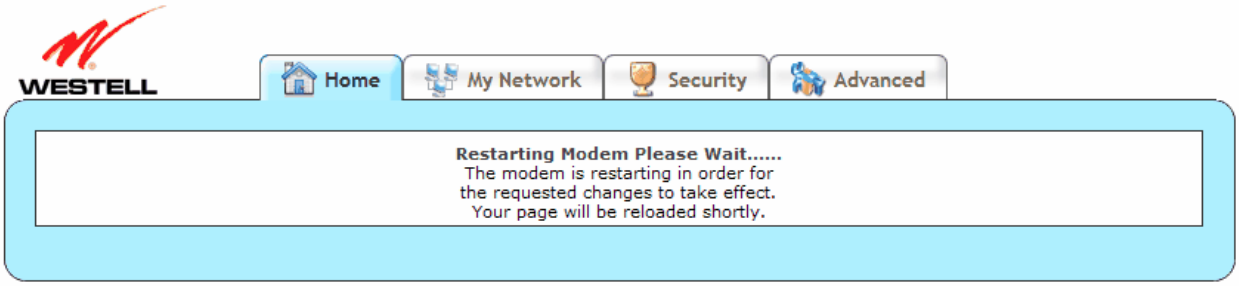
The following screen will appear if you select **Advanced > WAN > WAN Detection** from the main menu. If you click the **detect configuration** button, your modem will initiate automatic detection of the WAN protocol per VPI/VCI settings. The process detects DHCP-Enabled, Routed Bridge, or PPPoE Protocols. The process is as follows:

1. The modem tries to detect the protocol to use for connecting to your ISP.
2. The modem waits indefinitely for the DSL/Ethernet hardware link to come up.
3. The modem tries the PPPoE and Routed IP protocols.

The modem will try up to two times until a protocol is detected or until cancelled. You will be unable to access any other modem screens while the detection is in progress. Once a protocol is detected, automatic detection is not run again.

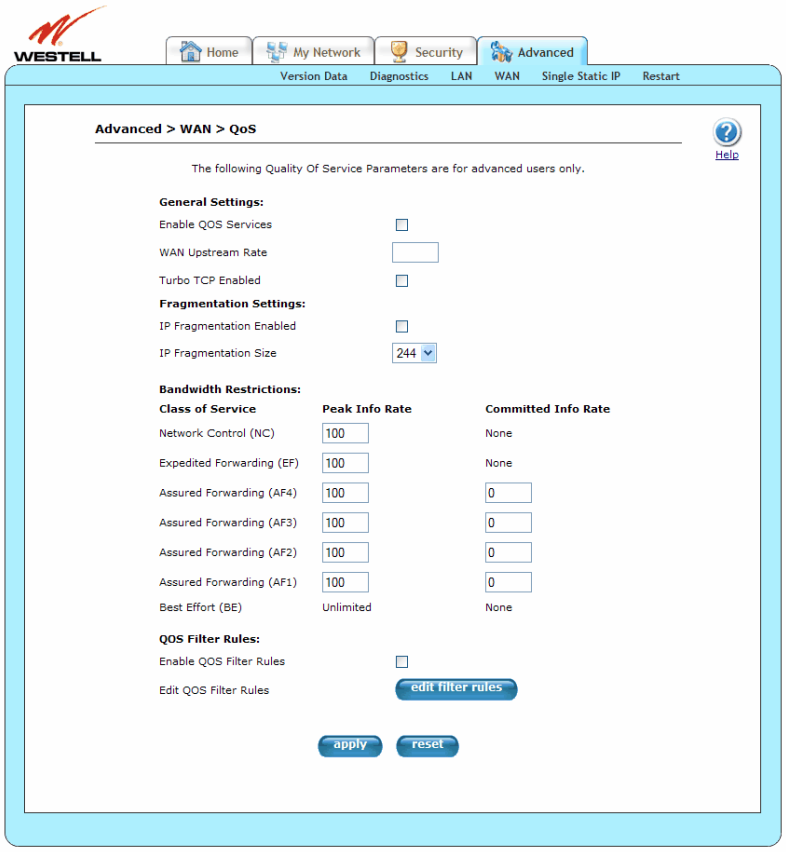


Clicking the **detect configuration** button will cause the modem to restart.



13.4.5 QoS

The following screen will appear if you select **Advanced > WAN > QoS** from the main menu. The QoS (Quality of Service) feature helps ensure data integrity in high-speed transmissions. QoS provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QoS features can be utilized to assign the appropriate traffic handling policies, including congestion management, bandwidth allocation, and delay bounds for each traffic class. Modifying parameters identified on this screen can cause severe disruption of your service. It is recommended that nothing be changed on these screens unless explicitly instructed by your ISP. If you change the settings in this screen, click **apply** and then **OK**. If you click **reset** or **Cancel**, the screen will return to its previous settings.

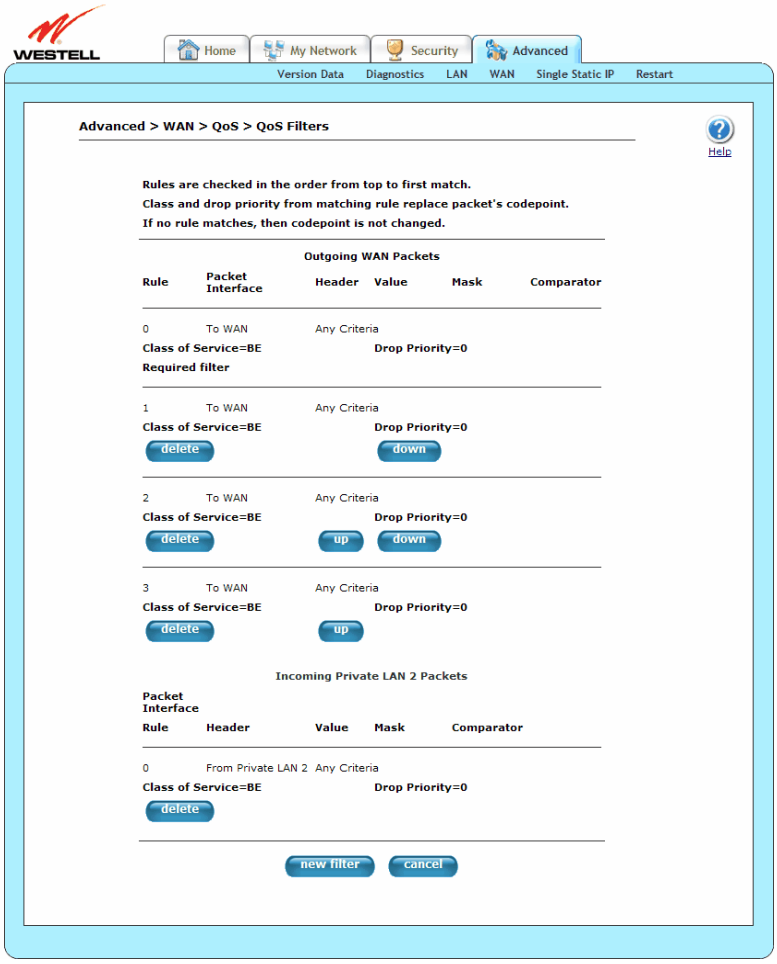


Enable QOS Services	Click this check box to enable or disable QOS Services. By default, **Enable QOS Services** is enabled (checked).
WAN Upstream Rate	Displays the effective WAN upstream rate in kbps (kilobits per second). This value is used to calculate Bandwidth Restrictions. The valid range is between 100 (100 kbps) and 100000 (100 mbps). Leave blank to use the automatically determined rate.
Turbo TCP Enabled	Click this check box to enable or disable Turbo TCP. By default, **Turbo TCP Enabled** is disabled (unchecked).
IP Fragmentation Enabled	Click this check box to enable or disable IP Fragmentation. IP Fragmentation fragments (breaks apart) large, fragmentable, low-priority packets to reduce latency for higher-priority traffic. For large, non-fragmentable, low-priority packets, the modem sends back an ICMP message specifying the fragment size as the link MTU. When enabled, and packets larger than 1500 bytes total are received by the modem, these packets will be fragmented. By default, **IP Fragmentation Enabled** is disabled (unchecked).

	Note: Later versions of the Windows OS may not honor this ICMP message for any except the very largest fragment size. If this occurs, then many Web operations may not work if a voice call is in progress.
IP Fragmentation Size	Click this drop-down menu to select the size (bytes) that the packets will be fragmented into. The available numbers consider ATM cell size boundaries, ATM Ethernet encapsulation, IP headers, and PPPoE encapsulation: 100, 148, 244, 292, 340, 388, or 436 bytes.
Class of Service	Displays the supported classes of service (ordered from lowest priority to highest priority). • Network Control (NC) • Expedited Forwarding (EF) • Assured Forwarding (AF4) • Assured Forwarding (AF3) • Assured Forwarding (AF2) • Assured Forwarding (AF1) • Best Effort (BE)
Peak Info Rate	Displays the maximum allowed rate for this Class of Service, expressed as a percentage of the WAN rate. Packets will be discarded if the offered rate exceeds this value. The Peak Information Rate can be used to prevent higher priority traffic from using all available bandwidth. No limit is necessary for the lowest priority traffic (BE). No limit is necessary for the lowest priority traffic (BE). A value of zero causes the modem to drop all packets for this class of service.
Committed Info Rate	Displays the committed rate (for Assured Forwarding classes), expressed as a percentage of the WAN rate. Packets may have the drop priority of the DSCP increased if the offered rate exceeds this value. Note that this only occurs for non-zero committed rates (i.e., a value of zero turns off the committed filter).
Enable QOS Filter Rules	Click this check box to enable or disable Enable QOS Filter Rules, allowing remarking of the packet DiffServ CodePoint (DSCP). Various filtering (matching) options can be set to determine which packets should be re-marked. Changing the DSCP of a packet changes its priority for transmission. QOS Services does not have to be enabled for filter rules to be activated. By default, **Enable QOS Filter Rules** is enabled (checked).
Edit QOS Filter Rules	Click this button to edit QOS Filter Rules using the **QoS Filters** screen. Refer to section 13.4.5.1, “QoS Filters—Edit Filter Rules.”

13.4.5.1 QoS Filters—Edit Filter Rules

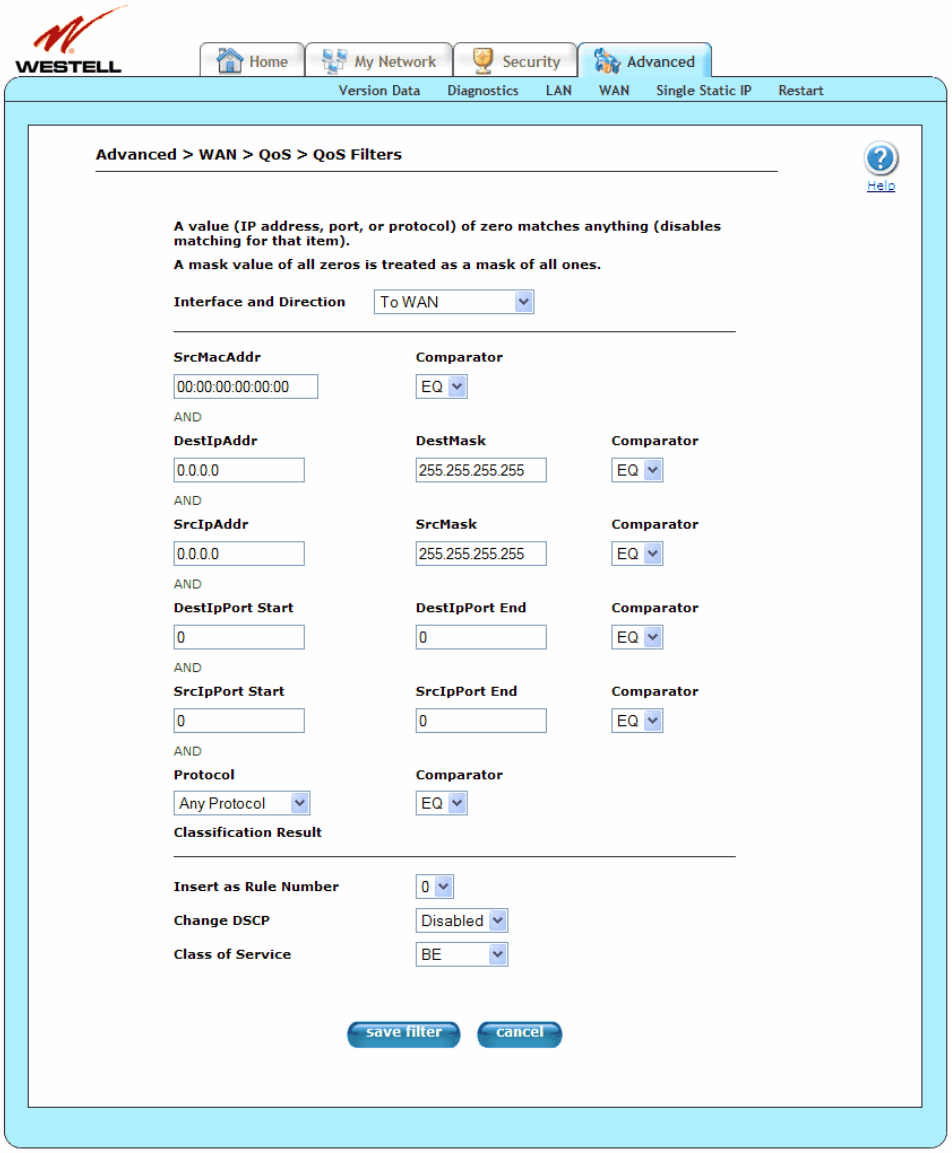
The following screen will appear if you click the **edit filter rules** button from the QoS screen (**Advanced > WAN > QoS > QoS Filters**). This screen allows you to edit any Internet Protocol QoS filters that have been created.



Rule	Displays the order in which rules are applied: Rule 0 is first.
Packet Interface	Displays direction of traffic where the rule will be applied.
Header	Displays the packet header attribute to be evaluated.
Value	Displays the value of the packet header attribute to be evaluated.
Mask	Displays the type of mask selected.
Comparator	Displays the type of comparison used.
delete	Click this button to delete a QoS Filter.
up	Click this button move a QoS Filter “Up” in priority.
down	Click this button to move a QoS Filter “Down” in priority.
new filter	Click this button to create a new QoS filter using the **QoS Filters** screen. Refer to section 13.4.5.2, “QoS Filters—New Filter.”
cancel	Click this button to return the screen to its previous settings.

13.4.5.2 QoS Filters—New Filter

The following screen will appear if you click the **new filters** button from the **QoS Filters** screen (**Advanced > WAN > QoS > QoS Filters**) from the main menu. This screen allows you to edit any Internet Protocol QoS filters that have been created. If you change the settings in this screen, click **save filter** and then **OK**. If you click **cancel**, the screen will return to its previous settings.

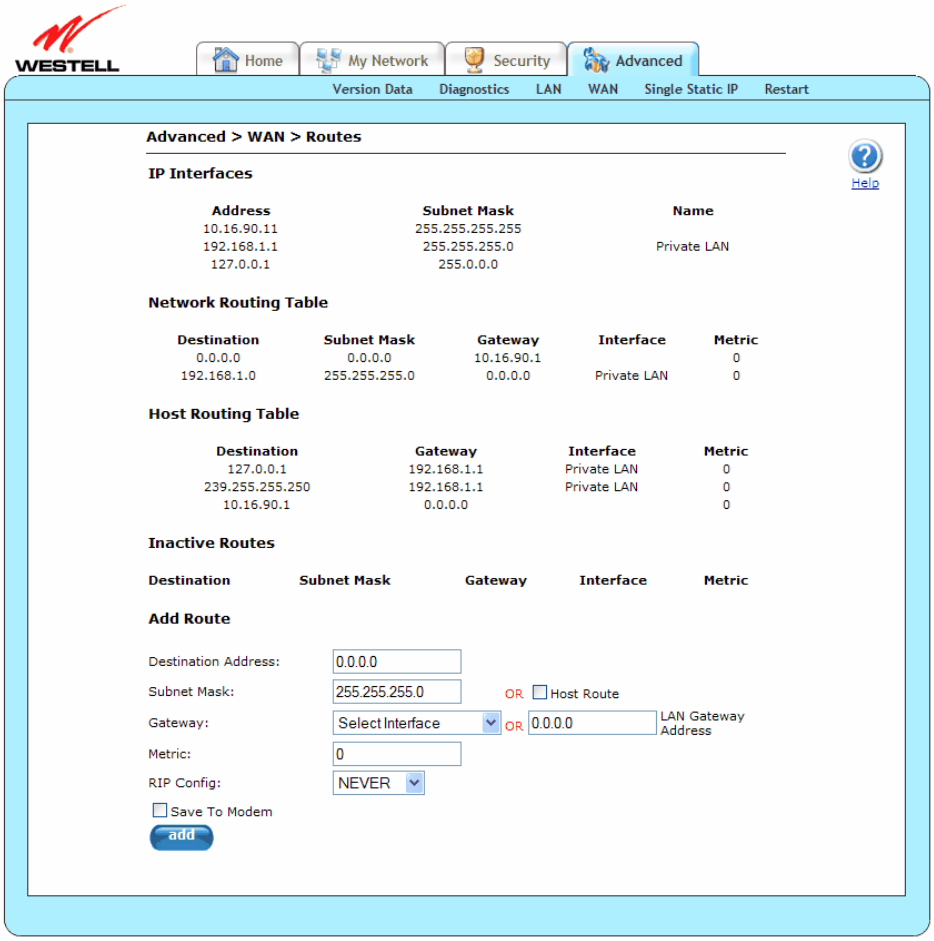


Interface and Direction	Click this drop-down menu to determine where the rule will be applied. Normally, all of the local ports (Ethernet and USB) are connected to bridge 0. Port mapping can be used to move ports to a different bridge. • To WAN: Applied to packets headed toward the WAN, after the packet is routed. • From WAN: Applied to packets coming from the WAN, before the packet is routed. • To Private LAN: Applied to packets headed toward the Private LAN, after the packet is routed. • From Private LAN: Applied to packets coming from the Private LAN, before the packet is routed. • To Public LAN: Applied to packets headed toward the Public LAN, after the packet is routed. • From Public LAN: Applied to packets coming from the Public LAN, before the packet is routed. • To Private LAN 2: Applied to packets headed toward the Private LAN2, after the packet is routed. • From Private LAN 2: Applied to packets coming from the Private LAN2, before the packet is routed.
SrcMacAddr	Displays MAC packet header source address.
Comparator	Click this drop-down menu to select the type of comparison to use. • EQ: MAC packet header destination address field is “Equal to.” • NE: MAC packet header destination address field is “Not Equal to.”
DestIpAddr	Displays the IP packet header destination address.
DestMask	Displays the IP packet header destination address “Mask” value. 0.0.0.0 is assumed to be 255.255.255.255.
SrcIpAddr	Displays the IP packet header source address.
SrcMask	Displays the IP packet header source address “Mask” value. 0.0.0.0 is assumed to be 255.255.255.255.
DestIpPort Start	Displays the IP packet header destination port start. Only matches UDP and TCP packets.
DestIpPort End	Displays the IP packet header destination port end. Only matches UDP and TCP packets.
SrcIpPort Start	Displays the IP packet header source port start. Only matches UDP and TCP packets.
SrcIpPort End	Displays the IP packet header source port end. Only matches UDP and TCP packets.
Protocol	Click this drop-down menu to select the protocol to be used. • Any Protocol • ICMP (1) • IGMP (2) • TCP (6) • UDP (17) • GRE (47) • IPSEC ESP (50) • IPSEC AH (51)
Insert As Number	Displays the order in which the rules are applied (0 is the highest).
Change DSCP	Click this drop-down menu to disable or enable the Change DSCP feature.

Class of Service	Click this drop-down menu to select the Class Of Service for this filter. • BE • AF1 • AF2 • AF3 • AF4 • EF • CS6 (NC) • CS7 (NC)
Save filter	Click this button to save the newly created filter.
cancel	Click this button to return the screen to its previous settings.

13.4.6 Routes

The following screen will appear if you select **Advanced > WAN > Routes** from the main menu. The **Routes** screen maintains the routes (or paths) of where specific types of data are routed across a network, listing the active interfaces on the modem and their IP address and mask: eth0 is the local LAN interface, and lo0 is the loopback interface. To add a route, type the appropriate values and/or select the desired options in this screen, and then click **add** to establish a static route.



IP Interfaces Lists the active interfaces on the modem, their IP address and subnet mask. eth0 is the local LAN interface. lo0 is the loopback interface.	
Address	Displays the IP interface address.
Subnet Mask	Displays the IP interface subnet address.
Name	Displays the IP interface device name: • eth0: local LAN interface. • lo0: loopback interface. • Main PPP: local WAN interface.
Network Routing Table Lists the network routes. These can be either routes for directly connected interfaces or static routes. Static routes have a **delete** button to allow for their removal. Static routes that have not been saved to flash also have a **save** button, which make the static route permanent. The 0.0.0.0 route is the default route; any packet with a destination not explicitly listed in the route table would be routed using the default route. Each route consists of a destination IP subnet, mask, gateway, interface, and metric.	
Destination	Displays the IP address or subnet of the route.
Subnet Mask	Displays the following: • If the route is a network route, Subnet Mask is used to specify the subnet address. • If the route is a host route, then the Host Route check box is used.
Gateway	Displays the IP address of the gateway.
Interface	Displays where to send the packet if it matches this route.
Metric	Displays the RIP metric to be assigned to this route if/when it is advertised using RIP. The metric is equivalent to the RIP metric 0-15; it is used to differentiate routes with the same address and mask. Lower metrics are preferred. The RIP column indicates whether a static route should be advertised via RIP.
Host Routing Table Lists host routes. A host route is an IP route with a 32-bit mask, indicating a single destination (as opposed to a subnet, which could match several destinations).	
Destination	Displays the IP address or subnet of the Route.
Gateway	Displays the IP address of the gateway.
Interface	Displays the where to send the packet if it matches this route.
Metric	Displays the RIP metric to be assigned to this route if/when it is advertised using RIP.
Inactive Routes Lists static routes whose interface is currently not in service.	
Inactive Routes	Displays static routes whose interface is currently not in service.
Destination	Displays the IP address or subnet of the Route.
Subnet Mask	Displays the following: • If the Route is a network route, Subnet Mask is used to specify the subnet address. • If the Route is a Host route, then the Host Route check box is used.
Gateway	Displays the IP address of the gateway.
Interface	Displays where to send the packet if it matches this route.
Metric	Displays the RIP metric to be assigned to this route if/when it is advertised using RIP. The metric is equivalent to the RIP metric 0-15; it is used to differentiate routes with the same address and mask. Lower metrics are preferred. The RIP column indicates whether a static route should be advertised via RIP.
Add Route Used to add a new static route in the modem.	
Destination Address	Displays the IP address or subnet of the Route.

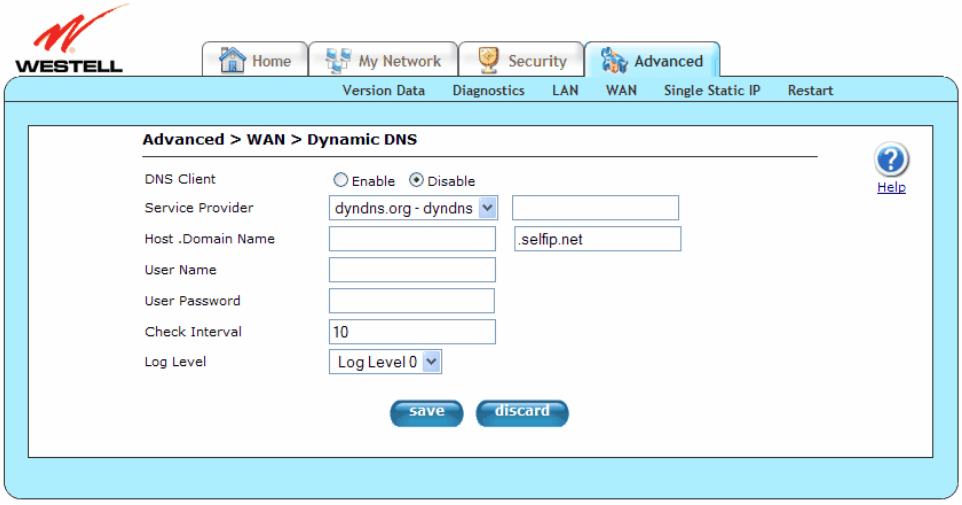
Subnet Mask/ Host Route	Displays the following: • If the Route is a network route, Subnet Mask is used to specify the subnet address. • If the Route is a Host route, then the Host Route check box is used.
Gateway/LAN Gateway Address	Click this drop-down menu to select the interface to use for sending the packet, if it matches this route. Only active gateways can be used to create a static route.
Metric	Displays the RIP metric to be assigned to this route if/when it is advertised using RIP. The metric is equivalent to the RIP metric 0-15; it is used to differentiate routes with the same address and mask. Lower metrics are preferred. The RIP column indicates whether a static route should be advertised via RIP.
RIP Config	Click this drop-down menu to select whether or not to advertise the static route, using RIP. (RIP must also be enabled before the route will be advertised.) • NEVER • ALWAYS
Save to Modem	If checked, then the route will be made permanent by saving it to flash memory. If not checked, the route will disappear the next time the modem restarts.
add	Click this button to add a newly created route.

13.4.7 Dynamic DNS

The following screen will appear if you select **Advanced > WAN > Dynamic DNS** from the main menu. Dynamic DNS allows a dynamic IP address to be aliased to a static hostname. For example, consider a situation where you're hosting a server on your modem's LAN and your modem receives a dynamic WAN IP address from your ISP. Without Dynamic DNS, if your WAN IP address changes, external users will have no way of knowing what your new WAN IP address is, and therefore, will not be able to access your server.

To address this situation, a number of companies (dynamic DNS ISPs) offer a service through which you may obtain a URL hostname for the server that you're hosting. This hostname is associated with the WAN IP address of your modem. The modem incorporates an "update client" that monitors for WAN IP address changes. If a change is detected, the update client notifies the dynamic DNS service provider of your new IP address. The dynamic DNS ISP then updates your DNS record by associating your new IP address to your hostname. Thus, external users access your server using your hostname and are unaffected by a change in your IP address.

If you change the settings in this screen, click **save** and then **OK**. If you click **discard**, the screen will return to its previous settings.



DNS Client	Click the option to enable or disable the DNS Client feature.
Service Provider	Click this drop-down menu to select a dynamic DNS service type. **Custom** allows for choosing a service not listed. • Dyndns.org – dyndns • Dyndns.org – statdns • Dyndns.org – custom • Zoneedit.com • No-ip.com • Custom: Allows you to add a service not included in the drop-down menu.
Host Name	Displays the name the dynamic DNS client is registered with. This defaults to the unique part of the MAC address and should not be changed.
Domain Name	Displays the name the dynamic DNS client is registered with. This defaults to a dyndns.org free domain.
User Name	Displays the name for the account registered with the dynamic DNS client service provider.
User Password	Displays the user password for the account registered with the dynamic DNS client service provider.
Check Interval	Displays how often the IP is checked (in minutes). Minimum is 10 min. Maximum is about 10 days.
Log Level	Click this drop-down menu to set the verbose debug level recorded in the syslog.

To configure Dynamic DNS (Service), please follow these steps:

1. Check **Enable** to enable the dynamic DNS client or **Disable** to disable the dynamic DNS client.
2. Choose the **Service Provider** from the drop-down menu.
3. Type the **Host Name** in the provided field.
4. Type the **Domain Name** in the provided field.
5. Type the **User Name** in the provided field.
6. Type the **User Password** in the provided field.
7. Type the **Check Interval** in the provided field.
8. Choose the **Log Level** from the drop-down menu.
9. Click **Save** to save the settings.

Congratulations! You have successfully configured Dynamic DNS.

13.5 Single Static IP

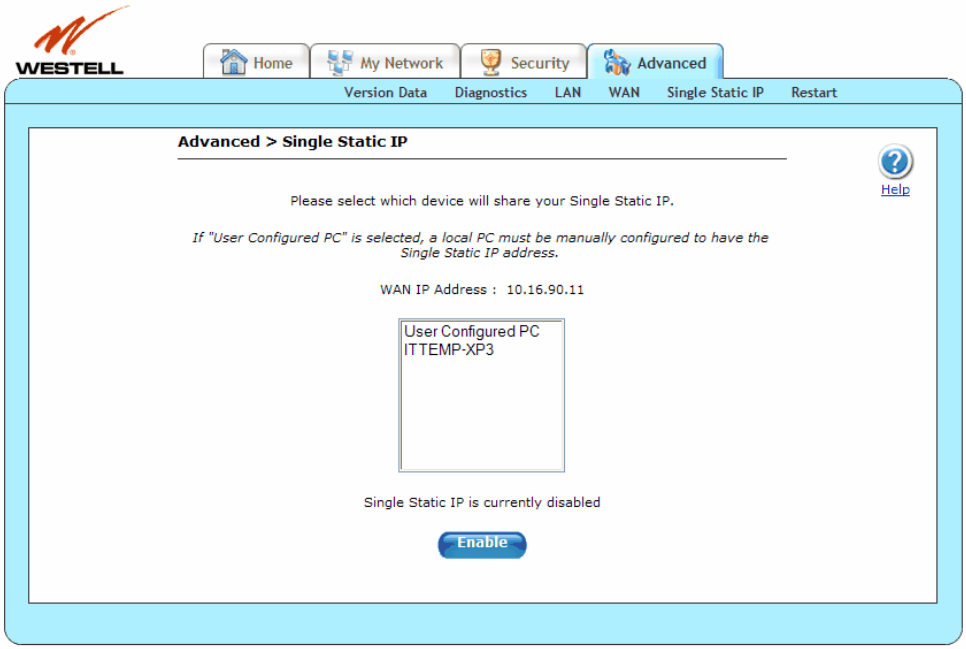
The following screen will appear if you select **Advanced > Single Static IP** from the main menu. This screen contains the settings that allow the PPP address received from the network to be propagated to a single LAN device behind the modem.

Single Static IP (SSI) allows you to select one device on your LAN that will share the WAN assigned IP address. By doing this, the device with the SSI becomes visible on the Internet. Network Address Translation (NAT) and Firewall rules do not apply to the device configured for SSI. If you are using Bridge (Routed Bridge) protocol, **Single Static IP** configuration will not be available.

IMPORTANT:

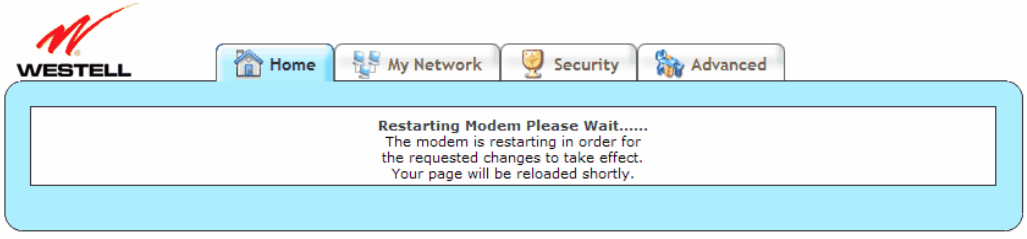
1. Before you begin this section, configure your PC settings to obtain an IP address from your modem automatically. If needed, refer to your computer's Windows help screen for instructions.

2. If you have previously enabled Public LAN, you will need to disable Public LAN and enable the DHCP for Private LAN and the Private LAN settings before you configure Single Static IP.
3. Static NAT and Single Static IP are mutually exclusive features. Static NAT should be disabled (if it has previously been enabled) before you enable **Single Static IP**. To disable Static NAT, select **Services** from the **Configuration** menu. Next, click the **static NAT** button. Select the device from the **Static NAT Device** drop-down menu and click **disable**. You can now configure Single Static IP.

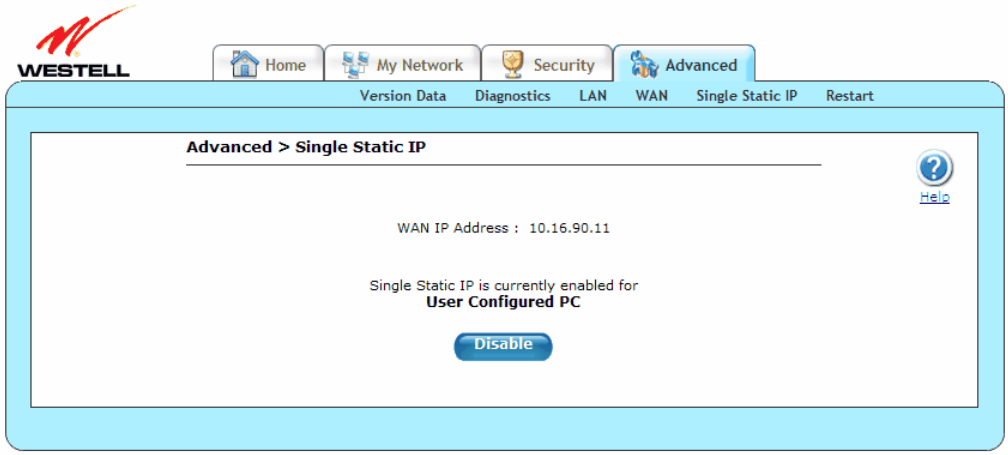


WAN IP Address	Displays the PPP IP address that the ISP has assigned the modem.
Selection box	Displays the devices available to share the Single Static IP address the ISP has assigned the modem. The names listed in the select box will be populated by the modem's DHCP server based on DHCP requests. If a device's name cannot be determined, the current IP address of the device will be placed in the list. • When the feature is enabled, the active machine will be highlighted in the select box and displayed at the bottom of the screen with the **Disable** button. • When the feature is disabled, no device in the select box will be highlighted, and the **Enable** button will be available. • When **User Configured PC** is selected, a local PC must be configured manually with the WAN IP address as its Ethernet adapter's IP address.

To enable Single Static IP, select a device that will share your Single Static IP from the options listed in the selection box, click **Enable** and then **OK**. Your modem will be reset, and the new configuration will take effect.



After a brief delay, the **Home** screen will appear. Confirm that you have a DSL sync and that your PPP session displays UP. (If necessary, click **connect** in the **Home > Connection Overview** screen to establish a PPP session). Select **Advanced > Single Static IP** to confirm that Single Static IP has been enabled, as shown in the following screen.



IMPORTANT: After you enable Single Static IP, reboot your computer to allow the changes to take effect.

NOTE: If you chose to enable **User Configured PC**, wait for the modem to reset, and then manually type the WAN IP, Gateway, and Subnet mask addresses you obtained from your ISP into a PC.

To disable Single Static IP, select a device that will share your Single Static IP from the options listed in the window, click **Disable** and then **OK**. Your modem will be reset, and the new configuration will take effect.

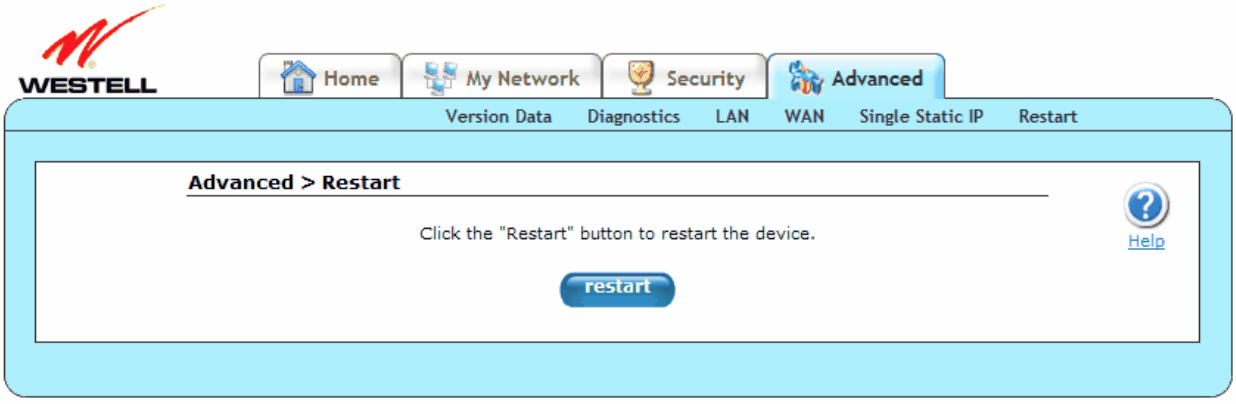
After a brief delay, the **Home** screen will appear. Confirm that you have a DSL sync and that your PPP session displays UP. (If necessary, click **connect** in the **Home > Connection Overview** screen to establish a PPP session). Select **Advanced > Single Static IP** to confirm that Single Static IP has been disabled.

13.6 Restart

The following screen will appear if you select **Advanced > Restart** from the main menu. This screen is used for performing a device restart while retaining the device's current configuration settings. Clicking the **restart** button is functionally equivalent to physically turning the power off and on to the device. Restarting may be useful for recovering from situations where the device is performing abnormally.

After you click **Restart**, please wait a brief moment while the modem is restarting. Refer to section 13.2.1, "Backup/Restore," for related information on backing up and restoring your modem.

NOTE: If you reset the modem to factory default settings, you will need to log in to the modem again to access the modem's Web pages and establish your Internet connection as explained in section 7, "Accessing Your Modem."



14. TECHNICAL SUPPORT INFORMATION

Contact your Internet service provider for technical support.

15. PRODUCT SPECIFICATIONS

System Requirements for 10/100 Base-T/Ethernet

- Pentium® or equivalent class machines or higher
- Microsoft® Windows® (Vista™, XP, 2000) Macintosh® OS X, or Linux installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- 10/100 Base-T Network Interface Card (NIC)
- Internet Explorer 5.5 or higher or Netscape Navigator 7.x or higher
- Computer Operating System CD-ROM

System Requirements for USB

- Pentium® or equivalent class machines or higher
- Microsoft® Windows® (Vista™, XP, 2000) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- USB Version 1.1 or higher compliant bus
- Internet Explorer 5.5 or higher or Netscape Navigator 7.x or higher
- Computer operating system CD-ROM

LEDs

- Power
- Ethernet
- USB
- DSL
- Internet

Connectors

- DSL: 6-pin RJ-11 modular jack-DSL
- Ethernet: 8-pin RJ-45 modular jack
- Power: Barrel connector

Power

- Power Supply: External 120 VAC (10%) to 12 VDC wall-mount power supply, small form factor
- Energy Star® qualified
- Power Consumption: Less than 3 watts typical, from 120 VAC

Dimensions

- Height: 1.21 in. (3.07 cm)
- Width: 4.0 in (10.16 cm)
- Depth: 3.88 in. (9.86 cm)

Weight

- Approx. 0.25 lb (0.11 kg)

Environmental

- Ambient Operating Temperature: +32 to +104 °F (0 to +40 °C)
- Relative Humidity: 5 to 95%, non-condensing

Certification

- EMC FCC, Part 15 Class B
- UL 60950, 3rd Edition
- ACTA 968-A

16. SOFTWARE LICENSE AGREEMENT

READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY. THIS SOFTWARE IS COPYRIGHTED AND LICENSED (NOT SOLD). BY INSTALLING AND OPERATING THIS PRODUCT, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE SOFTWARE AND HARDWARE TO WESTELL TECHNOLOGIES, INC. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND WESTELL TECHNOLOGIES, INC. (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

1. License Grant. Licensor hereby grants to you, and you accept, a nonexclusive license to install, execute and otherwise use the Compact Disk (CD) and the computer programs contained therein in machine-readable, object code form only (collectively referred to as the "SOFTWARE"), and the accompanying User Documentation, only as authorized in this License Agreement. Unless otherwise indicated, SOFTWARE excludes any "Third Party Software," as defined below. The SOFTWARE may be used only in connection with the computers or systems using the products for which the SOFTWARE is provided. You agree that you will not assign, sublicense, transfer, pledge, lease, rent, or share your rights under this License Agreement, except that you may transfer the SOFTWARE together with the product and the User's Manual to any third party if you uninstall the SOFTWARE from your system and transfer all copies of the SOFTWARE CD. You agree that you may not nor allow others to reverse assemble, reverse compile, or otherwise translate the SOFTWARE.You may retain the SOFTWARE CD for backup purposes only. In addition, you may make one copy of the SOFTWARE in any storage medium for backup purposes only. You may make one copy of the User's Manual for backup purposes only. Any such copies of the SOFTWARE or the User's Manual shall include Licensor's copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the SOFTWARE or any portions thereof may be made by you or any person under your authority or control.

2. Licensor's Rights. You acknowledge and agree that the SOFTWARE and the User's Manual are proprietary products of Licensor protected under U.S. copyright law. You further acknowledge and agree that all right, title, and interest in and to the SOFTWARE and the User's Manual, including associated intellectual property rights, are and shall remain with Licensor. This License Agreement does not convey to you an interest in or to the SOFTWARE, but only a limited right of use revocable in accordance with the terms of this License Agreement.

3. License Fees. The fees paid by you for the accompanying product are paid in partial consideration of the licenses granted to the SOFTWARE under this License Agreement.

4. Term. This License Agreement is effective upon your opening of this package and shall continue until terminated. You may terminate this License Agreement at any time by returning the SOFTWARE and all copies thereof and extracts therefrom to Licensor. Licensor may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Licensor, you agree to return to Licensor the SOFTWARE and all copies and portions thereof.

5. Limitation of Liability. Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the amounts paid to Licensor for the use of the SOFTWARE. In no event shall Licensor be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if Licensor has been advised of the possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

6. Governing Law. This License Agreement shall be construed and governed in accordance with the laws of the State of Illinois. You agree to submit to, and do hereby submit to, the jurisdiction of the state and federal courts of the state of Illinois and agree that venue is proper in those courts with regard to any litigation arising under this Agreement.

7. Costs of Litigation. If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses of litigation.

8. Severability. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof.

9. No Waiver. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

10. Third Party Software. You acknowledge that the CD may also include third-party computer programs and documentation ("Third Party Software"). Third Party Software, and your use of Third Party Software, is subject the terms of the license agreement included with the programs. You acknowledge that Third Party Software is provided to you as a convenience, and Licensor is not responsible for the content, quality or any liability arising from your use of Third Party Software. To the fullest extent possible, Licensor shall transfer to you all rights and warranties in the Third Party Software. In all other cases, Third Party Software is provided "AS IS, WHERE IS" WITHOUT WARRANTY OF ANY KIND, AND ANY USE OF THE SOFTWARE IS AT YOUR OWN RISK. TO THE FULLEST EXTENT PERMITTED BY LAW, LICENSOR DISCLAIMS ALL LIABILITY WITH RESPECT TO THIRD PARTY SOFTWARE.

17. PUBLICATION INFORMATION

Westell ProLine G90 DSL Modem (Models 6100, 6110)
Document Part Number 030-300564 Rev. A