



WESTELL
MEDIA GATEWAY™ (MODEL WMT)

USER GUIDE

DRAFT 1

TABLE OF CONTENTS

1. PRODUCT DESCRIPTION	4
2. SAFETY INSTRUCTIONS	4
3. CARING FOR YOUR MEDIA GATEWAY	4
4. REGULATORY INFORMATION	5
4.1 FCC Compliance Note	5
4.2 Canada Certification Notice	Error! Bookmark not defined.
5. NETWORKING REQUIREMENTS	7
6. HARDWARE FEATURES	8
6.1 LED Indicators	8
7. INSTALLING THE HARDWARE	9
7.1 Installation Requirements	9
7.2 Before you begin	9
7.3 Hardware Installations	10
8. CONFIGURING MEDIA GATEWAY FOR INTERNET CONNECTION	13
8.1 Setting Up an Account Profile	13
8.2 Establishing a PPP Session	18
8.3 Disconnecting a PPP Session	20
9. SETTING UP MACINTOSH OS X	22
10. SETTING UP ADVANCED CONFIGURATION	26
11. HOME	27
11.1 Adding Account Profiles	28
11.2 Editing Account Profiles	29
12. STATUS	31
12.1 Connection Summary	31
12.2 About	32
13. CONFIGURATION	33
13.1 Single Static IP – Single IP Address PassThrough	33
13.2 Service Configuration	38
13.3 Firewall Configuration	50
13.4 Wireless Configuration	54
13.5 Advanced LAN	60
13.6 Advanced WAN	76
14. SETTING UP ADVANCED SERVICE CONFIGURATION	90
14.1 Port Forwarding Ranges of Ports	91

14.2	Adding Port Forwarding Ports	91
14.3	Port Forwarding Trigger Ports	92
14.4	Adding Local Trigger Ports	93
14.5	Static NAT	94
14.6	Enabling Static NAT	95
14.7	Disabling Static NAT	96
15.	MAINTENANCE	98
15.1	Backup/Restore	98
15.2	Firewall Log	99
15.3	Administrative Password	101
15.4	Remote Access	102
15.5	Update Device	103
16.	TROUBLESHOOTING	108
16.1	System Self Tests	108
16.2	Diagnostic Logs	110
16.3	Statistics	114
16.4	Wireless Statistics	116
16.5	Status	118
17.	NAT SERVICES	124
18.	TECHNICAL SUPPORT INFORMATION	128
19.	PRODUCT SPECIFICATIONS	128
20.	SOFTWARE LICENSE AGREEMENT	129
21.	PUBLICATION INFORMATION	131

1. PRODUCT DESCRIPTION

The Westell® Media Gateway Communications Subsystem provides reliable, high-speed, Internet access to your existing phone line. Installation is easy ... no tools ... no headaches. Simply connect the hardware, apply power, and perform the simple software configuration for the Media Gateway and you are on the Internet.

The Media Gateway is capable of data rates hundreds of times faster than a traditional analog modem. But unlike analog modems, the Media Gateway 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. The Media Gateway supports a variety of networking interfaces such as wireless 802.11b/g and Ethernet.

Note: Hereafter, the Westell Media Gateway™ Communications Subsystem will be referred to as “Media Gateway,” “Gateway,” or “Modem.”

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. CARING FOR YOUR MEDIA GATEWAY

Please follow these guidelines to ensure the best use of your Media Gateway.

- ⌘ When using Stylus pen (Media Gateway in iobi mode), please be sure to gently tap the components in the LCD screen to navigate to various Iobi features.
- ⌘ **DO NOT** use a pen, pencil or other pointed object on the LCD screen as these items may cause damage to the screen. Always use the point of the Stylus for tapping on the LCD screen and making selections.
- ⌘ Warning: **DO NOT** use an abrasive cleaner on the LCD screen as this will damage the screen. **If the LCD becomes soiled, use a damp, clean cloth moistened with a window-cleaning solution to gently wipe the screen.**

4. REGULATORY INFORMATION

4.1 FCC Compliance Note

(FCC ID: CH8A90WMT-00)

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.

Modifications made to the product could void the users' right to operate the equipment.

PART 68 - COMPLIANCE REGISTRATION

This equipment (Model WMT) 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 not 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 (Model WMT) 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.

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 (Model WMT) 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.

5. NETWORKING REQUIREMENTS

The following system specifications are required for optimum performance of the Media Gateway via 10/100 Base-T Ethernet or Wireless installations.

CONNECTION TYPE	MINIMUM SYSTEM REQUIREMENTS
10/100 Base-T ETHERNET	<ul style="list-style-type: none"> ⌘ Pentium® or equivalent class machines ⌘ Microsoft® Windows® (98 SE, ME, NT 4.0, 2000, or XP) Macintosh® OS X, or Linux installed ⌘ 64 MB RAM (128 MB recommended) ⌘ 10 MB of free hard drive space ⌘ TCP/IP Protocol stack installed ⌘ 10/100 Base-T Network Interface Card (NIC) ⌘ Computer Operating System CD-ROM on hand
WIRELESS IEEE 802.11g	<ul style="list-style-type: none"> ⌘ Pentium® or equivalent class machines ⌘ Microsoft® Windows® (98 SE, ME, 2000, or XP) or Macintosh® OS X installed ⌘ Computer Operating System CD-ROM on hand ⌘ Internet Explorer 4.x or Netscape Navigator 4.x or higher ⌘ 64 MB RAM (128 MB recommended) ⌘ 10 MB of free hard drive space ⌘ An available IEEE 802.11b/g PC adapter

6. HARDWARE FEATURES

6.1 LED Indicators

This section describes the LED indicators located on the front of the Media Gateway. The LEDs described in this section are used to verify the unit's operation and status. Refer to the following chart for details on the LEDs.

LED States and Descriptions

LED	State	Description
POWER	Solid Green	Media Gateway power is ON.
	OFF	Media Gateway power is OFF.
	Solid Red	CS 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 (E1/WAN, E2, E3, E4)	Solid Green	Powered device is connected to one or more of the Ethernet ports (includes devices with wake-on LAN capability where slight voltage is supplied to an Ethernet connection).
	OFF	Communication Subsystem power is OFF, no cable or no powered device is connected to the Ethernet ports.
WIRELESS	Solid Green	Link Established.
	OFF	Media Gateway power is OFF or No Link.
INTERNET	Solid Green	IP connected (the Subsystem has a WAN IP address from IPCP or DHCP, or a static IP address is configured. PPP negotiation has successfully completed.
	Solid Red	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.).
	OFF	Media Gateway power is OFF, Media Gateway is in Bridge Mode, or an Internet connection is not present.
LINE IN USE	Solid Blue	Indicates telephone is in use (off-hook)
	OFF	Indicates telephone is not in use (on-hook)

NOTE: Safe Boot is reflected when the Power and Internet LED's are both Red and all other LED's are off.

7. INSTALLING THE HARDWARE

7.1 Installation Requirements

To install the Media Gateway, you will need the following:

- € A Network Interface Card (NIC) installed in your PC, or
- € An IEEE 802.11b/g adapter

7.2 Before you begin

Make sure that your kit contains the following items:

- € Media Gateway Base Unit
- € Power Supply
- € RJ-45 Ethernet cable (straight-through) (yellow)
- € RJ-11 Phone cable
- € Cordless Handset and Battery
- € Base Unit Stand
- € Stylus
- € Media Gateway CD-ROM
- € Quick Start Guide


7.3 Hardware Installations

NOTE: If you are using Your Media Gateway in conjunction with an Ethernet Hub or Switch, refer to the manufacturer's instructions for proper installation and configuration. **Westell recommends the use of a surge suppressor to protect equipment attached to the AC power supply.**

7.3.1 Installation via 10/100 Base-T Ethernet



NOTE: Before you connect via 10/100 Base-T, you must have an available Ethernet card installed in your computer. If your Ethernet card does not auto-negotiate, you must set it to half duplex. Refer to the Ethernet card manufacturer's instructions for installing and configuring your Ethernet card.

1. Connect the yellow Ethernet cable from the Ethernet (E2, E3, or E4) jacks marked  on the rear panel of the base unit to the Ethernet port on your computer. Repeat this step to connect up to two additional PCs to the Media Gateway.

NOTE: You may connect to any of the three Ethernet (E2, E3, or E4) jacks on the rear panel of the Media Gateway base unit as they serve as an Ethernet switch.

2. Connect the DC 12V power supply cord to the power connector marked **12V AC~** on the rear panel of the base unit. Plug the other end of the power supply into an AC wall socket, and then turn on the power switch (if it is not already turned on).
3. Check to see if the Power LED is solid green. If the Power LED is solid green, the base unit is powered up.
4. Check to see if the Ethernet LED on the base unit is solid green. Solid green indicates that the Ethernet interface is functioning properly.
5. After you have completed section 8 of this document and established an Internet connection, the Internet LED will be solid green. If this LED is not solid green, please refer to your ISP's instructions for establishing an Internet connection or to section 6.1 (LED Indicators) of this document for information on the LEDs.

Congratulations! You have completed the Ethernet hardware installation. Proceed to section 8 to configure your Media Gateway for an Internet connection.

7.3.2 Connecting PCs via Wireless

IMPORTANT: If you are connecting to your Media Gateway via a wireless network adapter, the SSID must be the same for both the Media Gateway and your PC's wireless network adapter. The default SSID for Media Gateway is the serial number of the unit (located below the bar code on the bottom of the unit and also on the Westell shipping carton). Locate and run the utility software provided with your PC's Wireless network adapter and enter the SSID value. The PC's wireless network adapter must be configured with the SSID (in order to communicate with the Media Gateway) before you begin the account setup and configuration procedures. Later, for privacy, you can change the SSID by following the procedures outlined in section 13.4 (Wireless Configuration).

NOTE: Client PCs can use any Wireless Fidelity (Wi-Fi) 802.11b/g certified card to communicate with the Media Gateway. The Wireless card and Media Gateway must use the same Wired Equivalent Privacy (WEP) security code type. The factory default for WEP is DISABLED. If you enable WEP, you must ensure the network setting for your wireless adapter is set to "Must Use Shared Key for WEP" or "Open Wi-Fi." You must ensure that your PC's Wi-Fi adapter is configured properly for whichever network setting you use. You can access the settings in the advanced properties of the wireless network adapter.

To network Media Gateway using a wireless installation, you will need to confirm the following:

1. Ensure that an 802.11b/g wireless network adapter has been installed in the PC on your wireless network.
2. Install the appropriate drivers for your Wireless IEEE802.11b or IEEE802.11g adapter used with your PC.
3. Connect the DC 12V power supply cord to the power connector marked **12V AC~** on the rear panel of the base unit. Plug the other end of the power supply into an AC wall socket, and then turn on the power switch (if it is not already turned on).
4. Check to see if the Power LED is solid green. If the Power LED is solid green, the base unit is powered up.
5. Check to see if the Wireless LED is solid Green. This means that the Wireless interface is functioning properly.
6. After you have completed section 8 of this document and established an Internet connection, the Internet LED will be solid green. If this LED is not solid green, please refer to your ISP's instructions for establishing an Internet connection or to section 6.1 (LED Indicators) of this document for information on the LEDs.


NOTE: After you have initially connected Media Gateway using a wireless installation, you can network the Media Gateway to additional computers in your home or office by completing steps 1 and 2 in this section for each PC that you want on your wireless network.

Congratulations! You have completed the Wireless installation for the Media Gateway. You must now go to section 8 to configure Media Gateway for an Internet connection.

7.3.3 Ethernet and Wireless Combination Installation

Media Gateway supports simultaneous use of 10/100 Base-T Ethernet and Wireless configurations. The following instructions explain how to install Media Gateway for simultaneous use of Ethernet and Wireless ports.

NOTE: Refer to section 7.3.1 and 7.3.2 for instructions on hardware installation via Ethernet and Wireless connections, respectively.

1. Ensure that an 802.11b/g wireless network adapter has been installed in the PC on your wireless network.
2. Install the appropriate drivers for your Wireless IEEE802.11b or IEEE802.11g adapter used with your PC.
3. Connect the yellow Ethernet cable from the Ethernet (E2, E3, or E4) jack marked  on the rear panel of the base unit to the Ethernet port on your computer. Repeat this step to connect up to two additional PCs to the base unit.

NOTE: You may connect to any of the three Ethernet (E2, E3, or E4) jacks on the rear panel of the Media Gateway base unit as they serve as an Ethernet switch.

4. Connect the DC 12V power supply cord to the power connector marked **12V AC~** on the rear panel of the base unit. Plug the other end of the power supply into an AC wall socket, and then turn on the power switch (if it is not already turned on).
5. Check to see if the Power LED is solid green. If the Power LED is solid green, the base unit is powered up.
6. Check to see if the Ethernet LED is solid green. Solid green indicates the Ethernet interface is functioning properly.
7. Check to see if the Wireless LED is solid Green. This means that the Wireless interface is functioning properly.
8. After you have completed section 8 of this document and established an Internet connection, the Internet LED will be solid green. If this LED is not solid green, please refer to your ISP's instructions for establishing an Internet connection or to section 6.1 (LED Indicators) of this document for information on the LEDs.

NOTE: After you have initially connected Media Gateway using a wireless installation, you can network Media Gateway to additional computers in your home or office by completing steps 1 and 2 in this section for each PC that you want on your wireless network.

Congratulations! You have completed the simultaneous hardware (Ethernet and Wireless) installation. You must now go to section 8 to configure Media Gateway for an Internet connection.

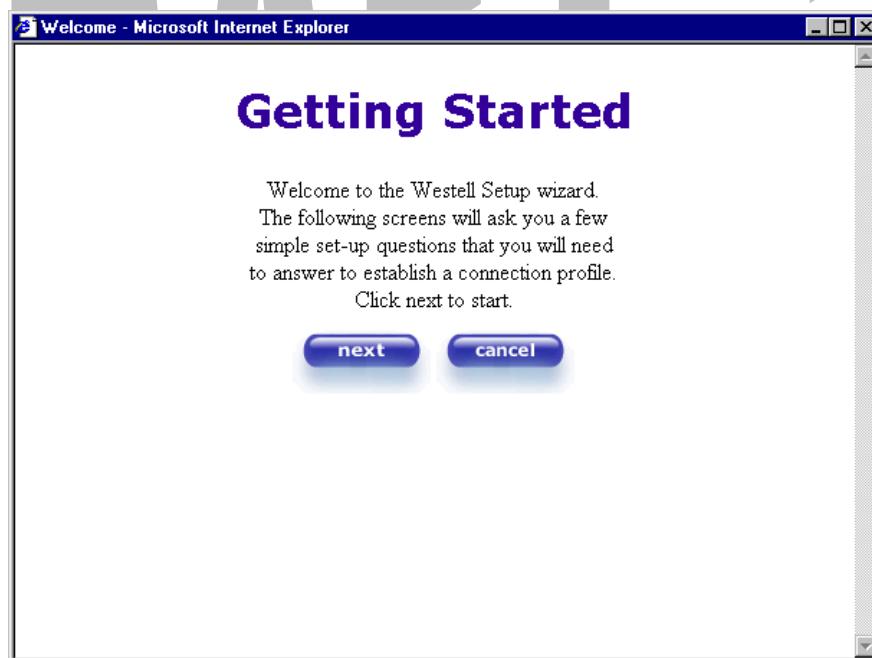
8. CONFIGURING MEDIA GATEWAY FOR INTERNET CONNECTION

To browse the Internet using your Media Gateway, you must set up your account profile and establish a PPP session with your ISP.

NOTE: The PPPoE protocol is often used to establish an Internet connection. However, if your Internet service provider does not support PPPoE, please refer to your service provider's instructions for establishing an Internet connection. If you are using PPPoE to establish your Internet connection, please following the instructions provided in this section.

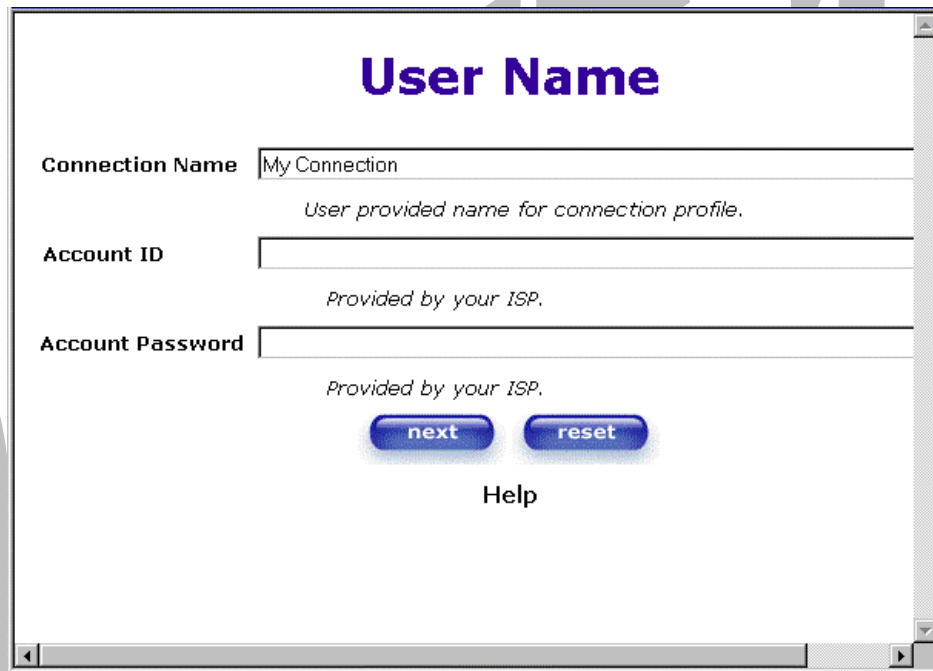
8.1 Setting Up an Account Profile

After you complete the hardware connection for your Media Gateway, power up the unit. Next, bring up your computer's Web browser and type **http://192.168.1.254** in the browser's address window, and then press **Enter** on your keyboard. The **Getting Started** screen will appear. Click on **next** to continue.



If you clicked on **Next**, the following screen will be displayed. This screen will allow you to set up your account profile.

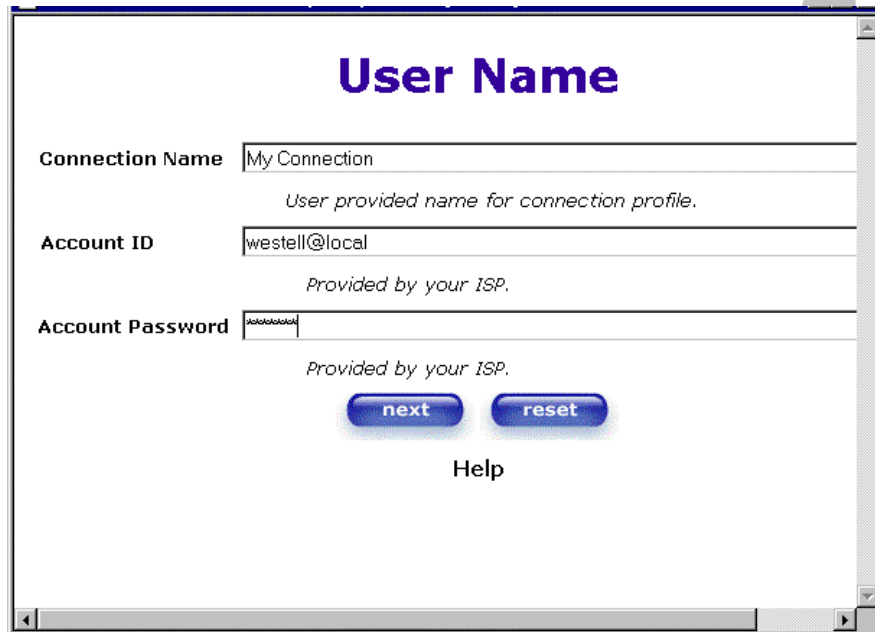
NOTE: Before you set up your account profile, you must obtain your **Account ID**, **Account Password**, and **VPI/VCI** values from your ISP. You will use this information when you set up your account parameters. If you are at a screen and need help, click on the **Help** button to learn more about the screen, or see section **Error! Reference source not found.** (Help) for additional information on the help messages.



Type in your account parameters. (Account parameters are required before connecting to the Internet.)
Account Parameters include:

- **Connection Name**-the Connection Name is a word or phrase that you use to identify your account. (You may enter up 64 characters in this field.)
- **Account ID**-the Account ID is provided by your ISP. (You may enter up 255 characters in this field.)
- **Account Password**-the Account Password is provided by your ISP. (You may enter up 255 characters in this field.)

When you enter your account parameters at the **User Name** screen, they will be displayed as shown in the screen below. Click **next** if you want your account parameters to take effect. Click on **reset** if you do not want the account parameters that you entered to take effect or if you want to re-enter the parameters.



The 'User Name' screen displays three input fields: 'Connection Name' with the value 'My Connection', 'Account ID' with the value 'westell@local', and 'Account Password' with masked characters. Below the fields are two buttons, 'next' and 'reset', and a 'Help' link.

User Name

Connection Name
User provided name for connection profile.

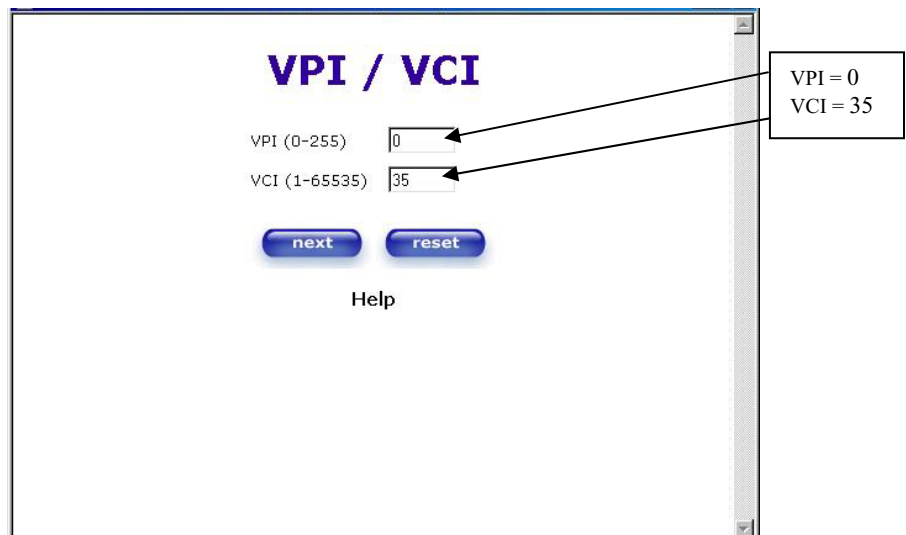
Account ID
Provided by your ISP.

Account Password
Provided by your ISP.

[Help](#)

Enter the VPI and VCI values (**0** for VPI and **35** for VCI default) you obtained from your ISP. Click on **next**.

NOTE: The **VPI/VCI** screen will come pre-configured and it will be displayed here. Do not change any values in this screen. Click **next** to go to the **PROTOCOL** screen.



The 'VPI / VCI' screen displays two input fields: 'VPI (0-255)' with the value '0' and 'VCI (1-65535)' with the value '35'. Below the fields are two buttons, 'next' and 'reset', and a 'Help' link. A callout box points to the VPI and VCI fields with the text 'VPI = 0' and 'VCI = 35'.

VPI / VCI

VPI (0-255)

VCI (1-65535)

[Help](#)

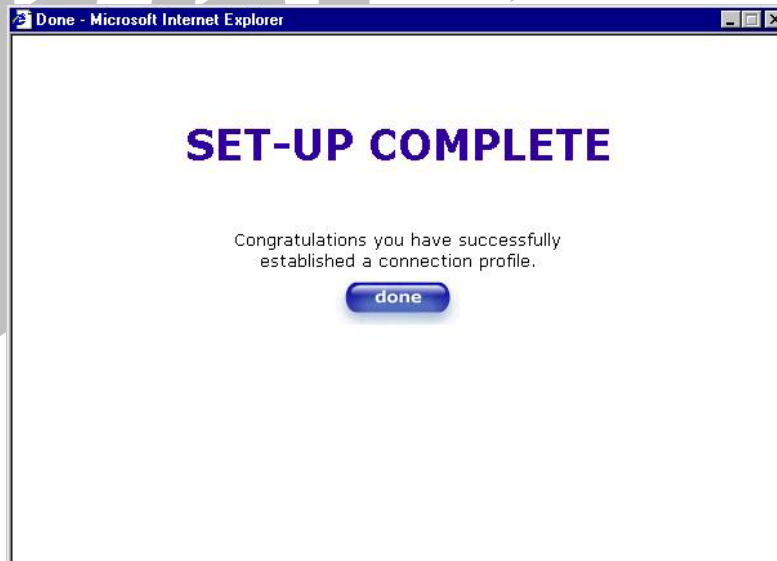
VPI = 0
VCI = 35

Select the Protocol type that you obtained from your ISP. Click on **next**.

NOTE: The **PROTOCOL** screen will come pre-configured and it will be displayed here. Click **next** to go to the **SET-UP COMPLETE** screen.

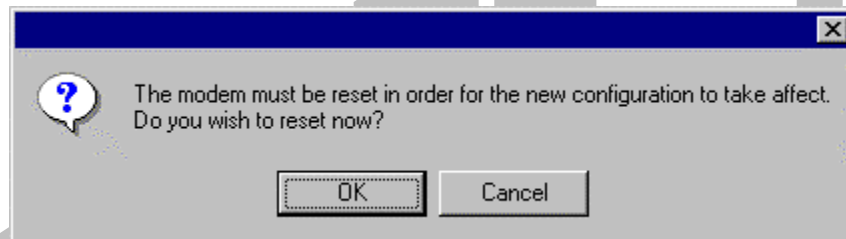


When the **SET-UP COMPLETE** screen appears, you have successfully completed your Account Profile setup. Click on **done**.

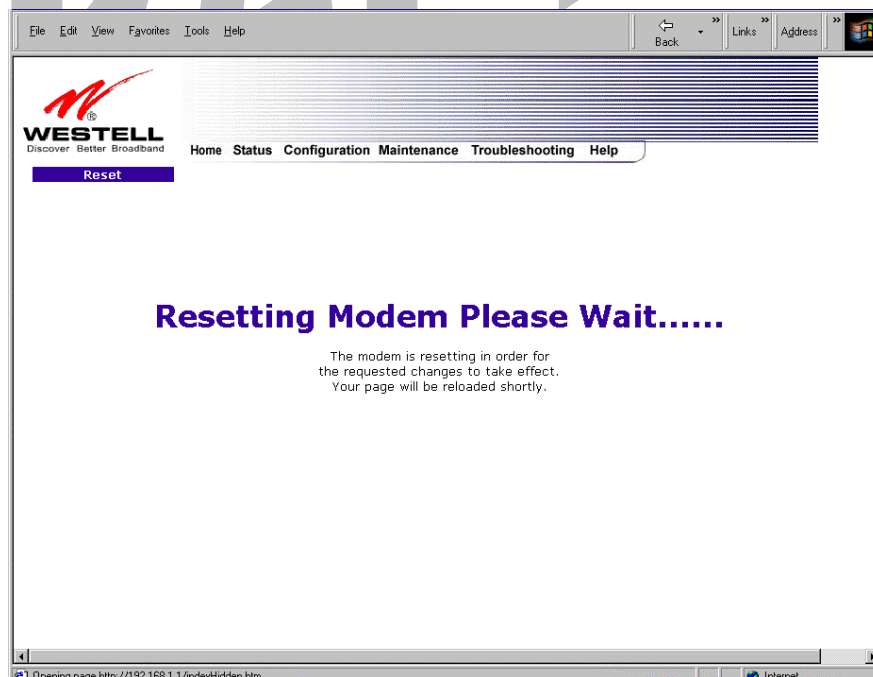


If you changed the **VPI/VCI** settings and clicked on **done** in the **SET-UP COMPLETE** screen, the following screen will appear. Click on **OK**.

NOTE: The following pop-up will appear only if you have changed the **VPI**, **VCI**, or **Protocol** values in the preceding screens. If you did not change any of these values, this pop-up screen will not appear and Media Gateway will not be reset. If the Media Gateway's connection setting is set to "Always On" and you have changed any of these values, Media Gateway will reset automatically. For instructions on editing your connection settings, see section 11.2.



If you clicked on **OK**, the following screen will be displayed. Media Gateway will be reset and the new configuration will take effect.

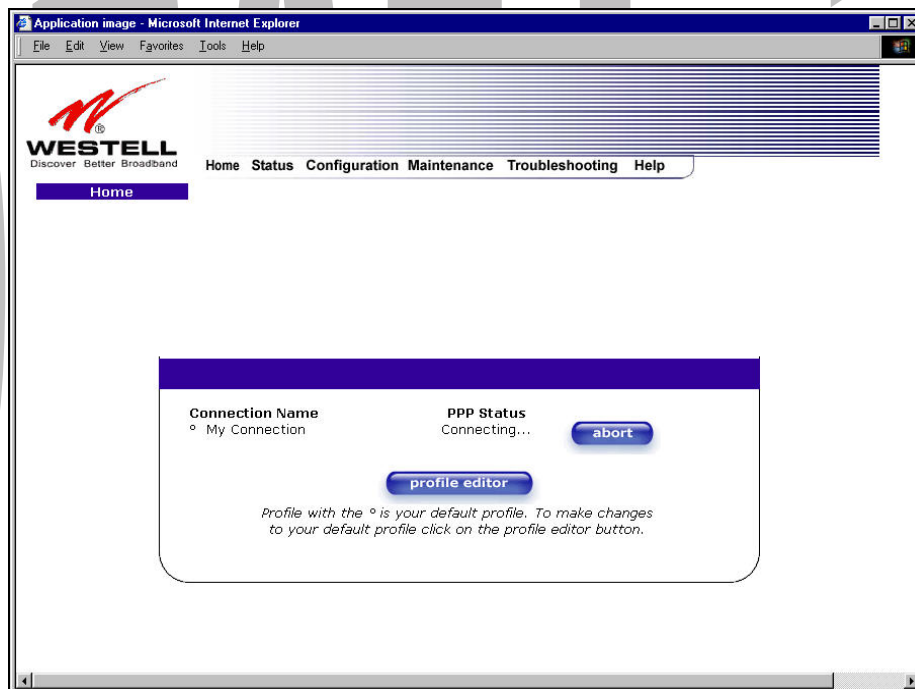


8.2 Establishing a PPP Session

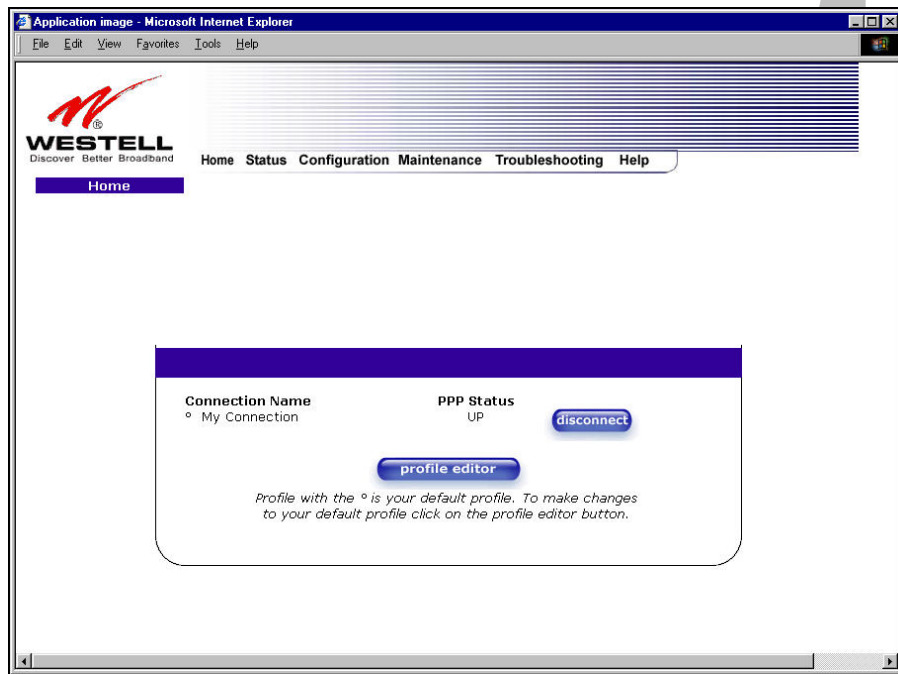
View the **PPP Status** at the Home page. If the PPP Status displays **DOWN**, click the **Connect** button to establish a PPP session.

NOTE: Whenever the PPP Status displays **DOWN**, you do not have a PPP session established. If the Media Gateway's connection setting is set to "Always On" or "On Demand," after a brief delay the PPP session will be established automatically and the PPP Status will display **UP**. If the connection setting is set to "Manual," you must click on the **Connect** button to establish a PPP session. Once the PPP session has been established (PPP Status displays **UP**), you may proceed with the Media Gateway's configuration. Section 11.2 provides instructions on editing the connection settings. (Refer to the 'Edit My Connection' screen.) The Media Gateway's factory default connection setting is "Manual."

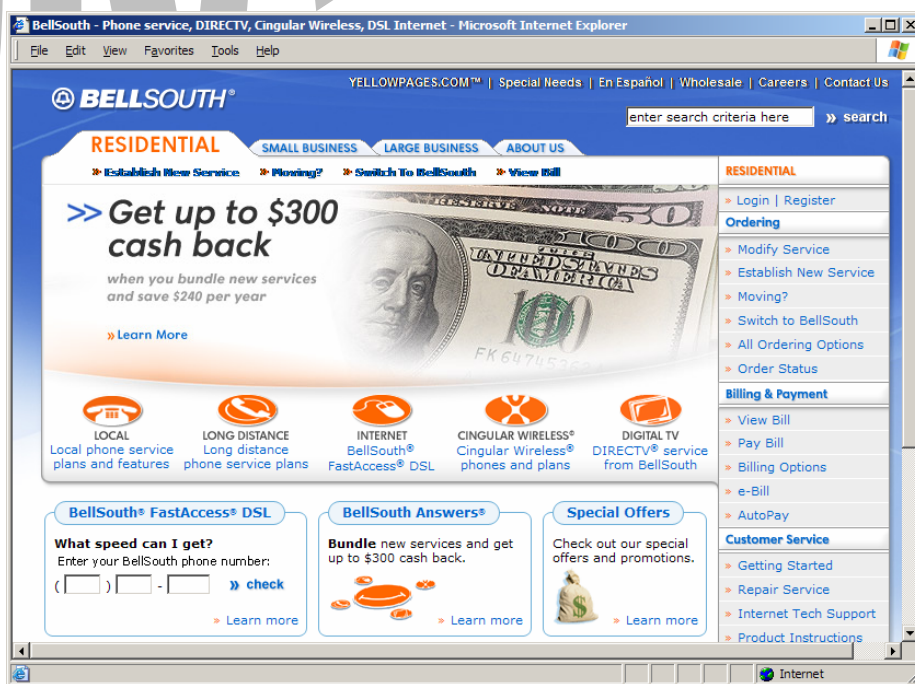
If you click the **Connect** button, the following screen will appear briefly. The **PPP Status** in the **Connection Overview** window allows you to view the state of your Media Gateway connection. When the **PPP Status** displays **Connecting...**, this means that you are establishing a PPP session.



After a PPP session has been established, the **PPP Status** will display **UP**. Congratulations! You may now browse the Internet.



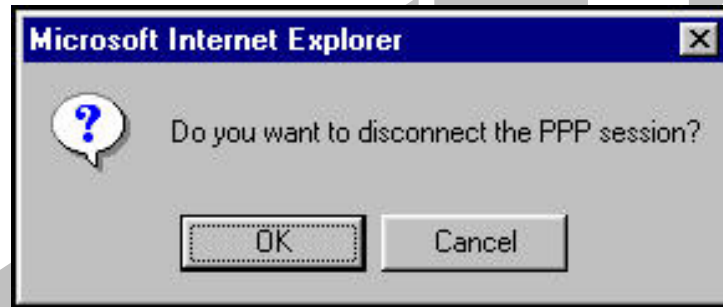
For example, if you want to visit BellSouth's home page, type **http://www.bellsouth.com** in your browser's address window.



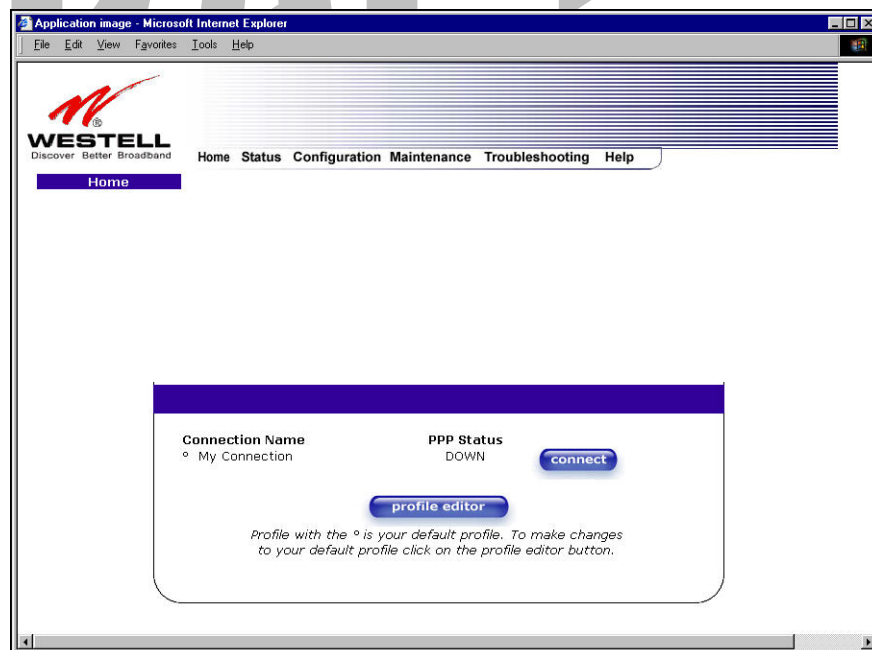
8.3 Disconnecting a PPP Session

If you have finished browsing the Internet and want to disconnect from your PPP session, click on the **Disconnect** button in the **Connection Overview** screen (the preceding screen). The following pop-up screen will appear. Click on **OK** to disconnect the PPP session.

Warning: If you disconnect the PPP session, this will disconnect Media Gateway from the Internet, and all computers on the LAN will be disconnected until the PPP session is re-established.



If you clicked the **Disconnect** button in the preceding **Connection Overview** screen, the **PPP Status** should display **DOWN**. This means that you no longer have a PPP session (no IP connection to your ISP).



When you are ready to re-establish a PPP session, click on the **connect** button.

NOTE: When you are ready to exit the Gateway's interface, click on the **X** (close) in the upper-right corner of the window. Closing the window will not affect your PPP Status (your PPP session will not be disconnected). You must click the **disconnect** button to disconnect your PPP session. When you are ready to restore the Media Gateway interface, you must launch your Internet browser and type **http://192.168.1.254/** in the browser's address window and press **Enter** on your keyboard.

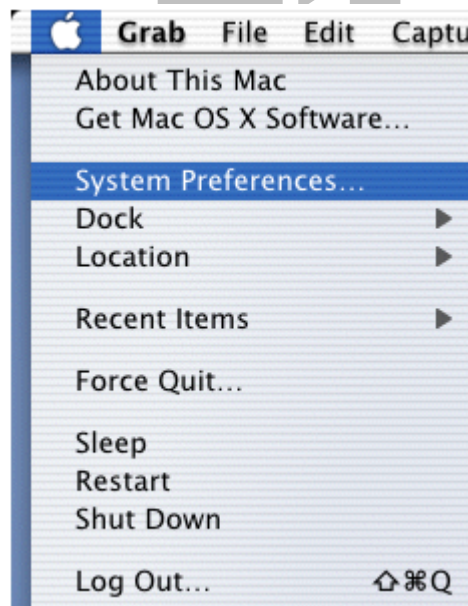
DRAFT 1

9. SETTING UP MACINTOSH OS X

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

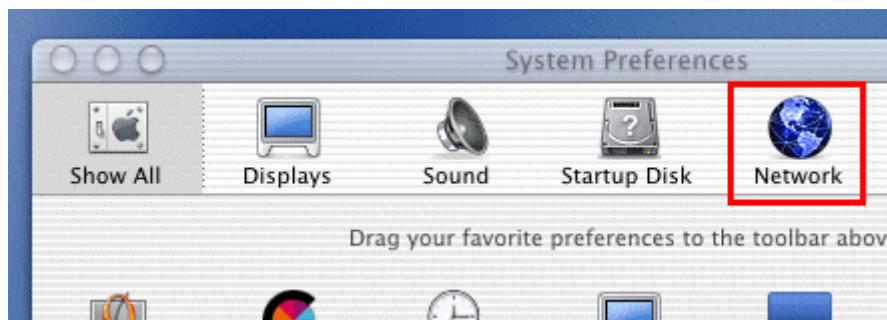
Open the System Preference Screen

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



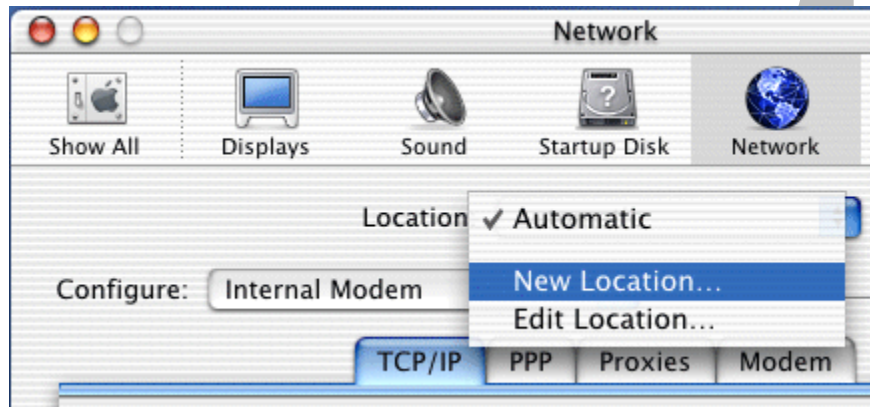
Choose the Network Preferences

After selecting **System Preferences...**, from the previous screen, the **System Preferences** screen will be displayed. From the **System Preferences** screen, click on the **Network** icon.



Create a New Location

After selecting the **Network** icon at the **System Preferences** screen, the **Network** screen will be displayed. Select **New Location** from the **Location** field.



Name the New Location

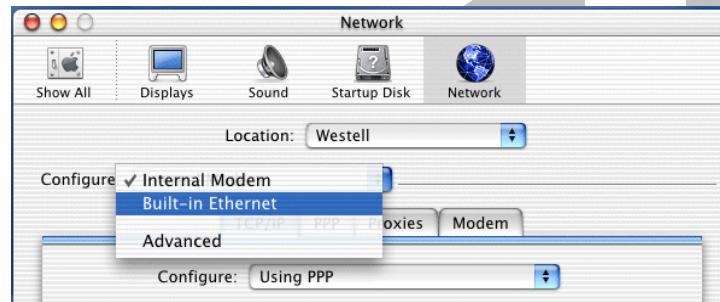
After selecting **New Location** from the **Network** screen, the following screen will be displayed. In the field labeled **Name your new location:**, change the text from “Untitled” to “Westell.” Click **OK**.



Select the Ethernet Configuration

After clicking on **OK** in the preceding screen, the **Network** screen will be displayed. The **Network** screen shows the settings for the newly created location. From the **Configure** field in the **Network** screen, select **Built-in Ethernet**. Click on **Save**.

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

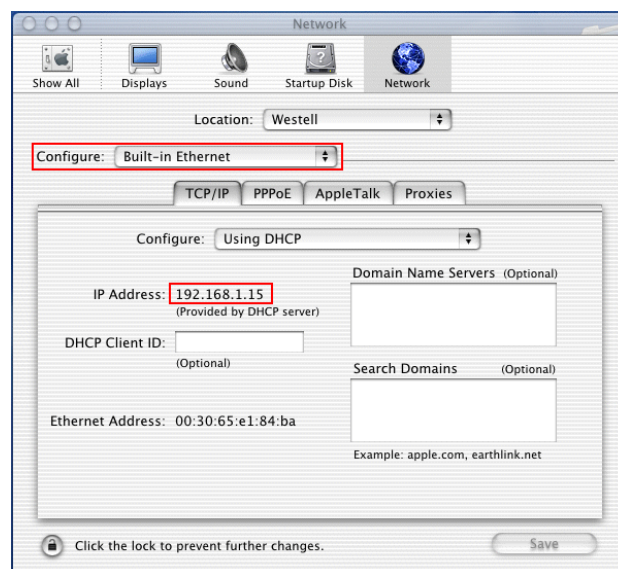


Check the IP Connection

To verify that the computer is communicating with Media Gateway, follow the instructions below.

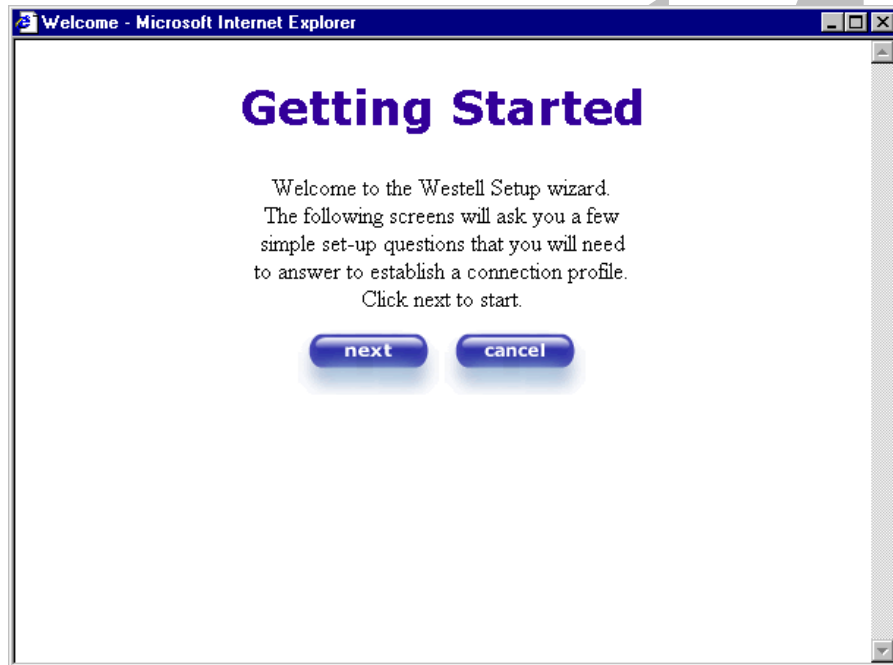
1. Go to the “**Apple**” icon in the upper-right corner of the screen and select **System Preferences**.
2. From the **System Preferences** screen, click on the **Network** icon. The **Network** screen will be displayed.
3. From the **Configure** field in the **Network** screen, select **Built-in Ethernet**.
4. View the IP address field. An IP address that begins with **192.168.1** should be displayed.

NOTE: The DHCP server provides this IP address. If this IP address is not displayed, check The Gateway’s wiring connection to the PC. If necessary, refer to section 7 for hardware installation instructions.



Create a User Account

In the address window of your Internet Explorer web browser, type **http://192.168.1.254**, and then press **Enter** on your keyboard. The **Getting Started** screen will be displayed. You may now begin your Account Setup. Refer to section 8 (Configuring Media Gateway for Internet connection) to begin setting up your account.



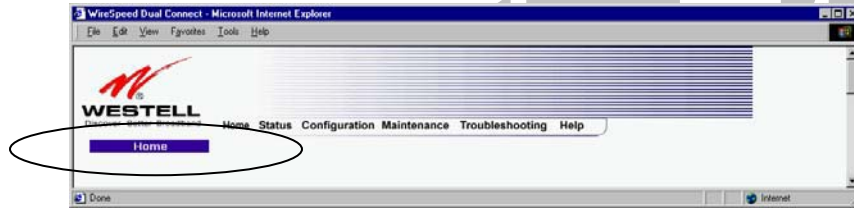
10. SETTING UP ADVANCED CONFIGURATION

Advanced Configuration instructions are explained in Section 11 through Section 17. If you want to set up advanced features for the Media Gateway, follow the instructions provided in sections 11 through 17.

The Media Gateway Communications Subsystem allows you to make changes to advanced features such as account profiles, routing configurations, and firewall settings. The following sections explain each feature and show you how to make changes to the Media Gateway's settings. A menu is displayed at the top of each screen and will allow you to navigate to the various configuration options of your Media Gateway. If you are at a screen and need help, click on the **Help** button to learn more about that screen.

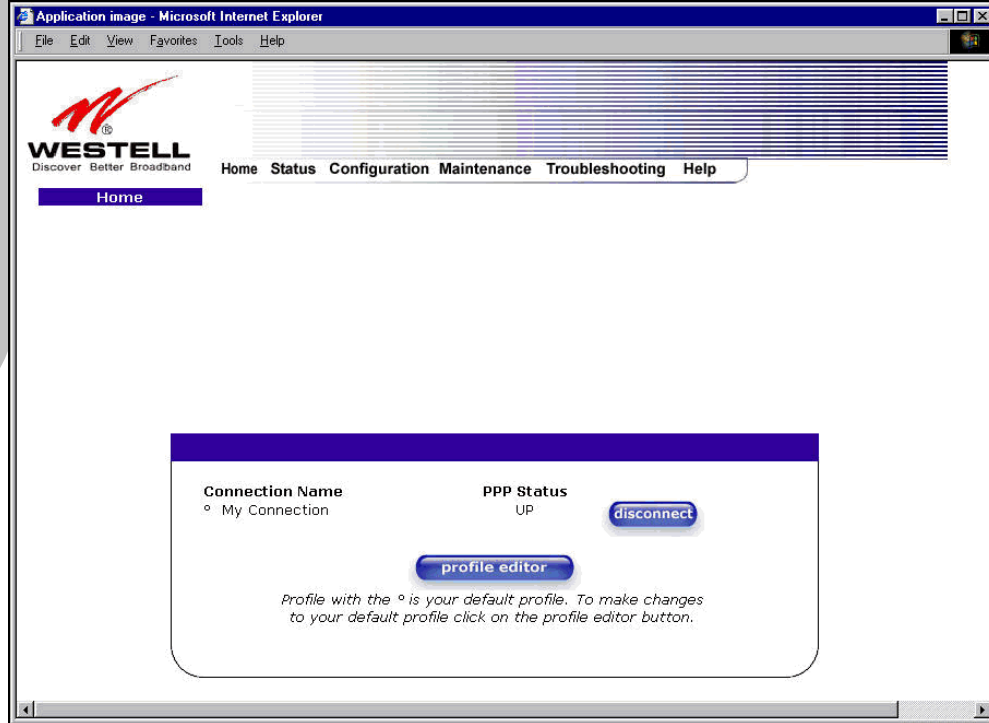
11. HOME

As you navigate through the various screens of Media Gateway Communications Subsystem, the name of the active page that you have selected will appear in the upper-left side of the screen, as shown below. Please note that the actual values may differ from the values displayed in the screens.



If you have set up your account profile and established your PPP session as discussed in section 8, the following settings will be displayed when you click on your **Home** page. Click on **profile editor** to edit your connection profile.

NOTE: If you have created multiple account profiles, select the option button for the active account profile.



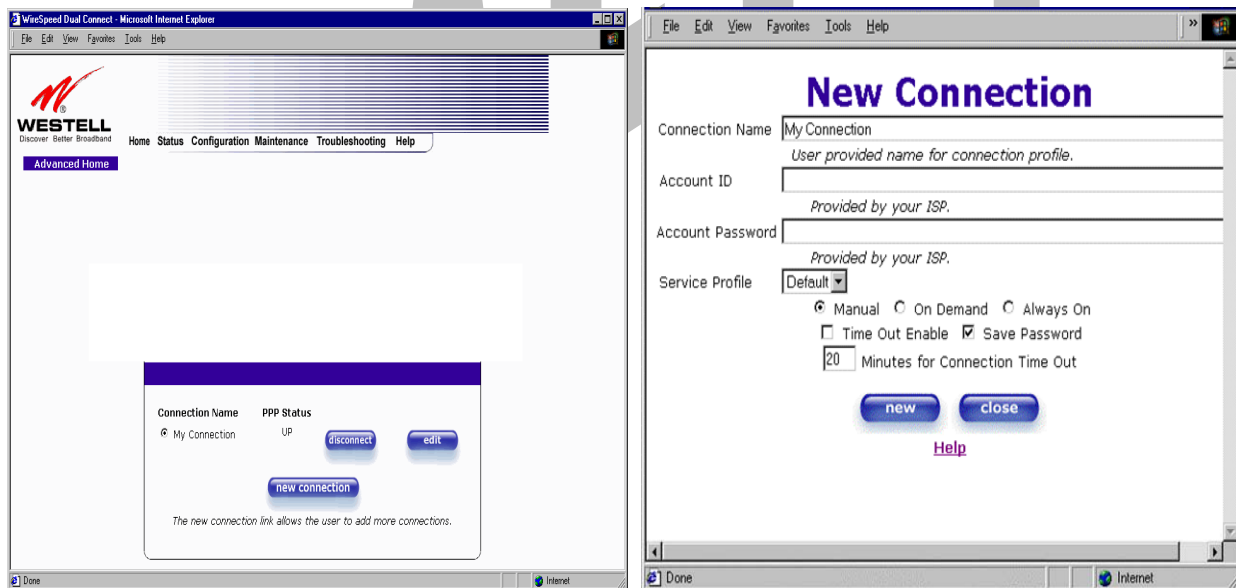
Connection Name	This Connection Name is from the connection profile that you established in section 8.
PPP Status	UP = PPP session established DOWN = No PPP session established.
Connect/Disconnect	CONNECT = Establish a PPP session

	DISCONNECT = Disconnect a PPP session
Profile Editor	This allows you to make changes to the profile that you created in section 8.

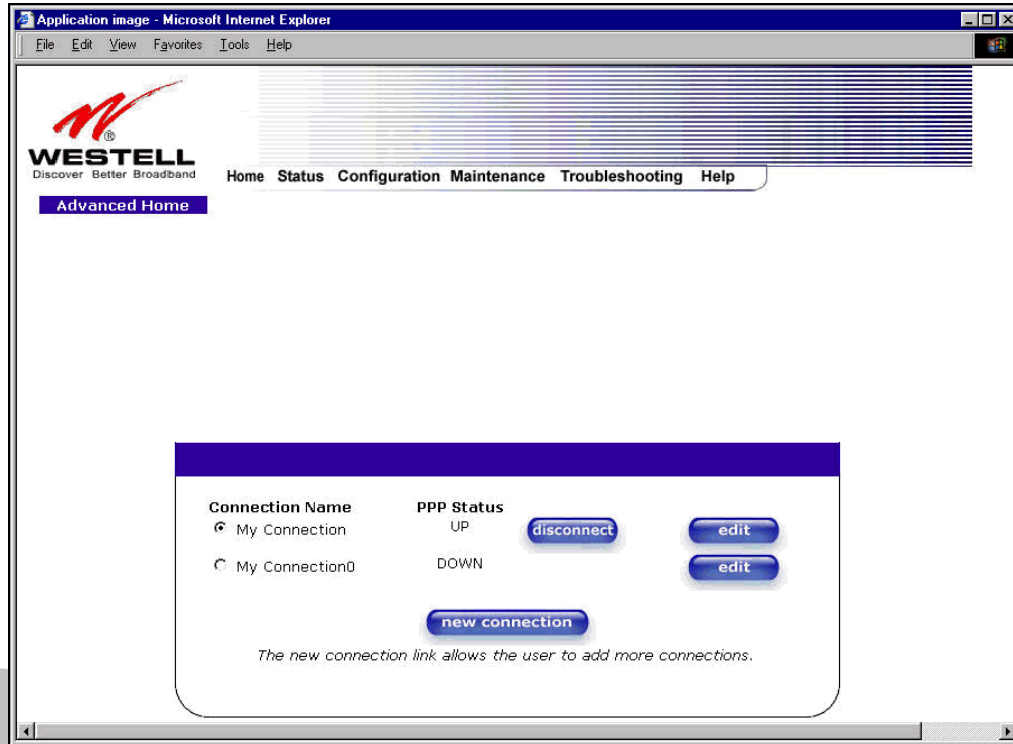
11.1 Adding Account Profiles

If you select the **Profile Editor** button from your **Home** page, the **Advanced Home** screen will appear, as shown below. Click on the **new connection** button in the **Advanced Home** screen. The **New Connection** screen will appear. Enter your account profile information and click on **New**. Next, click on **OK** in the pop-up screen to save your new connection. If you do not want to add a connection profile, click on **Close** in the **New Connection** screen.

NOTE: NAT Profiles allow you to create specific service settings. A NAT Profile may be associated with a certain connection setting, or NAT services. This allows you to customize the profile for specific users. You may store up to eight unique user profiles in the Media Gateway. Details on the **New Connection** screen are located at the end of this section.

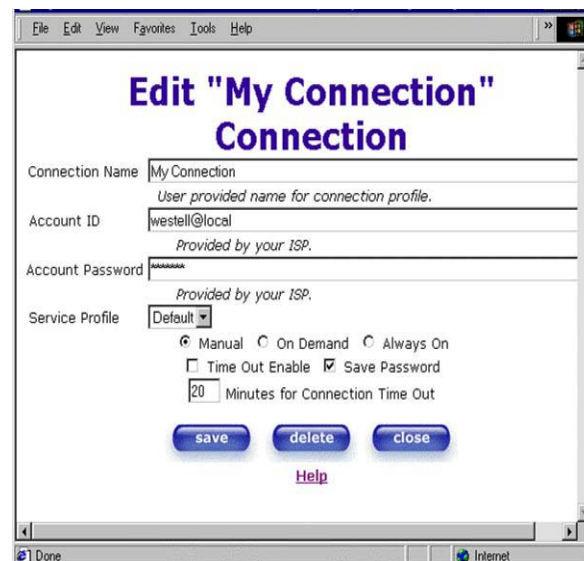


If you clicked **OK** in the “**Save new connection?**” pop-up screen, the following screen will be displayed. This screen will allow you to edit a connection profile. Select a profile name from the **Connection Name** field and click on the **edit** button adjacent to the name.



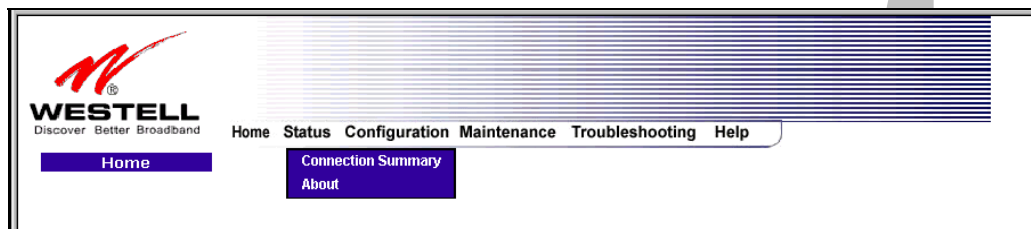
11.2 Editing Account Profiles

If you clicked on **Edit** in the preceding screen, the **Edit "My Connection"** screen will appear. Follow the steps in the **Edit "My Connection"** screen to change your existing connection profile, which you set up in section 8. If you do not want to change your connection profile, click on **close** in the screen. Click on **delete** if you want to delete your connection profile.

A screenshot of the "Edit 'My Connection' Connection" form in a web browser. The form contains the following fields and options: "Connection Name" (text box with "My Connection"), "Account ID" (text box with "westell@local"), "Account Password" (password box with "*****"), "Service Profile" (dropdown menu with "Default"), and radio buttons for "Manual", "On Demand", and "Always On". There are also checkboxes for "Time Out Enable" and "Save Password", and a text box for "Minutes for Connection Time Out" with the value "20". At the bottom are "save", "delete", and "close" buttons, along with a "Help" link.

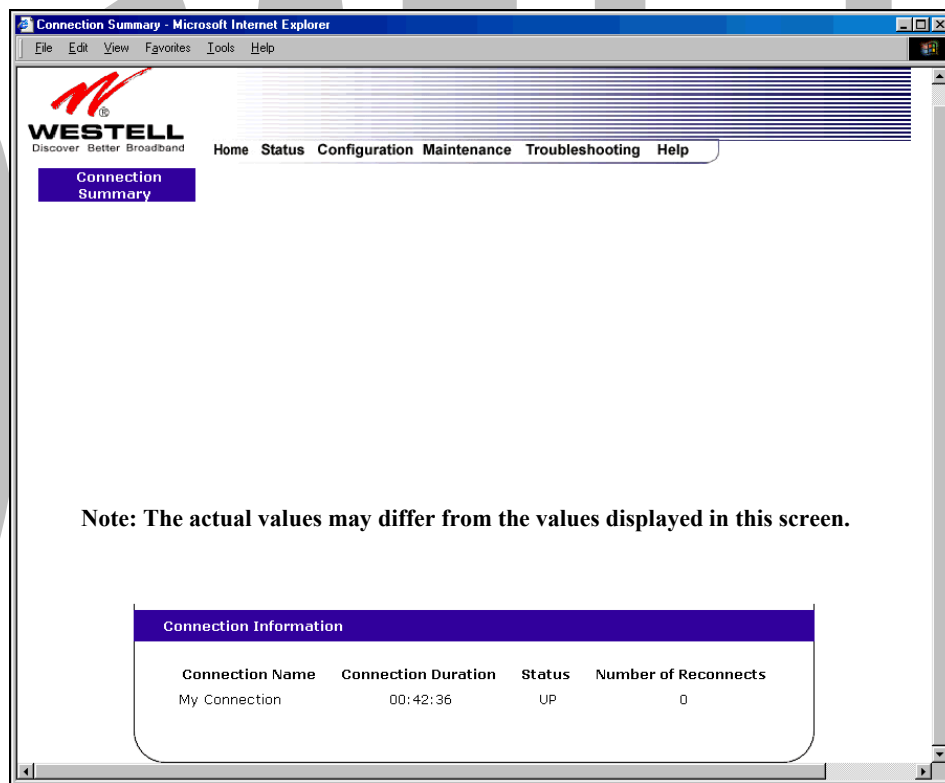
Connection Name	This field allows you to enter a new connection name of your choice (up to 64 characters).
Account ID	The account ID that you used in section 8.
Account Password	The account password that you used in section 8.
Service Profile	Westell recommends that you use the Default parameter.
Manual	Factory default = MANUAL Selecting this feature allows you to manually establish your PPP session.
On Demand	Selecting this feature allows Media Gateway to automatically re-establish your PPP session on demand anytime your PC requests Internet activity (for example, browsing the Internet, email, etc.). When you have traffic, it may cause a delay.
Always On	Selecting this feature allows Media Gateway to automatically establish a PPP session when you log on, or if the PPP session goes down.
Time Out Enable	Factory Default = DISABLED Selecting this feature allows you to enable the timeout parameter of your PPP session, which is set to a factory default of 20 minutes.
Save Password	Selecting this feature allows you to save the password for your new connection profile in Media Gateway so that you will not have to re-enter it in case of a reboot.
Minutes for Connection Time Out	This option allows you to specify the number of minutes that you want a PPP session to stay active before it is disconnected due to inactivity. (This feature works if you have selected the Time Out Enable feature explained above.)

12. STATUS



12.1 Connection Summary

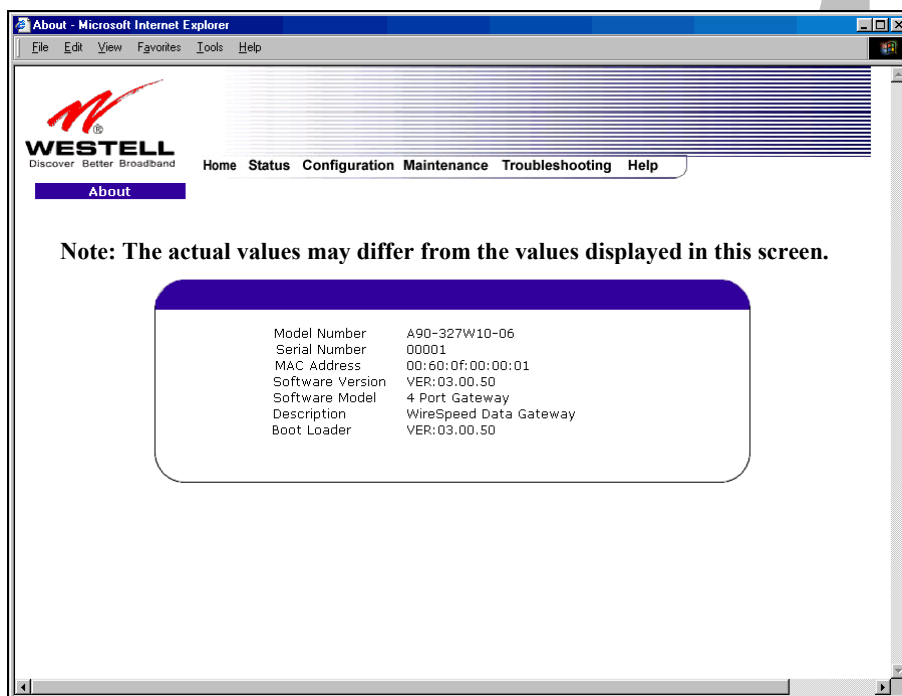
The following settings will be displayed if you select **Connection Summary** from the **Status** menu.



PPP Connection Information	
Connection Name	This is from the connection profile that you established in section 8.
Connection Duration	This field will display how long your PPP session has been connected.
Status	This field will display the status of your PPP session. UP=Connected DOWN=Disconnected
Number of Reconnects	This field will display the number of attempts that were made to establish a PPP session.

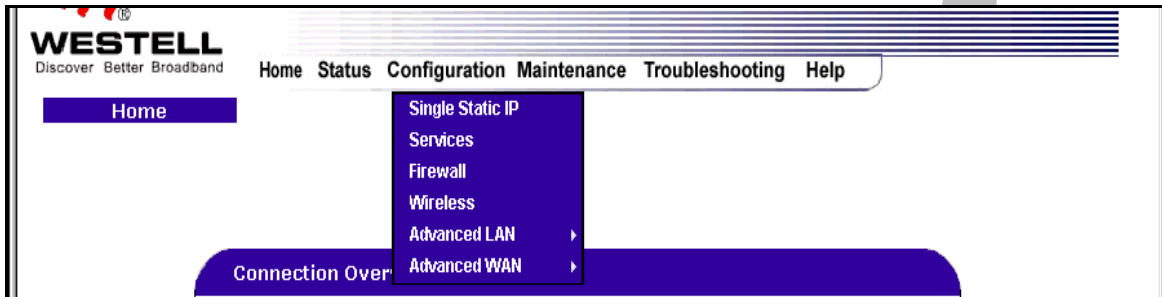
12.2 About

The following settings will be displayed if you select **About** from the **Status** menu.



Model Number	Media Gateway manufacturer's model number.
Serial Number	Media Gateway manufacturer's serial number.
MAC Address	Media Access Controller (MAC) i.e., hardware address of this device.
Software Version	Version of Application Software.
Software Model	Media Gateway application type.
Description	Product description.
Boot Loader	Version of boot loader software

13. CONFIGURATION

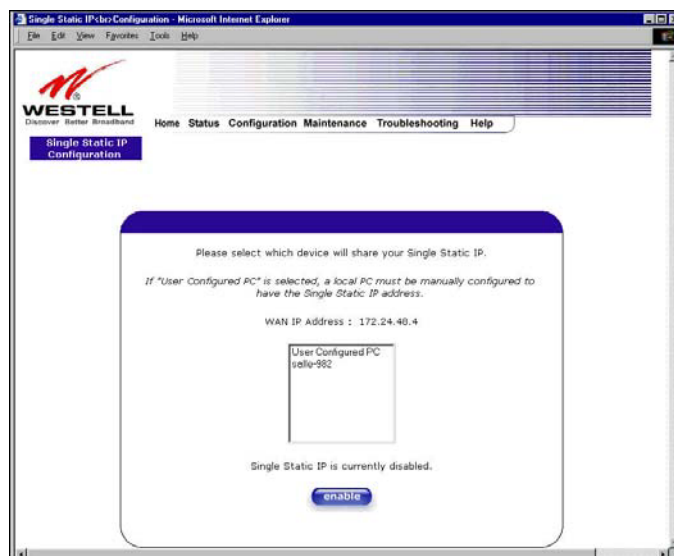


13.1 Single Static IP – Single IP Address PassThrough

The following settings will be displayed if you select **Single Static IP** from the **Configuration** menu. The Single Static IP Configuration screen allows you to select the device on your LAN that will share your Single Static IP. Before you begin this section, configure your PC settings to obtain an IP address from Media Gateway automatically. (Refer to your Windows Help screen for instructions.)

NOTE: Single Static IP (SSI) allows the user to share the WAN assigned IP address with one device on the LAN. 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.

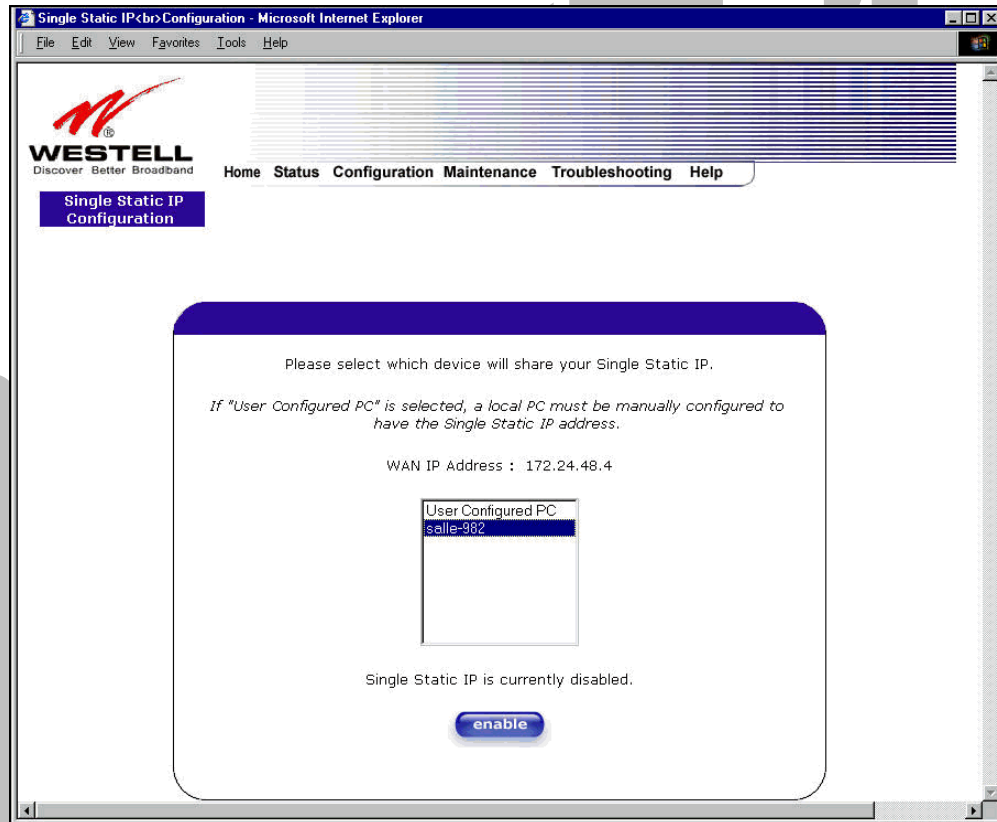
STOP: Static NAT must be disabled before you can enable **Single Static IP**. To disable Static NAT, select **Services** from the **Configuration** menu. Next, click on the **static NAT** button. Select the device from the **Static NAT Device** drop-down menu and click on **disable**. Return to Single Static IP Configuration by selecting **Single Static IP Configuration** from the **Configuration** menu.



13.1.1 Enabling Single Static IP – Single IP Address PassThrough

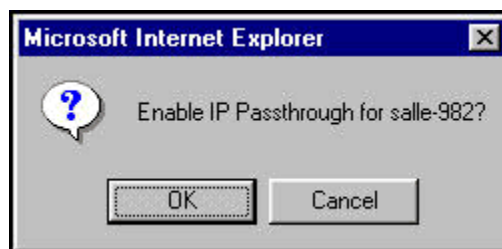
To enable Single Static IP, select a device that will share your Single Static IP from the options listed in the window. Click on **enable**.

NOTE: The Single Static IP Configuration screen allows you to select the device on your LAN that will share your Single Static IP.

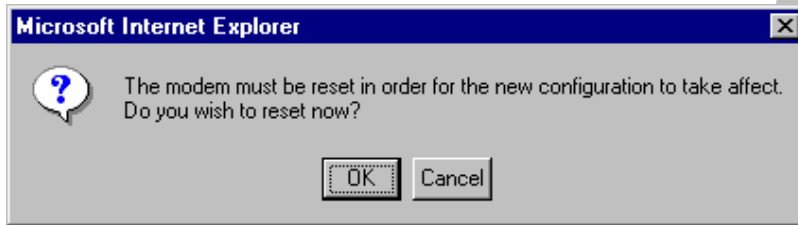


If you select a device and clicked on **enable**, the following pop-up screen will appear. Click on **OK** to enable this device for Single Static IP. Click on **Cancel** if you do not want to enable Single Static IP.

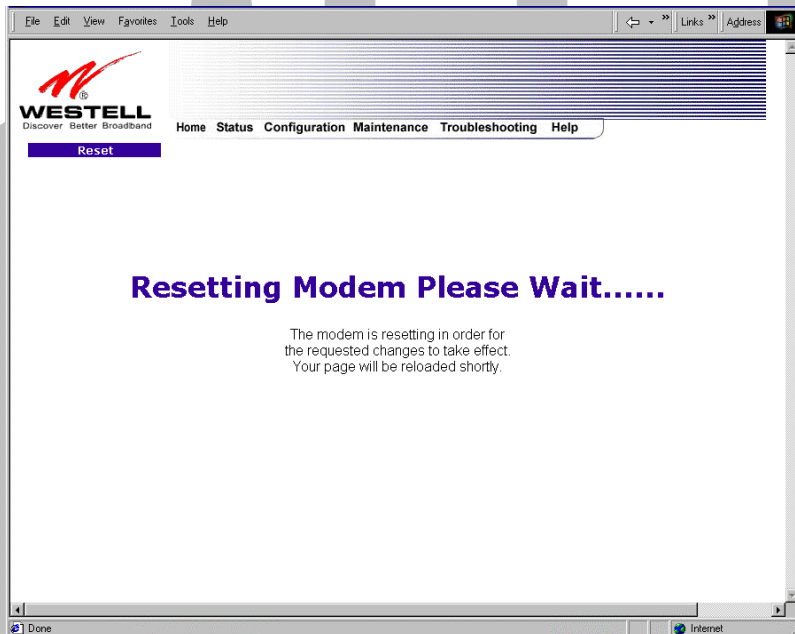
NOTE: The actual device name may differ from the name displayed in this screen.



If you clicked on **OK** in the preceding pop-up screen, the following pop-up screen will appear. Media Gateway must be reset to allow the new configuration to take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. Media Gateway will be reset and the new configuration will take effect.



After a brief delay, the home page will be displayed. Confirm that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session). Next, Select **Single Static IP** from the **Configuration** menu to confirm that Single Static IP is **enabled**, as shown in the following screen.

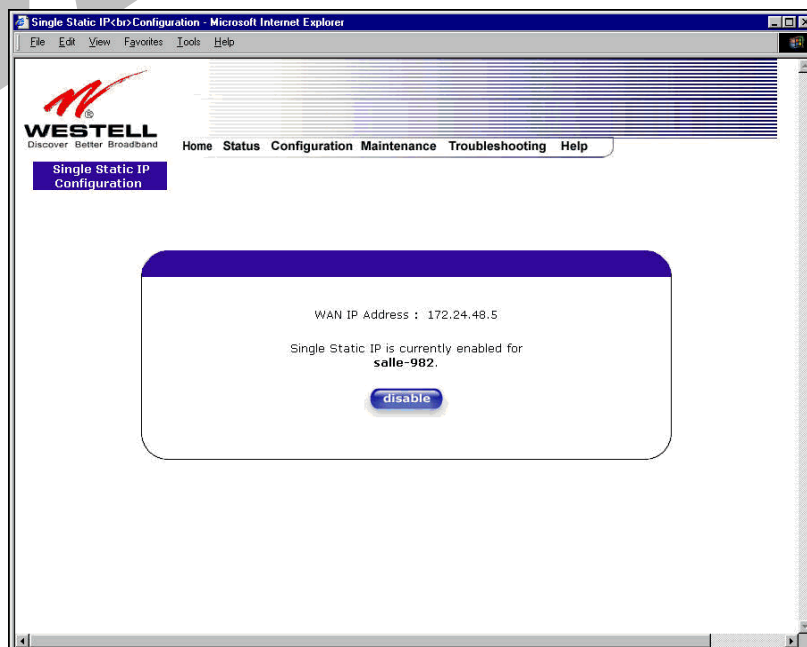


STOP! After you enable Single Static IP, you must reboot your computer.

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

13.1.2 Disabling Single Static IP – Single IP Address PassThrough

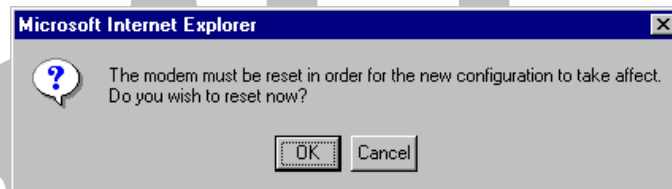
To disable Single Static IP, select **Single Static IP** from the **Configuration** menu. Click on **disable**.



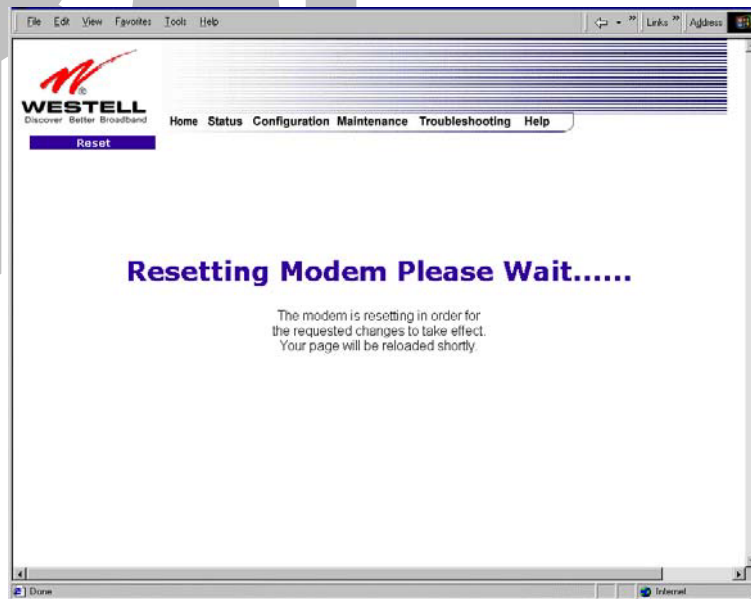
If you clicked on **disable** in the preceding screen, the following pop-up screen will be displayed. Click on **OK**.



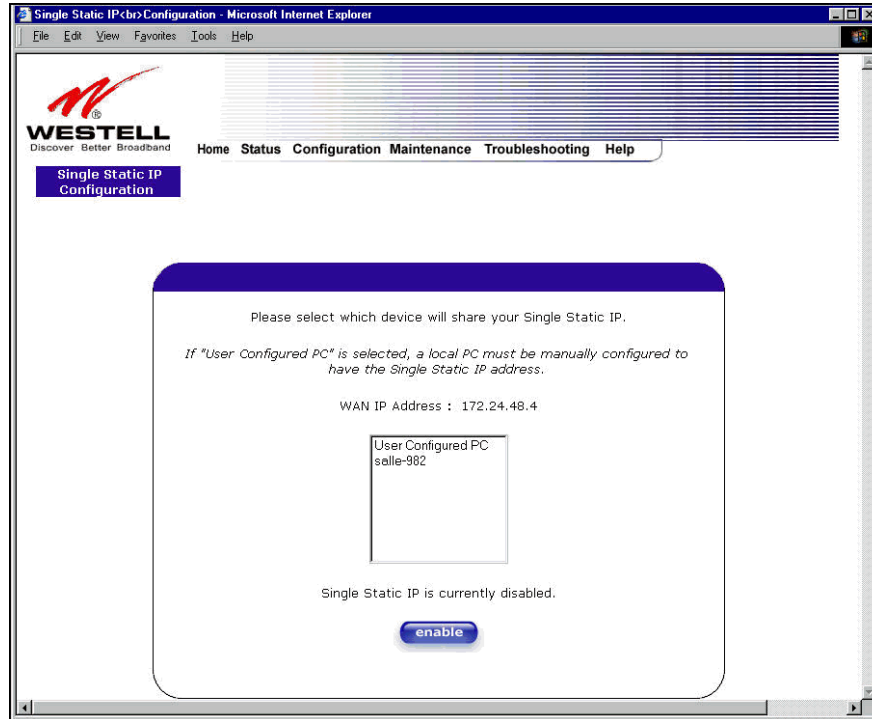
If you clicked on **OK** in the **Disable IP Passthrough?** screen, the following pop-up screen will be displayed. This screen will allow the modem to be reset and the new configuration will take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. Media Gateway will be reset and the new configuration will take effect.



After a brief delay, the home page will be displayed. Confirm that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session). Next, Select **Single Static IP** from the **Configuration** menu to confirm that Single Static IP is **disabled**, as shown in the following screen.



STOP! After you disable Single Static IP, you must reboot your computer.

13.2 Service Configuration

The following settings will be displayed if you select **Services** from the **Configuration** menu.

Westell has developed an extensive list of NAT services and you may select any service from this list. By selecting your specific NAT service and setting up a NAT profile, you will ensure that the appropriate ports on Media Gateway are open and that the required application traffic can pass through your LAN. For a list of supported services, go to section 17 (NAT Services).

NAT Profiles allow you to create specific service settings. The NAT profile may then be associated with a connection profile, allowing you to customize profiles for specific users. For example, if you want to attach specific NAT services to a profile, or if you want to set up a different connection setting for a profile, you can create new NAT profiles and customize them to your preference.

NOTE: You may create up to four NAT profiles and attach an unlimited number of services to each profile.

Service Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

WESTELL
Discover Better Broadband

Home Status Configuration Maintenance Troubleshooting Help

Service Configuration

Current Profile: Default new edit

Service Name Select A Service enable delete edit
* * Denotes Custom Service

UPNP Enable ☐

Service Name Service Mode Host Device

define custom service
static NAT

Current Profile	Displays the NAT (Network Address Translation) services that you have selected.
Service Name	Drop down selection menu of NAT (Network Address Translation) service you can select to configure the Media Gateway.
UPNP Enable	Factory Default = Disable Enabling UPNP (Universal Plug and Play) allows automatic device discovery by your operating system.

13.2.1 Configuring UPNP on the Media Gateway

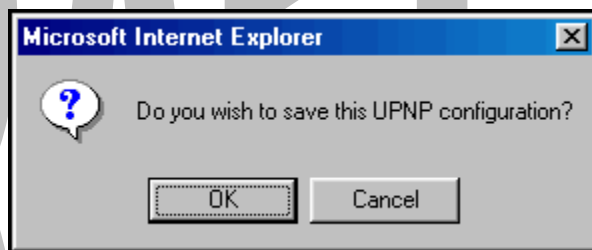
Note: To use the UPNP functionality in the Media Gateway, your Windows XP operating system must also support UPNP. Please contact your computer manufacturer to verify that UPNP is enabled in your Windows XP operating system.

To enable UPNP on Media Gateway perform the following steps:

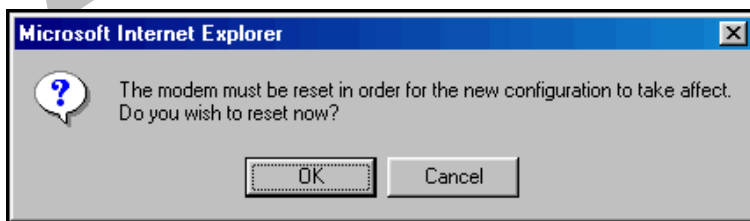
- 1) Select **Service Configuration** from the Configuration screen
- 2) Click the **UPNP Enable** box (a check mark will appear in the box).
- 3) Follow the instructions in the pop-up screens.
- 4) Click **OK** to Reset the Media Gateway.

NOTE: When you are ready to disable UPNP, uncheck the **UPNP Enable** box in the **Service Configuration** screen.

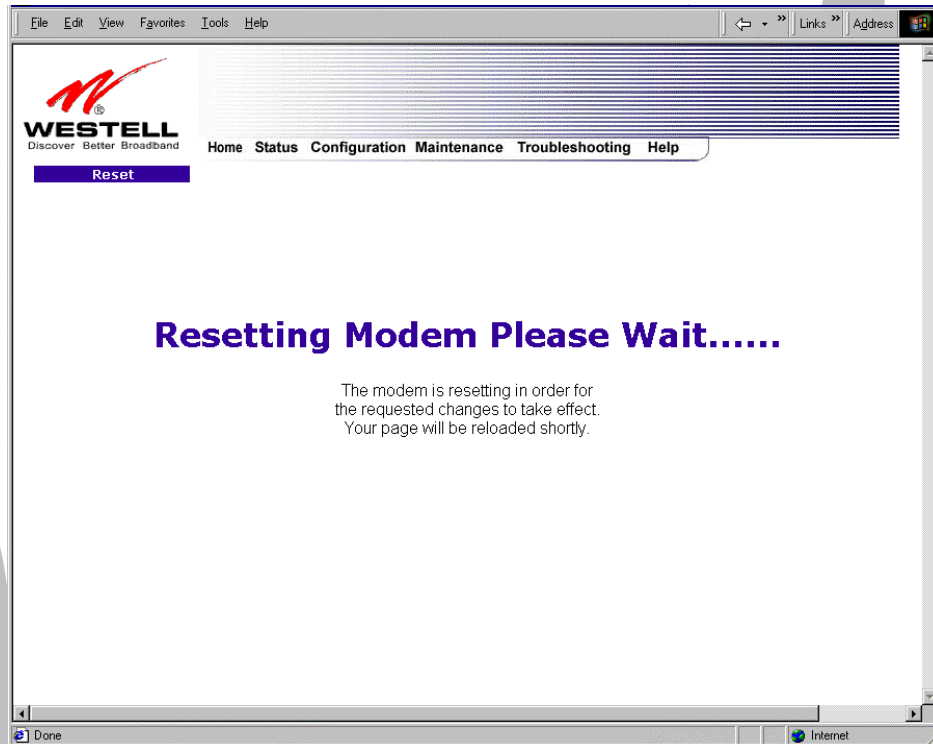
If you click the **UPNP Enable** box in the **Service Configuration** screen, a check mark will appear in the box and the following pop-up screen will be displayed. Click **OK** to continue.



If you click **OK** in the preceding screen, the following pop-up screen will be displayed. Click on **OK** to reset the Media Gateway.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. Media Gateway will be reset automatically, and the new configuration will take effect.



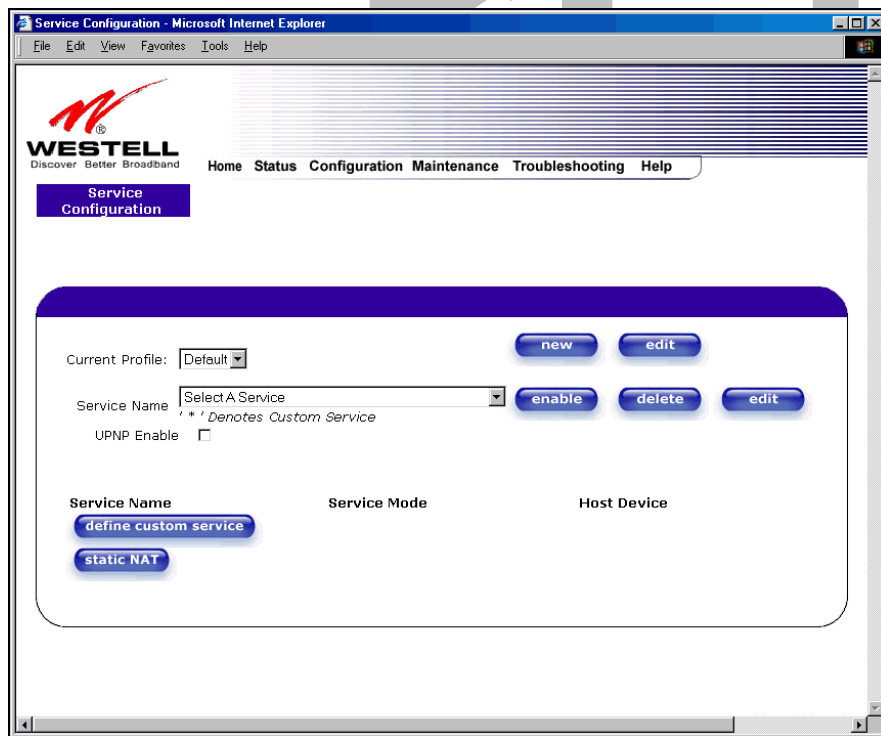
After a brief delay, the home page will be displayed. Confirm that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session).

13.2.2 Creating a New NAT Service Profile

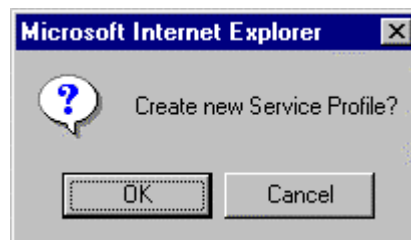
NAT Profiles allow you to create specific service settings. The NAT profile may then be associated with a connection profile, allowing you to customize profiles for specific users. For example, if you want to attach specific NAT services to a profile, or if you want to set up a different connection setting for a profile, you can create new NAT profiles and customize them to your preference.

NOTE: You may create up to four NAT profiles and attach an unlimited number of services to each profile.

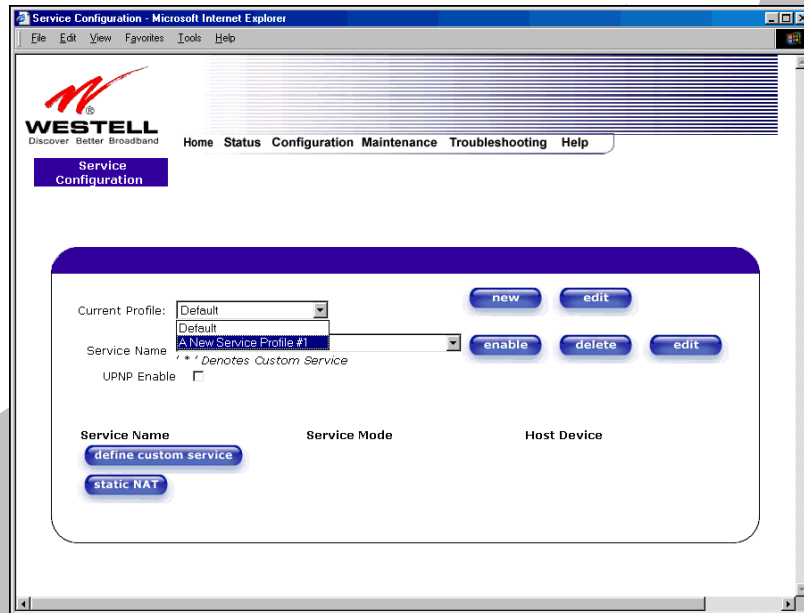
To create a new NAT profile, click **new** in the **Service Configuration** screen.



If you select **new** from the preceding **Service Configuration** screen, the **Create new Service Profile?** pop-up screen will be displayed. Click on **OK** to begin creating your new NAT service profile. Click **Cancel** if you do not want to create a new NAT service profile.

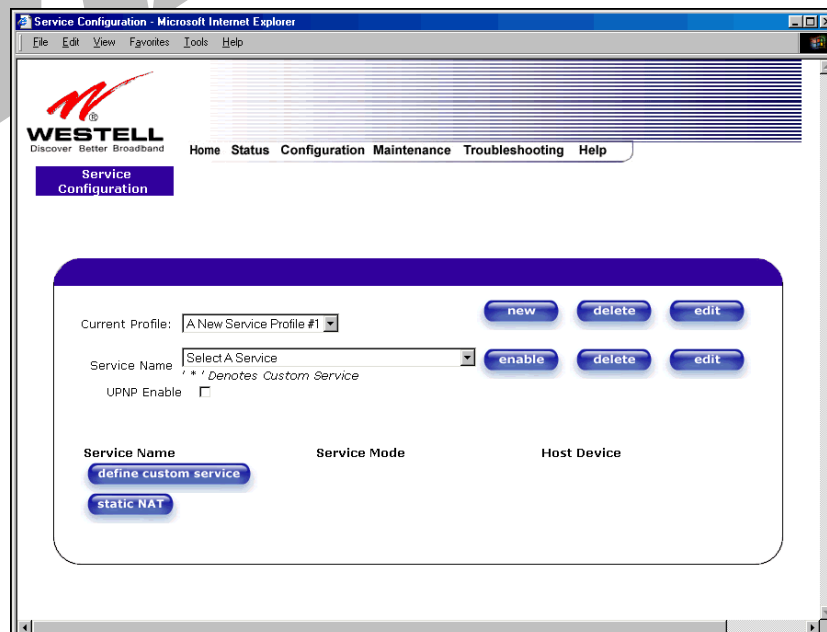


If you clicked on **OK**, the following screen will be displayed. Select **“A New Service Profile #1”** from the **Current Profile** drop-down arrow.



The screenshot shows a web browser window titled "Service Configuration - Microsoft Internet Explorer". The page features the Westell logo and a navigation menu with links: Home, Status, Configuration, Maintenance, Troubleshooting, and Help. A "Service Configuration" button is highlighted. The main content area has a "Current Profile:" dropdown menu set to "A New Service Profile #1". Below this is a "Service Name" dropdown menu with a note: "Denotes Custom Service". There is an "UPNP Enable" checkbox. Buttons for "new", "edit", "enable", "delete", and "static NAT" are visible. At the bottom, there are sections for "Service Name", "Service Mode", and "Host Device", each with a "define custom service" button.

If you selected **“A New Service Profile #1”** from the **Current Profile** drop-down arrow, the following screen will be displayed. This screen shows that you have chosen to create a new NAT service profile. You may create up to four NAT service profiles and attach an unlimited number of services to each profile.



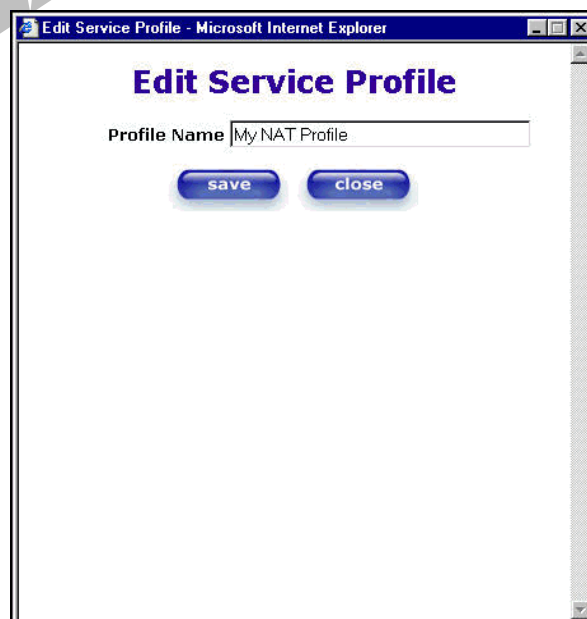
The screenshot shows the same web browser window as the previous one. The "Current Profile:" dropdown menu is still set to "A New Service Profile #1". The "Service Name" dropdown menu is now set to "Select A Service". The "UPNP Enable" checkbox is still unchecked. The buttons for "new", "edit", "enable", "delete", and "static NAT" are still present. The bottom sections for "Service Name", "Service Mode", and "Host Device" with their respective "define custom service" buttons are also visible.

13.2.3 Editing a NAT Service Profile

After you have created a NAT service profile, you may edit the profile's name. If you select **edit** from the **Service Configuration** screen, the following screen will be displayed. By selecting the **edit** button, you can make changes to your profile name, and then, later, add to or delete NAT services from that profile. Type your new NAT service profile name in the field labeled **Profile Name**.



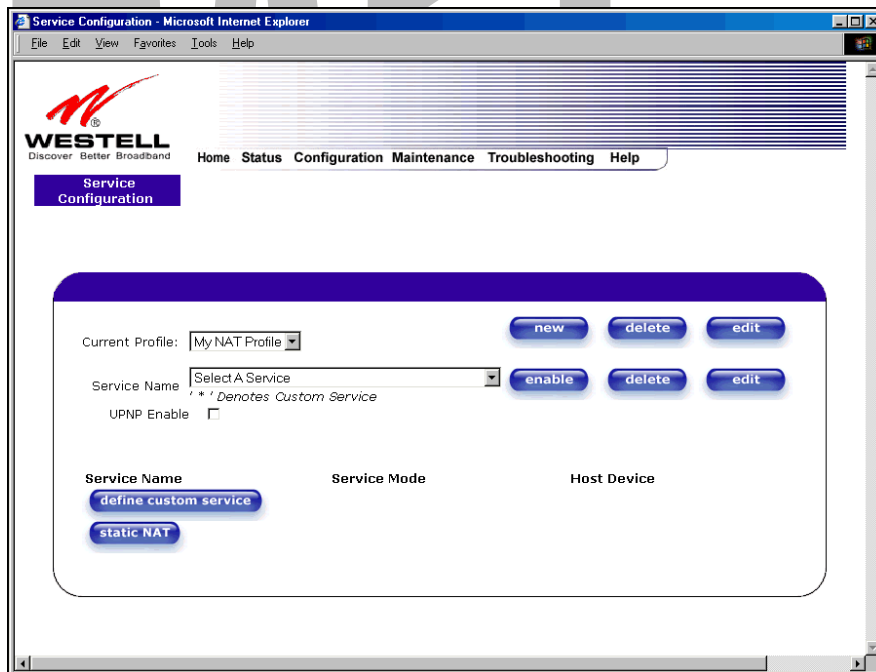
The following screen shows that a new profile name called '**My NAT Profile**' was entered into the **Profile Name** field. If you want save the new NAT profile, click on **save**. If you do not want to save the new NAT profile, click on **close**.



If you clicked on **save** in the **Edit NAT Profile** screen, the following pop-up screen will be displayed. Click **OK** to save your new profile settings. If you click on **Cancel**, your new profile settings will not be saved.



The following screen displays the current profile. If desired, you may create a new profile and delete or edit an existing profile.



13.2.4 Adding NAT Services to a Profile

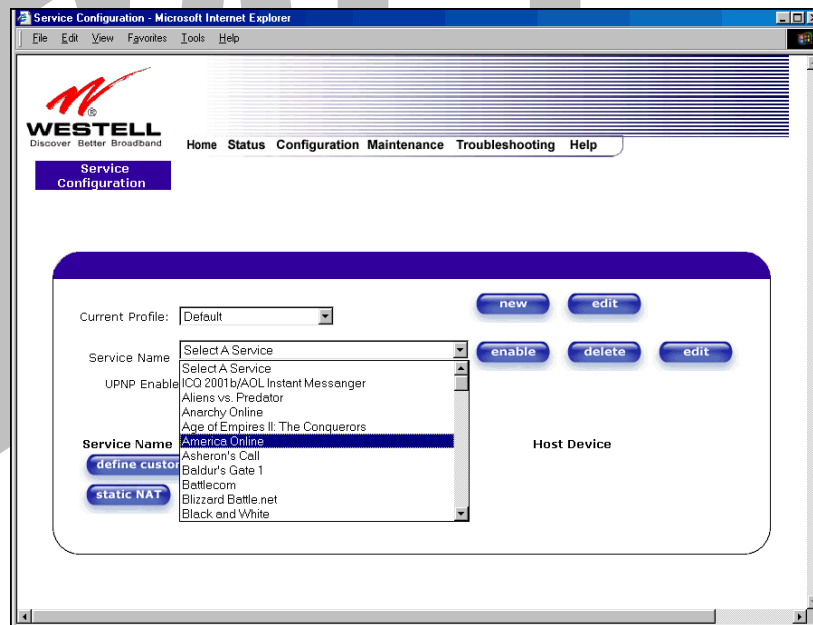
This section explains how to add NAT services to your NAT service profile. Remember, you may attach an unlimited number of NAT services to any profile.

NOTE: Westell has developed an extensive list of NAT services and you may select any service from this list. By selecting your specific NAT service and setting up a NAT profile, you will ensure that the appropriate ports on Media Gateway are open and that the required application traffic can pass through your LAN. For a list of supported NAT services, go to section 17 (NAT Services).

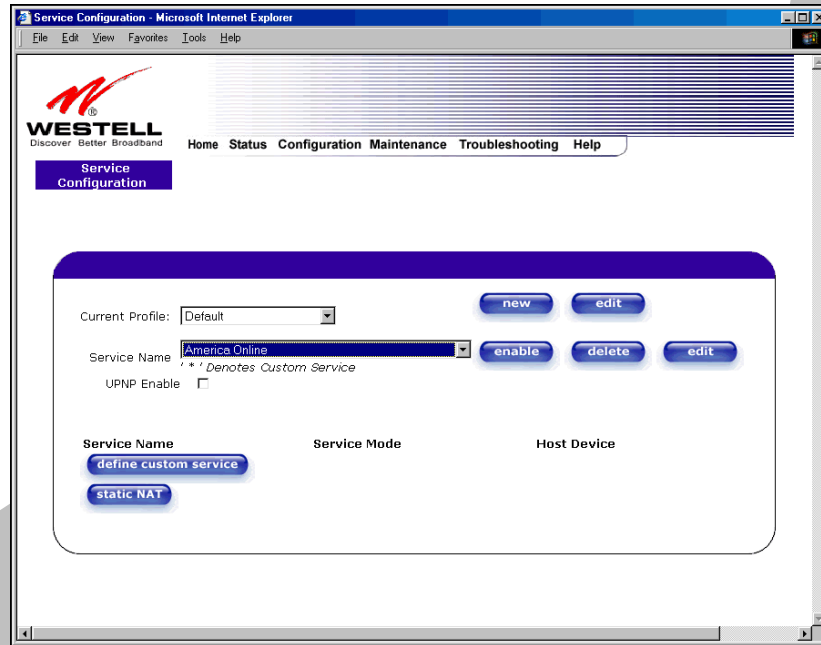
To add a NAT service, select **Services** from the **Configuration** menu. Next, Select a NAT service from the options provided at the **Service Name** drop-down arrow.

NOTE: You can attach multiple NAT services to your profile. However, for each NAT service that you attach to your profile, you must first select the new NAT service. Then, you must load the new NAT Configuration, as explained in section 13.2.2.

In the following screen, the 'Default' profile has been selected as the profile that will host the selected NAT service. However, you can attach a NAT service to any profile.

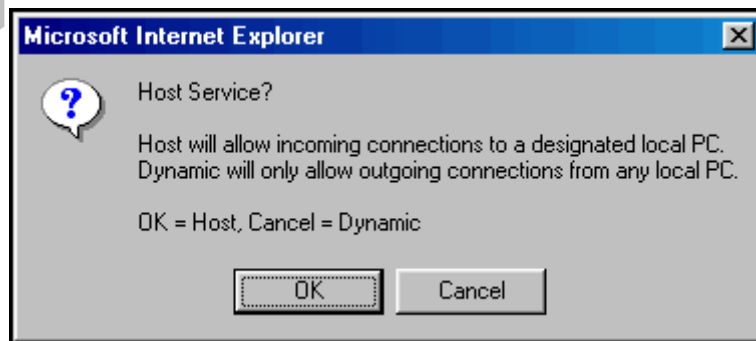


For example, the screen below displays **America Online** as the NAT service selected. After you have selected a service, click on **enable**.



If you click **enable**, the following pop-up screen will be displayed. If you click **OK**, you will allow incoming connections to be forwarded to a designated local PC. If you click **Cancel**, you will allow only outgoing connections from any local PC. Click **OK** or click **Cancel**.

NOTE: If you click **Cancel** in the following pop-up screen, the NAT service you selected in the **Service Configuration** screen is still configured; however, it will not be assigned to any device on the local LAN. You must click **OK** to host the NAT service.

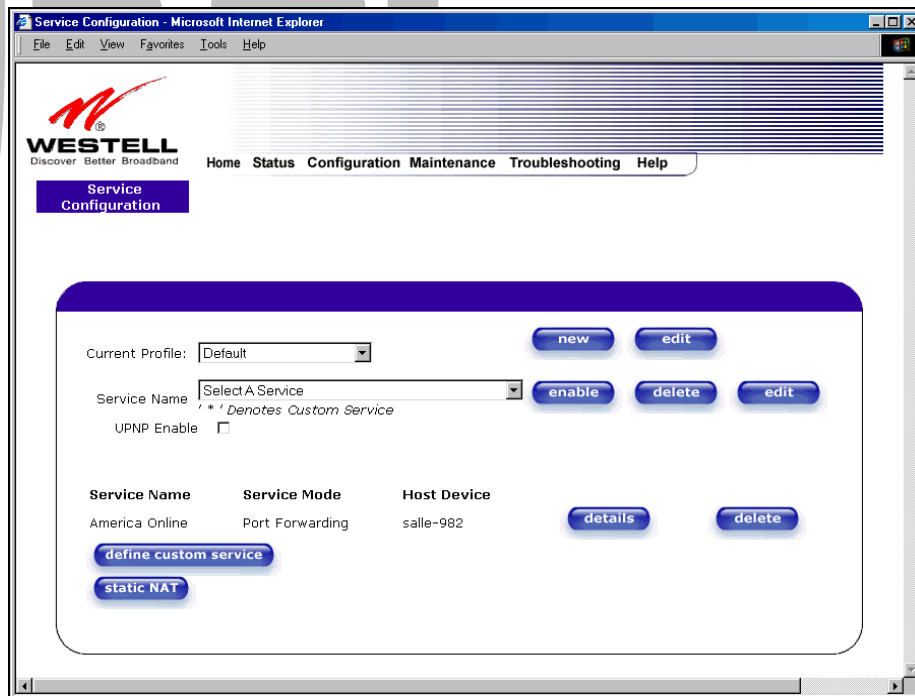


If you clicked on **OK** in the preceding pop-up screen, the **Host Device** screen will be displayed. The **Host Device** screen will allow you to select which device will host the NAT service you selected on your local area network. You must either select the device from the **Host Device** drop-down arrow or type an IP address in the field labeled **IP Address**. If you click on **Cancel**, the connection will be dynamically assigned. Click on **done**.



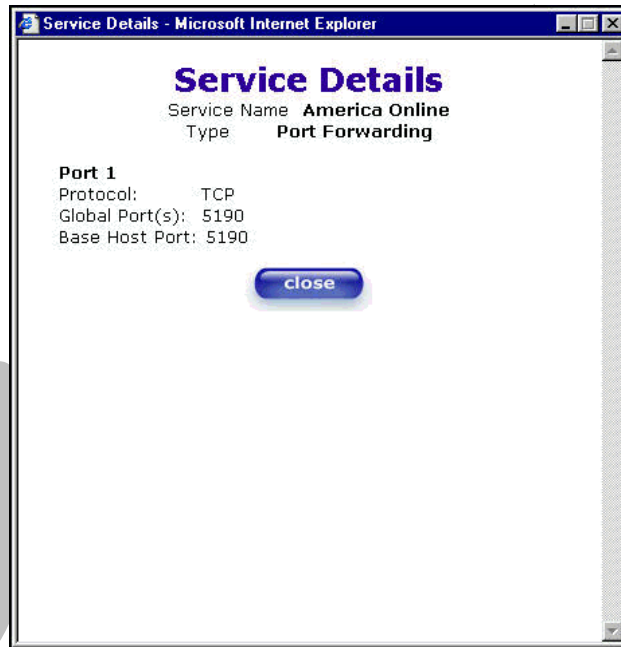
The screenshot shows a web browser window titled "Host Device - Microsoft Internet Explorer". The main content area has a purple header bar. Below it, there is a "Host Device" label followed by a dropdown menu showing "salle-982". Below this, the text "or specify" is displayed. Underneath is an "IP Address" label followed by a text input field. At the bottom center is a blue button labeled "done".

After you have selected a NAT service and you have saved it to your NAT service profile, the following screen will be displayed. It shows which NAT service is active for the selected profile.



The screenshot shows a web browser window titled "Service Configuration - Microsoft Internet Explorer". The page has a purple header bar with the Westell logo and the tagline "Discover Better Broadband". Below the header is a navigation menu with links: Home, Status, Configuration, Maintenance, Troubleshooting, and Help. The "Service Configuration" link is highlighted. The main content area has a purple header bar. Below it, there is a "Current Profile:" label followed by a dropdown menu showing "Default". To the right of the dropdown are "new" and "edit" buttons. Below this is a "Service Name" label followed by a dropdown menu showing "Select A Service". To the right of the dropdown are "enable", "delete", and "edit" buttons. Below this is a "UPNP Enable" checkbox, which is currently unchecked. Below the checkbox is a table with three columns: "Service Name", "Service Mode", and "Host Device". The table has one row with the following data: "America Online", "Port Forwarding", and "salle-982". To the right of the table are "details" and "delete" buttons. Below the table are two buttons: "define custom service" and "static NAT".

If you select the **details** button in the **Service Configuration** screen, the following screen will display the details of the selected NAT service. If you click on the **delete** button in the **Service Configuration** screen, you will remove that NAT service from your NAT service profile. Click on **close** to continue.



NOTE: If you would like to set up additional Advanced Service Configuration options, refer to section 14 (Setting Up Advanced Service Configuration).

13.3 Firewall Configuration

The following settings will be displayed if you select **Firewall** from the **Configuration** menu.

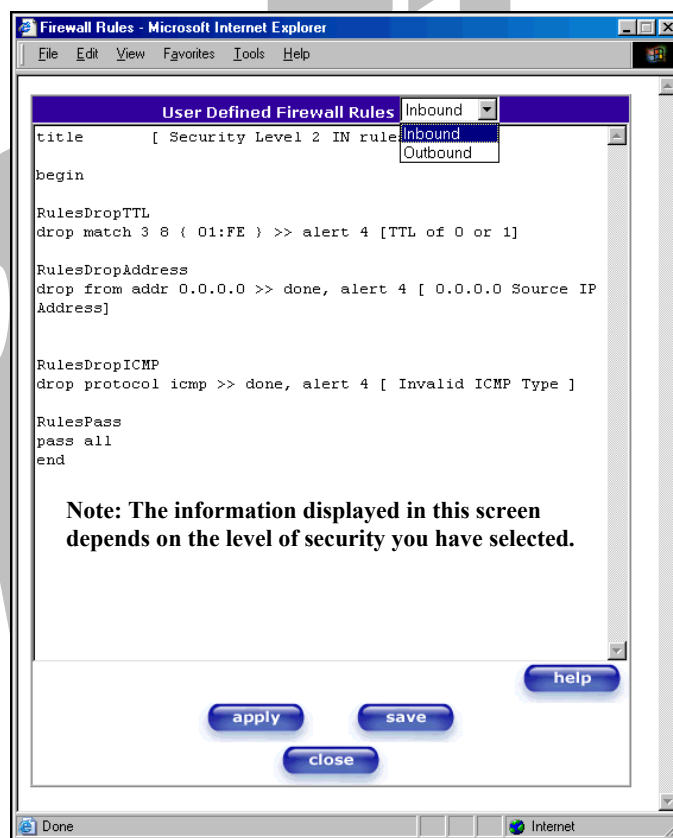


Security Level	
High	High security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. All other traffic is prohibited.
Medium	Factory Default = MEDIUM Like High security, Medium security only allows basic Internet functionality by default. However, Medium security allows customization through NAT configuration so that you can enable the traffic that you want to pass.
Low	The Low security setting will allow all traffic except for known attacks. With Low security, Media Gateway is visible to other computers on the Internet.
None	Firewall is disabled. (All traffic is passed)
Custom	Custom is an advanced configuration option that allows you to edit the firewall configuration directly. NOTE: only the most advanced users should try this.
Remote Logging	
Enable	Factory Default = Disable If enabled, Media Gateway will send firewall logs to a syslog server.
Remote IP Address	The IP address of the syslog server machine to which the diagnostics logs to be sent.

Important: Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset Media Gateway to factory default settings, push the reset button on the rear of the Media Gateway.

If you select **Edit** from the **Security Level** screen, the **User Defined Firewall Rules** screen will be displayed. This screen allows you to change the security parameters on your Inbound and Outbound Firewall rules via the **User Defined Firewall Rules** drop-down arrow. If you select **Inbound**, this will restrict inbound traffic from the WAN to the LAN. **Outbound** restricts outbound traffic to the WAN from the LAN. To apply the new settings, click **Apply** in the screen labeled **User Defined Firewall Rules**.

The information displayed in the following screen depends upon the Firewall security setting you have selected. If you selected "None" in the preceding Firewall **Security Level** screen, no values will be displayed in the following **User Defined Firewall Rules** screen.

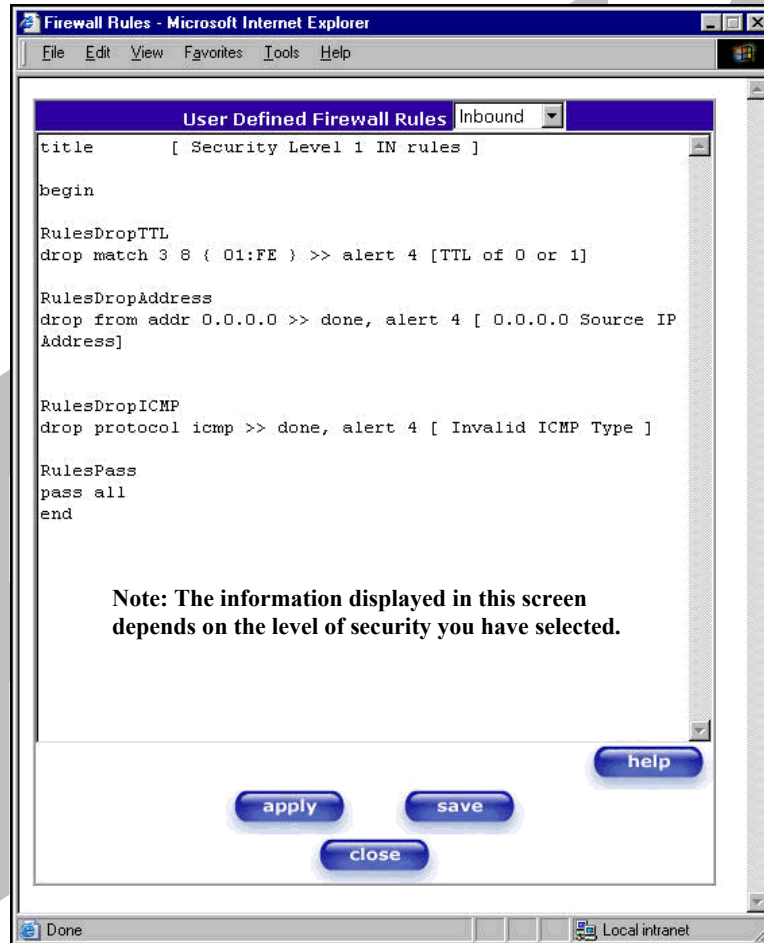


If you clicked **Apply** in the **User Define Firewall Rules** screen, the following pop-up screen will be displayed. Click on **OK** if you want your new firewall setting to take effect. If you click on **Cancel**, your new firewall settings will not take effect.



If you want to save your new firewall settings, click on **save** in the screen labeled **User Define Firewall Rules**.

Important: Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset Media Gateway to factory default settings, push the reset button on the rear of the Media Gateway.



If you clicked save in the User Define Firewall Rules screen, the following pop-up screen will be displayed. Click OK when asked Do you wish to save these Rules to Flash and switch you Security Level to "User"? This will save your new firewall settings. If you click Cancel, your new firewall settings will not be saved.



If you select **Help** in the screen labeled **User Defined Firewall Rules**, the following screen will be displayed. This screen gives a detailed explanation of the Firewall Rules.

DRAFT

File/Buffer Format

The RDL file or buffer format is divided into two sections. The first portion of the file defines any number of keys and associated values. The second portion contains the filtering rule definitions.

Key Definition Section

A key definition consists of the key followed by the associated value. A value is actually a character string. The string is delimited by the open and close square brackets. An example of a keyword definition would look like the following.

```
file [ High security RDL file ]
```

The packet filter engine does not use keys. They are intended to provide information associated with the file. The user interface treats the key definition and value pairs as standard text.

Rules Section

The rules section of the RDL file or buffer is delimited by the **begin** and **end** keywords. The rules listed between these delimiters are parsed and converted to a decision tree data structure used by the packet filter engine. The rules listed are implemented sequentially as listed in the RDL source. Once the packet filter engine finds a match for a rule it will note the filter action to be taken (pass or drop) and continue to compare the following rules with the given packet unless otherwise instructed (see the description of the **done** action in section 3.2.1.2.3).

Rule Names

RDL rules may be given names. The packet logging facility and the user interface uses these rule names. A name applies to all rules following its declaration in the Rules Section until another name is declared or the end statement. An identifier (one or more alphanumeric characters beginning with an alpha character) on a line by itself declares a new name for the following rule(s).

RDL Comments

Comments begin with the # character. The parser ignores all characters following the comment character to the end of the line.

RDL Command Syntax

An RDL command consists of a filter keyword followed by a condition expression optionally followed by one or more action keywords.

```
Filter Condition [ Condition2, [ == Action, Action2, ]
```

The filter keyword specifies if the packet will be passed or dropped. The condition defines the portion of the packet and the bit string to which it will be compared. The action keyword may specify additional action(s) to be taken.

Filter Keywords

The RDL filter token may be either passed or dropped.

pass Specifies that the matching packet is to be passed onto the associated interface or the SENS MUX.

drop Specifies that the matching packet will not be forwarded to the associated interface or the SENS MUX.

Condition Keywords

The condition expression determines if the rule is a match for the given packet.

all Specifies all packets. If the all condition is specified in a rule, all other conditions are ignored.

match layer offset (bit-string-mask) Specifies one or more explicit bit strings and offsets into the layer header to compare. This keyword is followed by three parameters. The first numeric parameter is the header layer, valid values include 2 through 4 (ethernet = 2, ip = 3, tcp/udp/icmp/igmp = 4). The second numeric parameter is the offset into the packet to begin the comparison. 1 and the third third parameter, is the representation of the bit string and comparison bit mask itself. The bit string is delimited with the open and close curly braces {}. A colon delimits the bit string and mask. If no mask is provided, a mask value of all ones is assumed. Each byte of the bit string and mask is represented by a two character hexadecimal number and is separated by white space from the previous byte representation.

from [to [addr (p-addr:mask)] [port port_n port >= port_n port >= port_n]] Specifies particular fields (IP address or TCP/UDP port number) of the IP header. The **from** keyword designates the source fields, and the **to** keyword designates the destination fields. One or more "M" descriptors of the fields and their contents then follows the keyword. A list of descriptors is to be separated by colon(s). These field descriptors include addr (IP address), mask (network mask), and port (TCP or UDP port number).

addr Specifies the source or destination IP address field and comparison mask. This keyword is followed by a IP address in dotted-decimal notation and mask separated by a forward slash. The mask is a number from 1 to 32 and it signifies how many bits of the IP address are compared. If no mask is provided, a mask value of 32 is assumed.

port Specifies the source or destination UDP/TCP port number. This keyword is followed by the 16 bit port number represented hexadecimal or decimal format. Using the >= or > operators allows for matching on ranges of ports.

protocol tcp | udp | icmp | igmp | value Specifies the value of the protocol field found in the IP header. It is followed by a parameter that specifies the protocol value. There are built in keywords for the TCP, UDP, ICMP, and IGMP protocols. If a different protocol value is required, it may be represented by a decimal or hexadecimal value between 0 and 255.

tcp Specifies the TCP protocol.

udp Specifies the UDP protocol.

icmp Specifies the ICMP protocol.

igmp Specifies the IGMP protocol.

flags urg | ack | push | rst | syn | fin Specifies some combination of the flag bits found in the TCP header. The parameters following the keyword should be represented in a colon delimited list.

igmp-type query | report Specifies the IGMP packet type found in the IGMP header. The **report** type checks for both version 1 and version 2 type codes. No check is made by the parser to verify that the IGMP protocol is specified. So it is up to the user to include the **protocol igmp** condition in a rule using the **igmp-type** condition.

icmp-type request | reply Specifies the ICMP packet type found in the ICMP header. No check is made by the parser to verify that the ICMP protocol is specified. So it is up to the user to include the **protocol icmp** condition in a rule using the **icmp-type** condition.

Action keywords

Specifies any further action to be taken upon a match between the rule condition and the packet content.

log level Specifies that the contents of any matching packet header should be recorded in the log table. The level parameter is a mechanism to indicate the source of the log entry. This value rule name is stored with each log entry resulting from this rule. The log may subsequently be searched or sorted by this value rule name. Log entries appear in the table with a default severity of 0. The level value is represented by a decimal or hexadecimal value between 0 and 255.

alert severity [Alert text] Specifies that the contents of any matching packet header should be recorded on the log table with the corresponding severity value and text explanation. Severity is a decimal number between 0 and 4. The alert text is delimited by brackets/brackets delimit the alert text.

done Specifies that the filtering engine should stop checking any subsequent rules should this rule match. This action provides a mechanism to optimize the decision tree implemented by the filtering engine.

state Specifies that the TCP/ICMP/IGMP session (particularly the sequence number in the case of TCP and the packet type and source/destination addresses and ports in the case of ICMP and IGMP) associated with this packet will be added to the state table maintained by the filtering engine. As long as that session remains in the state table all packets associated with that session are passed without comparing them to the rules decision tree. The filtering engine state table logic maintains the state of the session with successive packets and closes or times it out (removes it from the state table) whenever appropriate.

13.4 Wireless Configuration

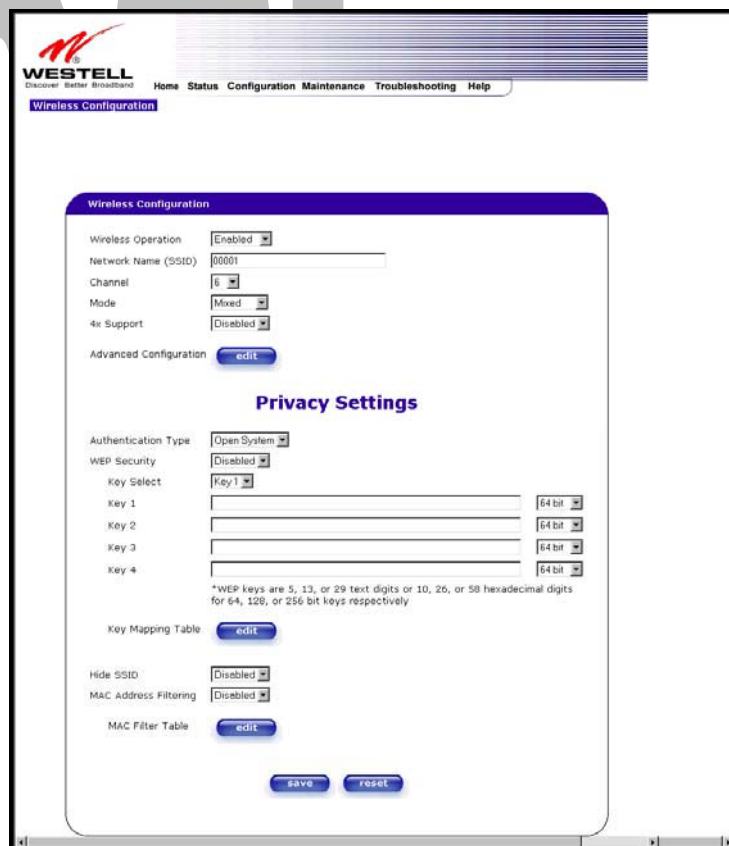
The following fields will be displayed if you select **Wireless** from the **Configuration** menu.

IMPORTANT: If you are connecting to Media Gateway via a wireless network adapter, the service set ID (SSID) must be the same for both Media Gateway and your PC's wireless network adapter. The default SSID for Media Gateway is the serial number of the unit (located below the bar code on the bottom of the base unit and also on the Westell shipping carton). Locate and run the utility software provided with your PC's Wireless network adapter and enter the SSID value. The PC's wireless network adapter must be configured with the SSID (in order to communicate with the Media Gateway) before you begin the Media Gateway's account setup and configuration procedures. For privacy, you may change the **Network Name (SSID)** value in the **Wireless Configuration** screen to your desired value.

NOTE: Client PCs can use any Wireless Fidelity (Wi-Fi) 802.11b/g certified card to communicate with the Media Gateway. The Wireless card and Media Gateway must use the same Wired Equivalent Privacy (WEP) security code type. The factory default for WEP is DISABLED. If you enable WEP, you must ensure the network setting for your wireless adapter is set to "Must Use Shared Key for WEP" or "Open Wi-Fi." You must ensure that your PC's Wi-Fi adapter is configured properly for whichever network setting you use. You can access the settings in the advanced properties of the wireless network adapter.

To select a network setting, click on the drop-down arrow at the field labeled **Authentication Type**, and then select either **Open System** or **Shared Key**. If you change any settings in this screen, you must click on the **Save** button to ensure that the settings take effect.

NOTE: For privacy, you should change the **Network Name (SSID)** value to your desired value.



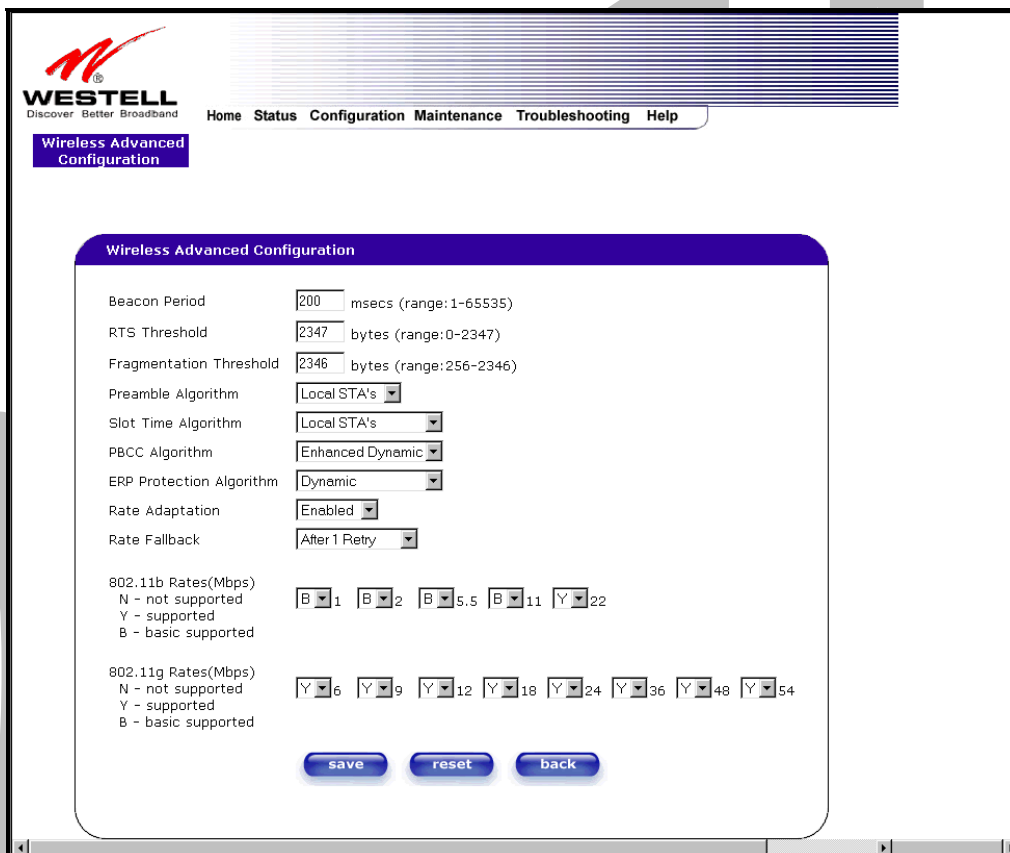
The screenshot displays the 'Wireless Configuration' web page for a Westell Media Gateway. At the top, the Westell logo and navigation links (Home, Status, Configuration, Maintenance, Troubleshooting, Help) are visible. The 'Wireless Configuration' section includes a 'Wireless Operation' toggle set to 'Enabled', a 'Network Name (SSID)' field with the value '00001', a 'Channel' dropdown set to '6', a 'Mode' dropdown set to 'Mixed', and a '4x Support' toggle set to 'Disabled'. Below these is an 'Advanced Configuration' link. The 'Privacy Settings' section features an 'Authentication Type' dropdown set to 'Open System', a 'WEP Security' dropdown set to 'Disabled', and a 'Key Select' dropdown set to 'Key 1'. There are four input fields for 'Key 1' through 'Key 4', each with a '64 bit' dropdown menu to its right. A note states: '*WEP keys are 5, 13, or 29 text digits or 10, 26, or 58 hexadecimal digits for 64, 128, or 256 bit keys respectively'. Below the keys is a 'Key Mapping Table' link. At the bottom, there are 'Hide SSID' and 'MAC Address Filtering' toggles, both set to 'Disabled', and a 'MAC Filter Table' link. 'Save' and 'reset' buttons are at the very bottom.

Wireless Card Information	
Wireless Operation	Factory Default = Enabled. When disabled, no stations will be able to connect to the Media Gateway.
Network Name (SSID)	This string, (32 characters or less) is the name associated with the AP. To connect to the AP, the SSID on a Station card must match the SSID on the AP card or be set to "ANY."
Channel	The AP transmits and receives data on this channel. The number of channels to choose from is pre-programmed into the AP card. Station cards do not have to be set to the same channel as the AP; the Stations scan all channels, and look for an AP to connect to.
Mode	This setting allows station to communicate with the Media Gateway. Possible Responses: Mixed: Station using any of the 802.11b, 802.11b+, and 802.11g rates can communicate with the Media Gateway. 11b only: Communication with Media Gateway is limited to 802.11b 11b+ : Stations using any of the 802.11b and 802.11b+ rates can communicate with the Media Gateway 11g only: Communication with Media Gateway is limited to 802.11g
4x Support	Factory Default = Disabled When selected, this enables/disables the 4X option. If enabled, 4X support provides additional algorithms for increased throughput. The station cards must also support this option.
Advanced Configuration edit button	Selecting this button allows access to the Wireless Advanced Configuration settings.
Privacy Settings	
Authentication Type	Factory Default = Open System Possible Response: Open System: Open System authentication is the default selection. Shared Key: To use Shared Key authentication, WEP must be enabled, and a valid WEP key must be present. Enabling WEP does not force the use of Shared Key authentication. It is permissible to have WEP enabled and still use Open System authentication.
WEP Security WEP Security WEP (Wired Equivalent Privacy)	Factory Default=DISABLED The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. If WEP is disabled, any station can connect to the AP (as long as its SSID matches the AP SSID). IF WEP is enabled, the risk of someone nearby accessing the AP is minimized.
Key Select	If selected, the WEP Key is treated as a string of text characters, and the number of characters must be either 5 (for 64-bit encryption) or 13 (for 128-bit encryption) or 29 (for 256-bit encryption). If not selected, the WEP key is treated as a string of hexadecimal characters, and the number of characters must be either 10 (for 64-bit encryption), 26 (for 128-bit encryption), or 58 (for 256-bit encryption). The only allowable hexadecimal characters are 0-9 and A-F. NOTE: The WEP key must be the same value and type for both Media Gateway and the wireless network adapter. "Pass Phrase" is not the same as "text" and should not be used.
Key Mapping Table button	Selecting this button will allows access to the Wireless Key Mappings settings.
Hide SSID	Factory Default = Disabled. If Enabled, Media Gateway will not broadcast the SSID. Stations must configure the SSID to match the Network Name (SSID) to connect to the Media Gateway.
MAC Address Filtering	Factory Default = Disabled. If Enabled, only the stations in the MAC Filter Table can connect to the Media

	Gateway.
MAC Filter Table button	Selecting this button allows access to the Wireless MAC Address Filter Table.

13.4.1 Wireless Advanced Configuration

The following screen will be displayed if you click on the **edit** button adjacent to **Advanced Configuration** in the **Wireless Configuration** screen.



WESTELL
Discover Better Broadband

Home Status Configuration Maintenance Troubleshooting Help

Wireless Advanced Configuration

Wireless Advanced Configuration

Beacon Period: 200 msec (range:1-65535)

RTS Threshold: 2347 bytes (range:0-2347)

Fragmentation Threshold: 2346 bytes (range:256-2346)

Preamble Algorithm: Local STA's

Slot Time Algorithm: Local STA's

PBCC Algorithm: Enhanced Dynamic

ERP Protection Algorithm: Dynamic

Rate Adaptation: Enabled

Rate Fallback: After 1 Retry

802.11b Rates(Mbps)
N - not supported
Y - supported
B - basic supported

[B] 1 [B] 2 [B] 5.5 [B] 11 [Y] 22

802.11g Rates(Mbps)
N - not supported
Y - supported
B - basic supported

[Y] 6 [Y] 9 [Y] 12 [Y] 18 [Y] 24 [Y] 36 [Y] 48 [Y] 54

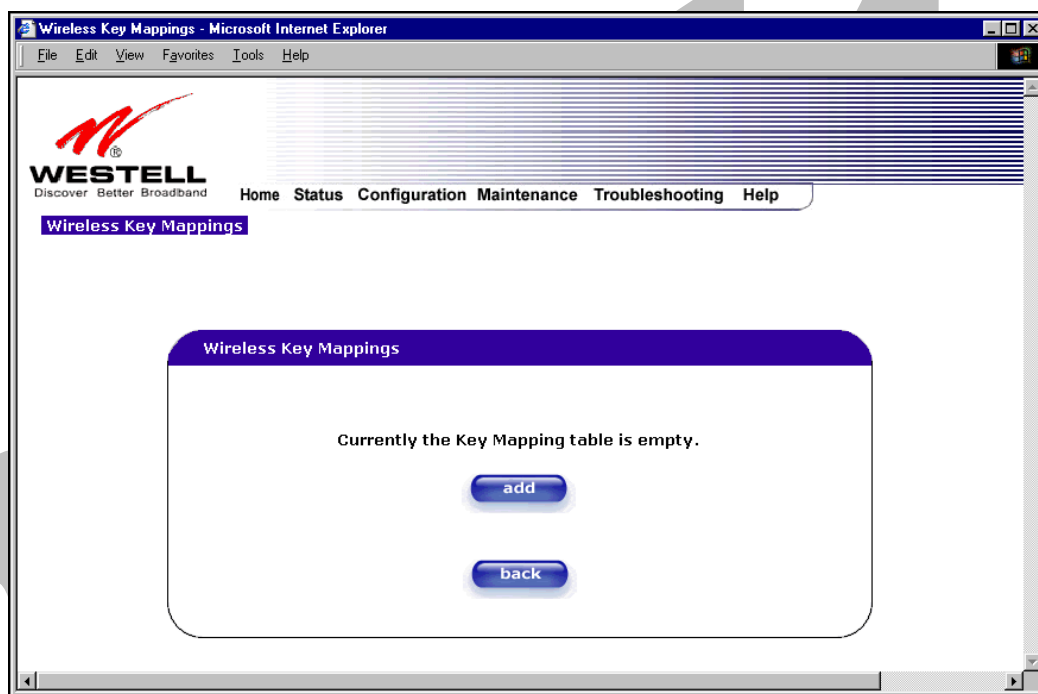
save reset back

Beacon Period	The time interval between beacon frame transmissions. Beacons contain rate and capability information. Beacons received by stations can be used to identify the access points in the area.
RTS Threshold	RTS/CTS handshaking will be performed for any data or management MPDU containing a number of bytes greater than the threshold. If this value is larger than the MSDU size (typically set by the fragmentation threshold), no handshaking will be performed. A value of zero will enable handshaking for all MPDUs.
Fragmented Threshold	Any MSDU or MMPDU larger than this value will be fragmented into an MPDU of the specified size.
Preamble Algorithm	Factory Default = Local STA's Possible Responses: Always Long: Transmissions are done using the long preamble algorithm. Always Short: Transmissions are done using the short preamble algorithm. Local STA's: If all associated stations support short preamble, then the short preamble algorithm is used. Otherwise, the long preamble algorithm is used.
Slot Time Algorithm	Factory Default = Local STA's

	<p>Possible Response:</p> <p>Always Off: Transmissions are done using a 20 usec slot time.</p> <p>Always ON: Transmissions are done using a 9 usec slot time (SST).</p> <p>Local STA's: If all associated stations support SST, then the 9 usec slot time is used. Otherwise, the 20 usec slot time is used.</p> <p>Enhanced Dynamic: Similar to Local STA's, with the following extension: If associated stations that do not support SST do not transmit for a period of time, the 9 usec slot time is used.</p>
PBCC Algorithm	<p>Factory Default = Enhanced Dynamic</p> <p>Possible Response:</p> <p>Always Off: PBCC is not used, operation at 22 Mbps is not possible.</p> <p>Always ON: PBCC is used.</p> <p>Local STA's: If all associated stations support PBCC, then PBCC is used. Otherwise, PBCC is not used.</p> <p>Dynamic: Similar to local STA's with the following extension: PBCC setting is also dependent on Beacon frames from overlapping BSS. If Beacon frames are received that do not support PBCC, then PBCC is not used.</p> <p>Enhanced Dynamic: Similar to Dynamic with the following extension: If associated stations that do not support PBCC do not transmit for a period of time, then PBCC is not used.</p>
ERP Protection Algorithm	<p>Factory Default = Dynamic</p> <p>Possible Response:</p> <p>Always Off: ERP is not used</p> <p>Always ON: ERP is used.</p> <p>Local STA's: If there are any associated stations that do not support ERP, a protection algorithm is used to prevent contention.</p> <p>Dynamic: Similar to local STA's with the following extension: The ERP protection setting is also dependent on Beacon frames from overlapping BSS. If Beacon frames are received that indicate ERP is not supported, then a protection algorithm is used.</p> <p>Enhanced Dynamic: Similar to Dynamic with the following extension: If associated stations that do not support ERP do not transmit for a period of time, then protection algorithm is not used.</p>
Rate Adaptation	<p>Factory Default = Enable</p> <p>If disabled, the highest rate shared between Media Gateway and STA is used for each transmission.</p>
Rate Fallback	<p>Factory Default = After 1 Retry</p> <p>The number of retries to attempt before falling back to the next lower rate. If Fallback is disabled, the starting rate is the only rate tried. If Rate Adaptation is also disabled, the maximum rate shared with the STA is always the starting rate and the only rate tried. This may not work in noisy environments, and will reduce roaming distances.</p> <p>Possible Response: After 1 Retry/ Disable/ After 1 Retry/ After 2 Retry</p>
802.11b Rates (Mbps) 802.11g Rates (Mbps)	<p>These are the allowable communication rates that Media Gateway will attempt to use. The rates are also broadcast within the connection protocol as the rates supported by the Media Gateway.</p>

13.4.2 Wireless Key Mappings

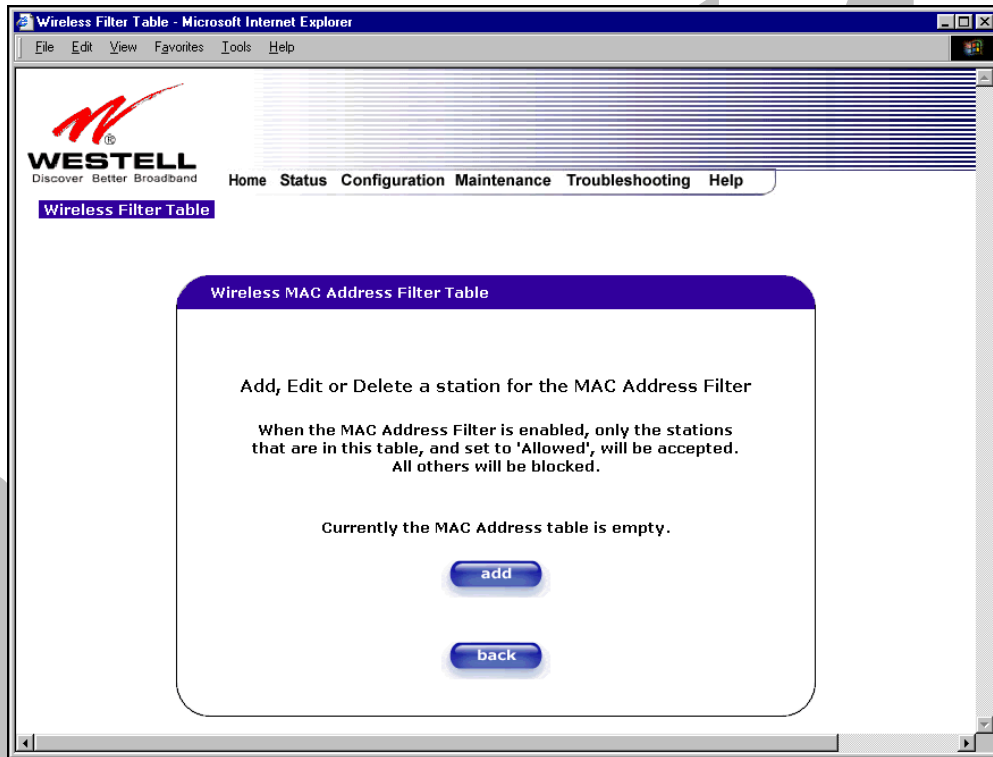
The following screen will be displayed if you click on the **edit** button adjacent to **Key Mapping Table** in the **Wireless Configuration** screen.



WEP Key	Select Enable if you want this WEP key enabled for the listed MAC Address.
MAC Address	The MAC address assigned to the station for which you want to assign a WEP key.
Key Length	The number of bits the encryption is going to use for WEP. The options are 64, 128, or 256 bits.
Key Value	The WEP key to be used for this station.

13.4.3 Wireless Filter Table

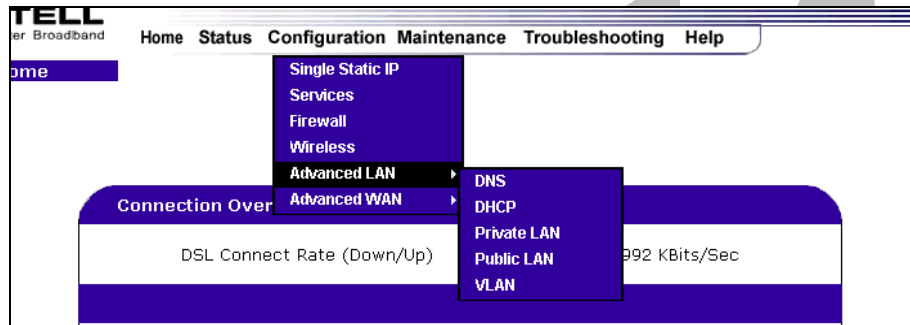
The following screen will be displayed if you click on the **edit** button adjacent to **MAC Filter Table** in the **Wireless Configuration** screen.



Traffic	Allowed: When the MAC Filter is enabled, only stations in the MAC Filter Table (which are set to “Allowed”) will have access to the AP. Blocked: This allows the station to remain in the table, but no access to the Media Gateway is allowed.
MAC Address	The MAC address assigned to the station that you want to allow access to.
Station Name	The station name or description that the MAC address is assigned to. This is an optional field that is useful in identifying the station.

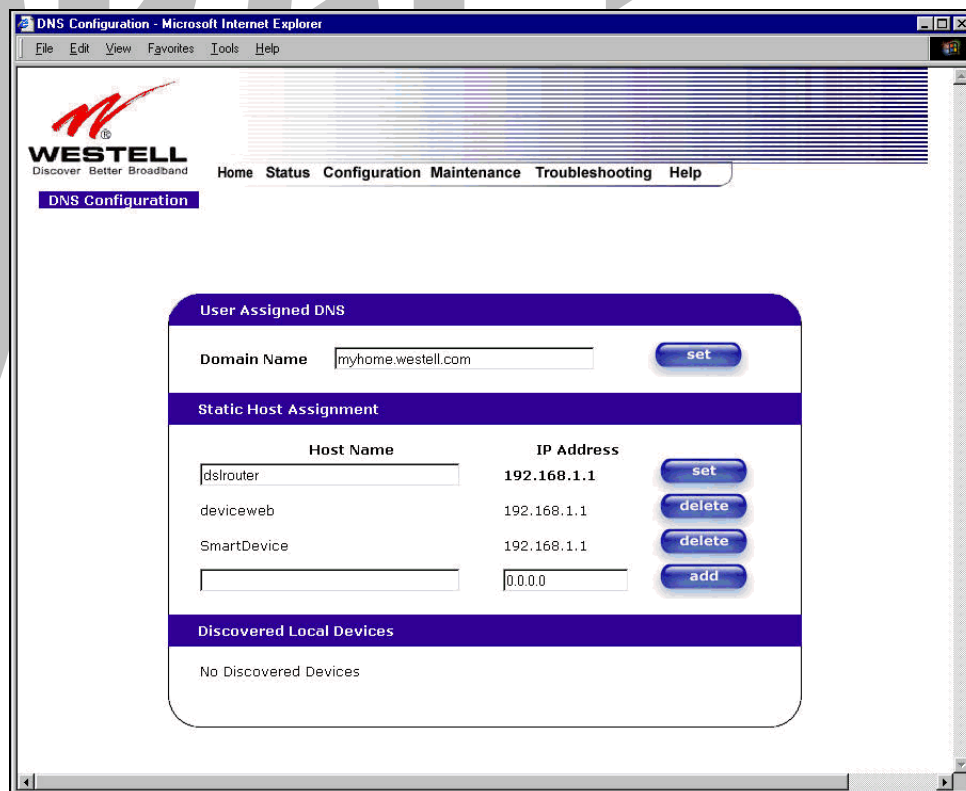
13.5 Advanced LAN

This section explains the configurable features of Media Gateway that are available if you select **Advanced LAN** from the **Configuration** menu.



13.5.1 DNS Configuration

The following settings will be displayed if you select **DNS** from the **Advanced LAN** menu.



User Assigned DNS	
Domain Name	This field allows you to enter a Domain Name for the Media Gateway.
NOTE: Your ISP may	To add a Domain Name, in the field under User Assigned DNS, type in your