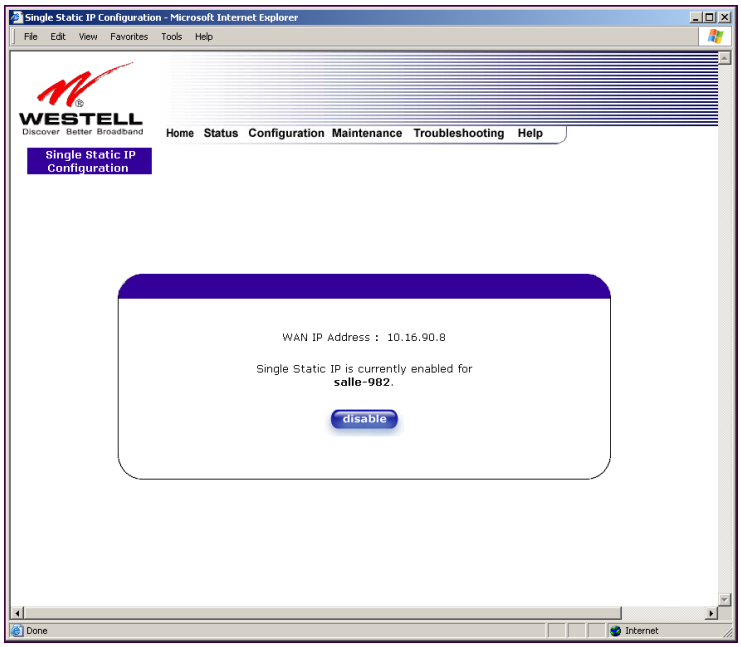
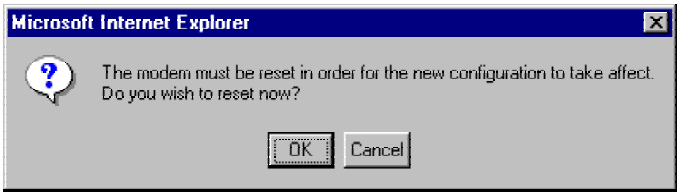
13.1.2 Disabling Single Static IP – Single IP Address PassThrough

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

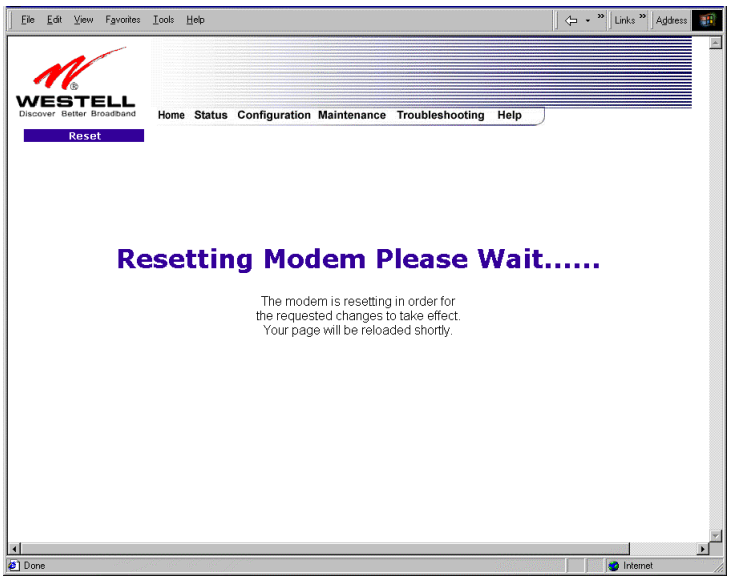


If you clicked **disable** in the preceding screen, the following pop-up screen will be displayed. Click on **OK.**

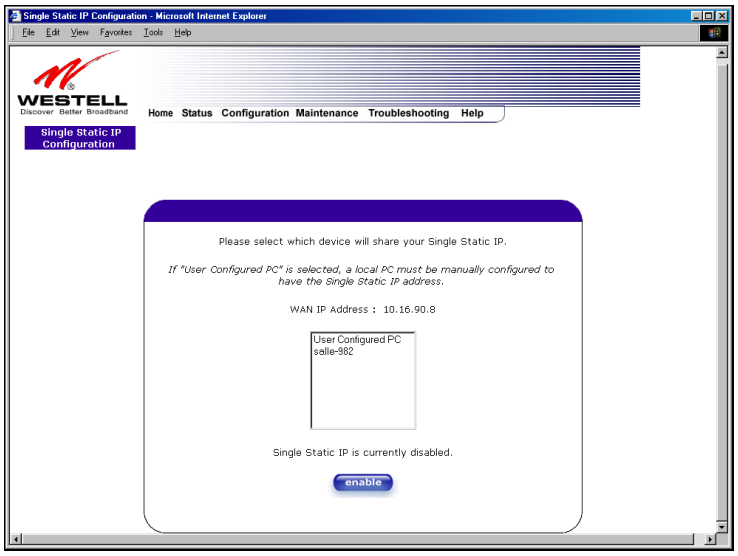
If you clicked **OK** in the **Disable IP Passthrough?** screen, the following pop-up screen will be displayed. This screen will allow the modem to be reset and the new configuration will take effect. Click on **OK.**



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



After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and 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.

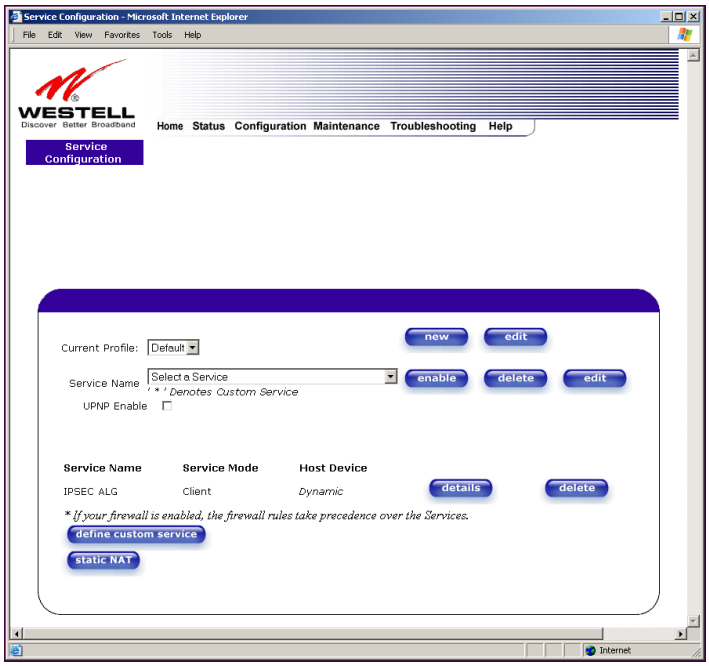
13.2 Service Configuration

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 the Router 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.



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 your Router.
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 your Router

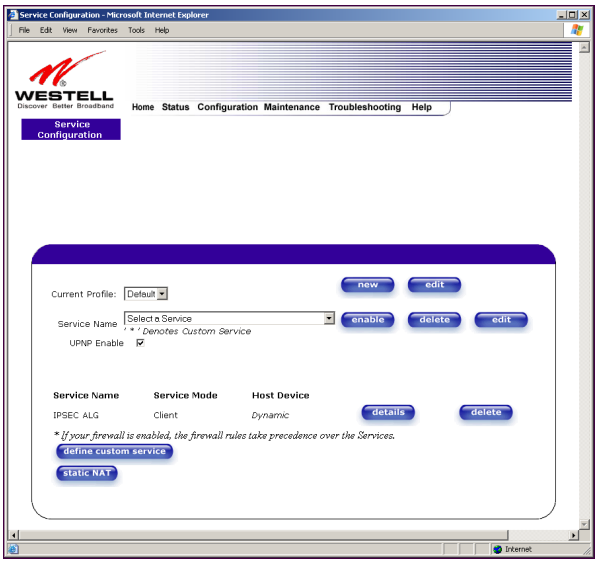
Note: To use the UPNP functionality in the Router, your Windows XP operating system must also support UPNP. Please contact your computer manufacturer to verify that UPNP is enabled in your Windows XP operating system.

To enable UPNP on the Router perform the following steps:

1) Select **Services** from the Configuration menu.
2) Click the **UPNP Enable** box in the **Service Configuration** screen. A check mark will appear in the box.
3) Follow the instructions in the pop-up screens.
4) Click **OK** to reset the Router.

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

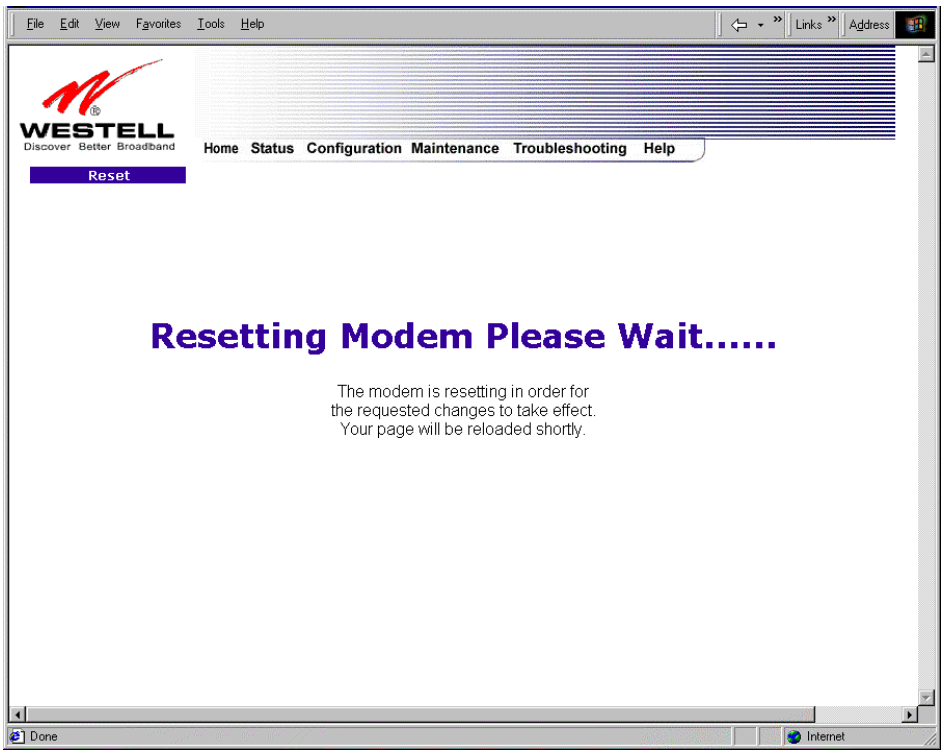
If you click the **UPNP Enable** box in the **Service Configuration** screen, a check mark will appear in the box, as shown below.



And the following pop-up screen will be displayed. Click on **OK.**

If you clicked **OK** in the preceding screen, the following screen will be displayed. Click on **OK** to reset the Router.

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



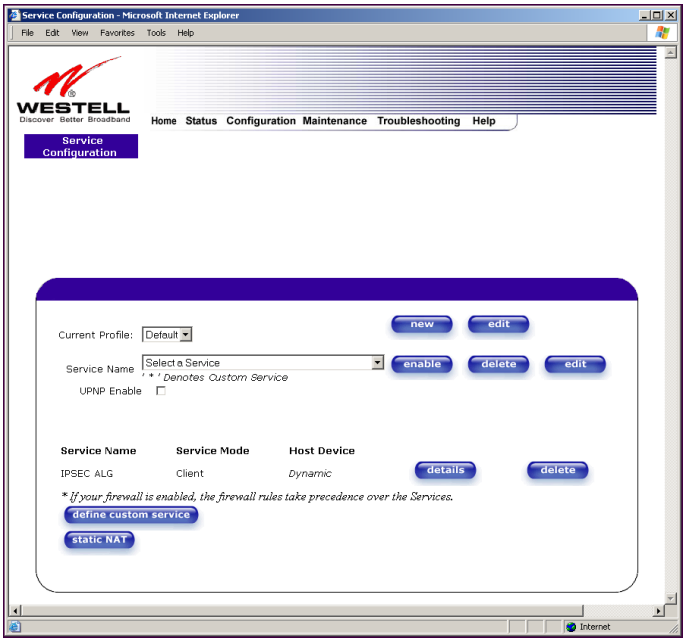
After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP.** (Click the **connect** button to establish a PPP session).

13.2.2 Creating a New NAT Service Profile

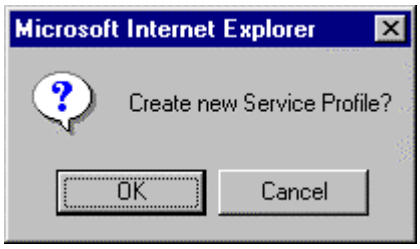
NAT Profiles allow you to create specific service settings. The NAT profile may then be associated with a connection profile, allowing you to customize profiles for specific users. For example, if you want to attach specific NAT services to a profile, or if you want to set up a different connection setting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

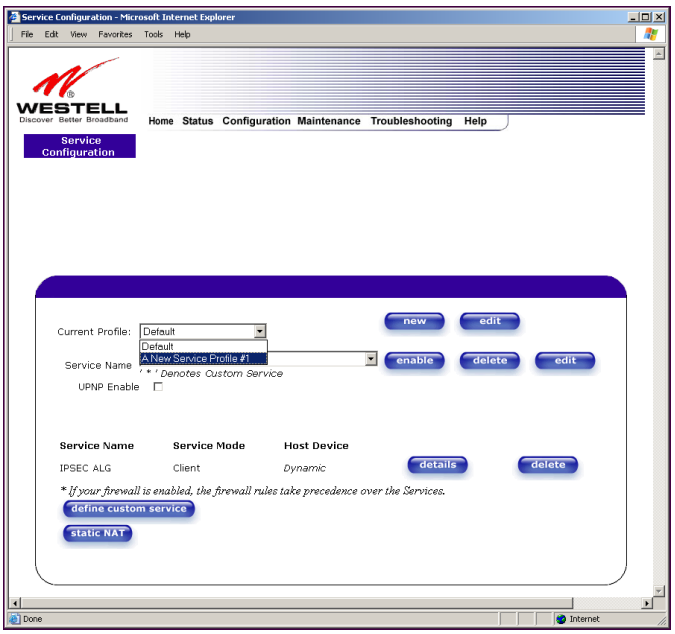
To create a new NAT profile, click **new** in the **Service Configuration** screen.



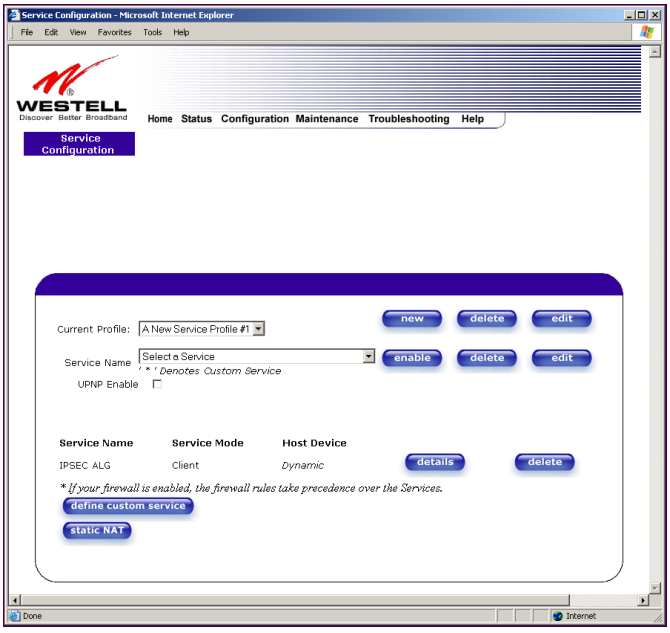
If you selected **new** from the preceding **Service Configuration** screen, the **Create new Service Profile?** pop-up screen will be displayed. Click on **OK** to begin creating your new NAT service profile. Click **Cancel** if you do not want to create a new NAT service profile.



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



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.



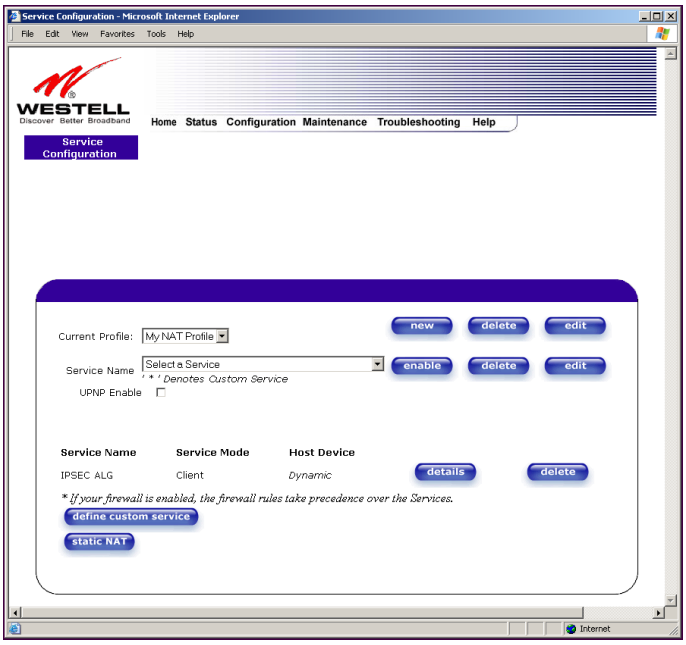
13.2.3 Editing a NAT Service Profile

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 add NAT services to or delete them from your 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 profile, click on **save.** If you do not want to save the new NAT profile, click **close**.

If you clicked **save** in the **Edit Service 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

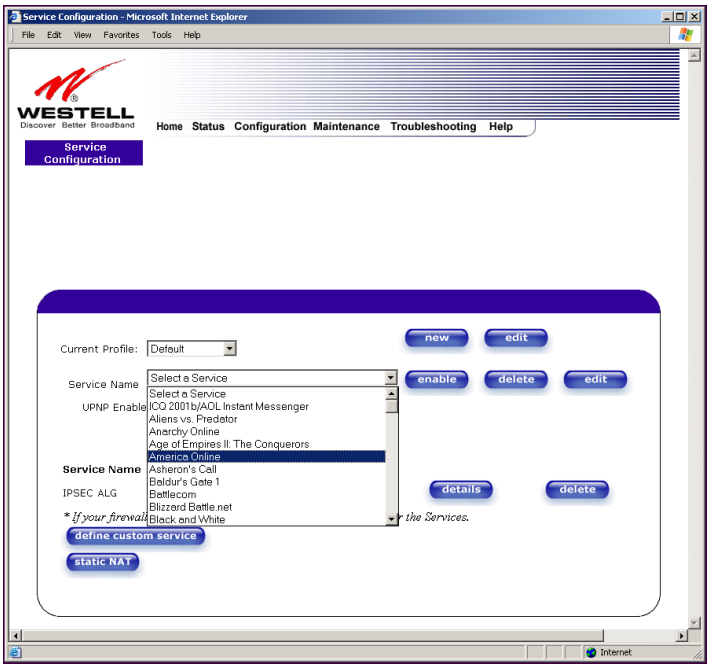
This section explains how to add NAT services to your NAT service profile. Remember, you may attach an unlimited number of NAT services to any profile.

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 the Router 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). **IPSEC ALG** is the Router's factory default NAT service.

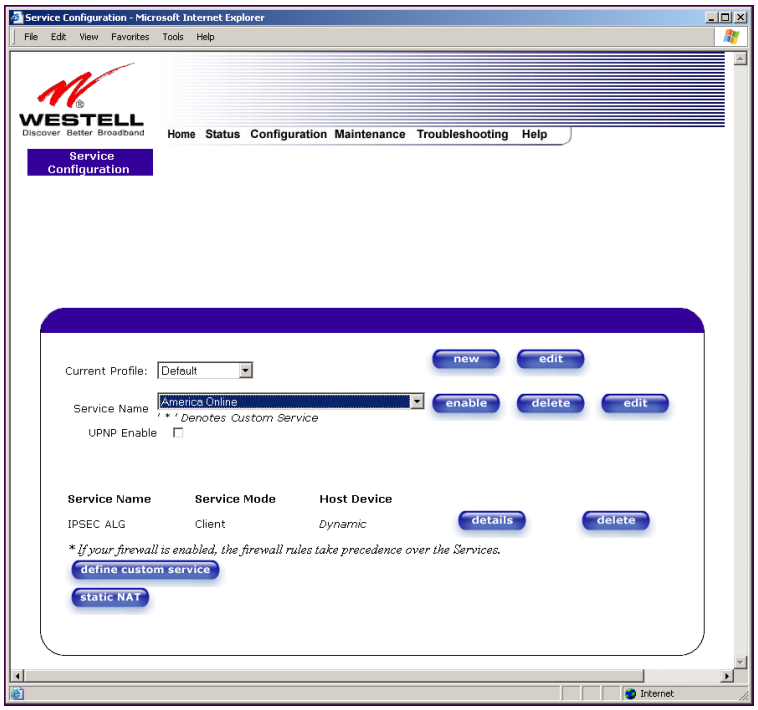
To add a NAT service, select **Services** from the **Configuration** menu. Next, Select a NAT service from the options provided at the **Service Name** drop-down arrow.

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 (Creating a New NAT Service Profile).

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

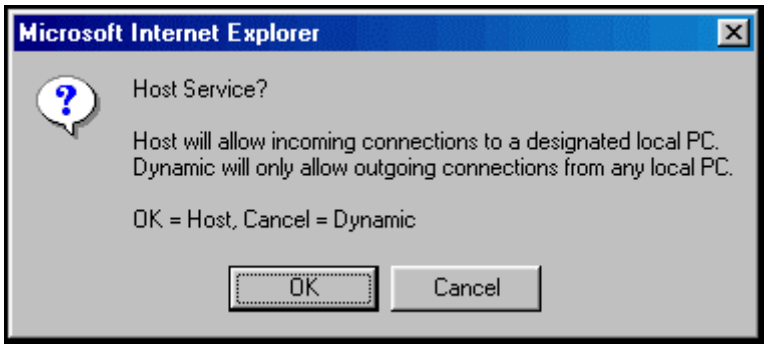


For example, the screen below displays **America Online** as the NAT service selected. After you have selected a service, click **enable.**

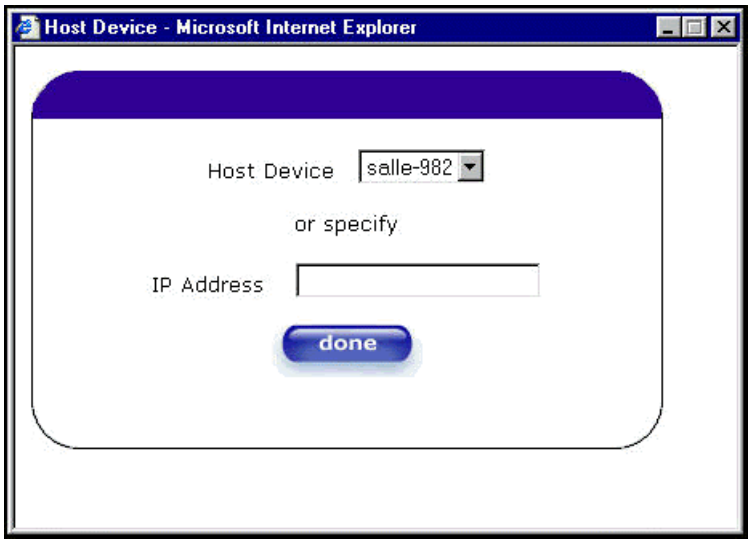


If you click **enable**, the following pop-up screen will be displayed. If you click **OK**, you will allow incoming connections to be forwarded to a designated local PC. If you click **Cancel**, you will allow only outgoing connections from any local PC. Click **OK** or click **Cancel.**

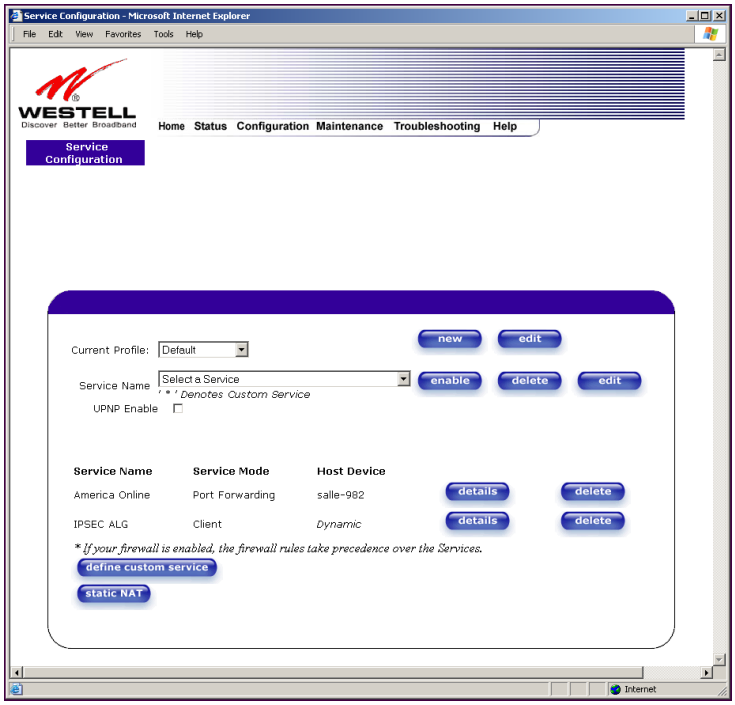
NOTE: If you click **Cancel** in the following pop-up screen, the NAT service you selected in the **Service Configuration** screen is still configured; however, it will not be assigned to any device on the local LAN. You must click **OK** to host the NAT service.



If you clicked **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.**



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.



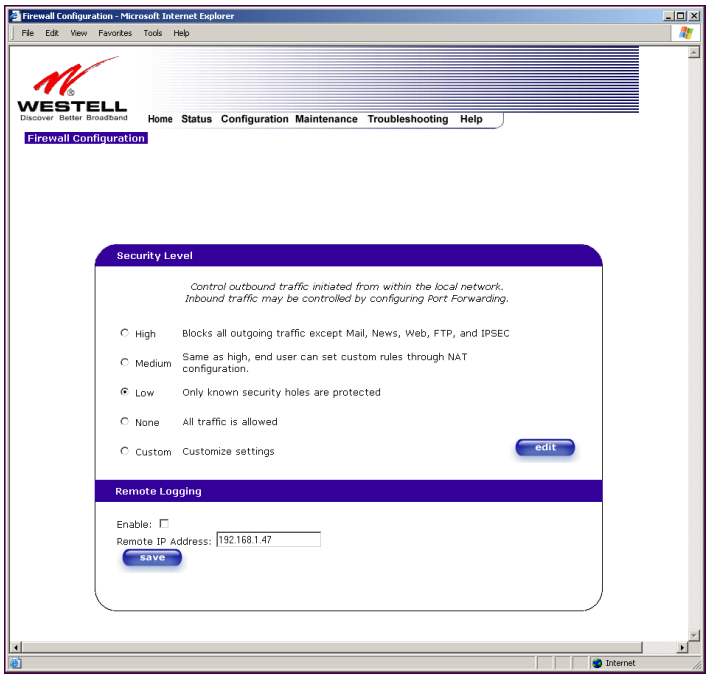
If you select the **details** button in the **Service Configuration** screen, the following screen will display the details of the selected NAT service. If you click on the **delete** button in the **Service Configuration** screen, you will remove that NAT service from your NAT service profile. Click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

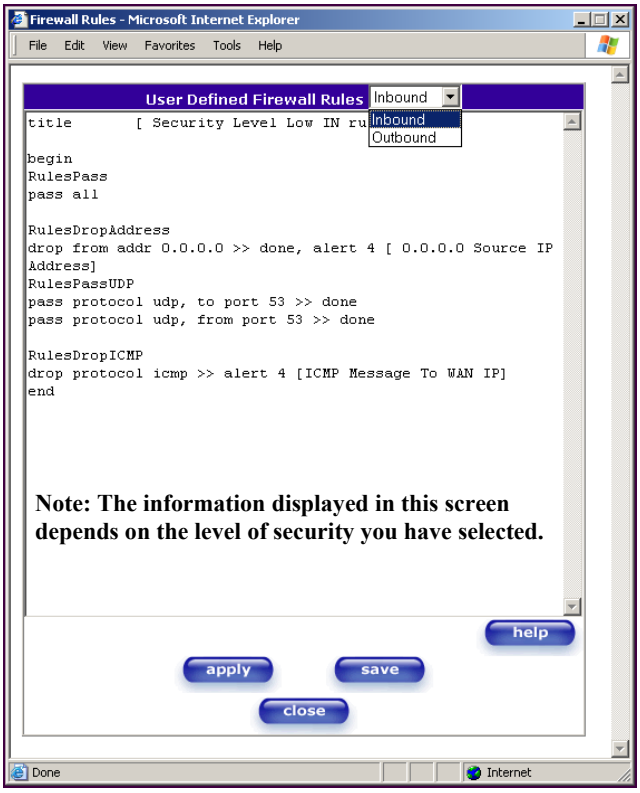
NOTE: Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset the Router to factory default settings, push the reset button on the rear of the Router.



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	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	Factory Default = Low The Low security setting will allow all traffic except for known attacks. With Low security, the Router 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, the Router 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.

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**.

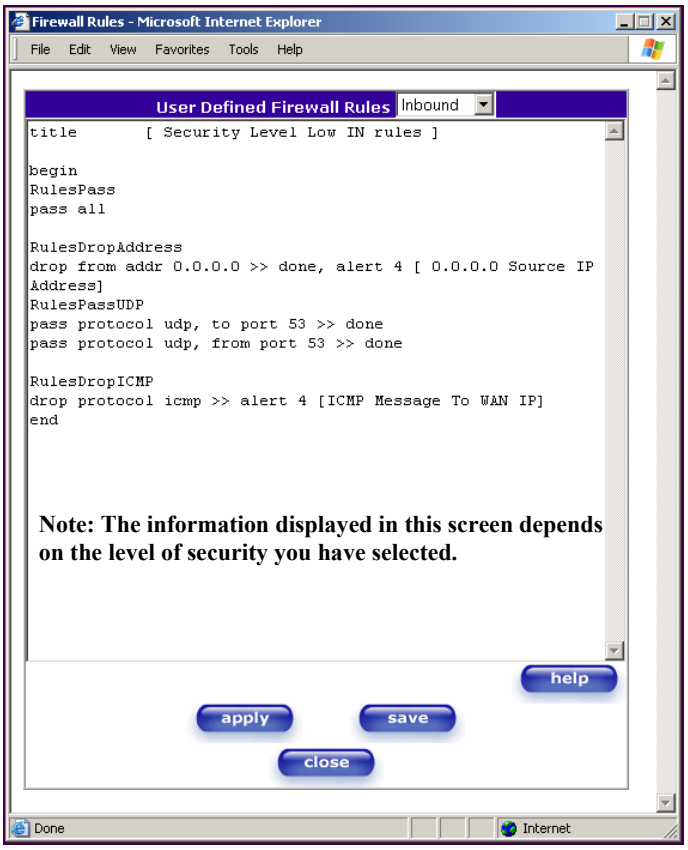
The information displayed in the following screen depends upon the Firewall security setting you have selected. If you selected "None" in the preceding Firewall **Security Level** screen, no values will be displayed in the following **User Defined Firewall Rules** screen.



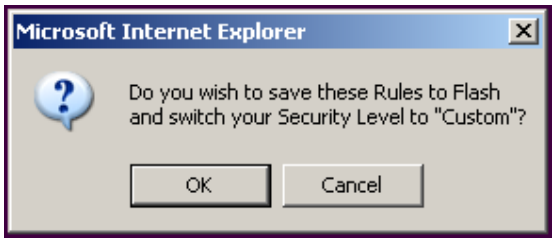
If you clicked **Apply** in the **User Define Firewall Rules** screen, the following pop-up screen will be displayed. Click on **OK** if you want your new firewall setting to take effect. If you click **Cancel**, your new firewall settings will not take effect.

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

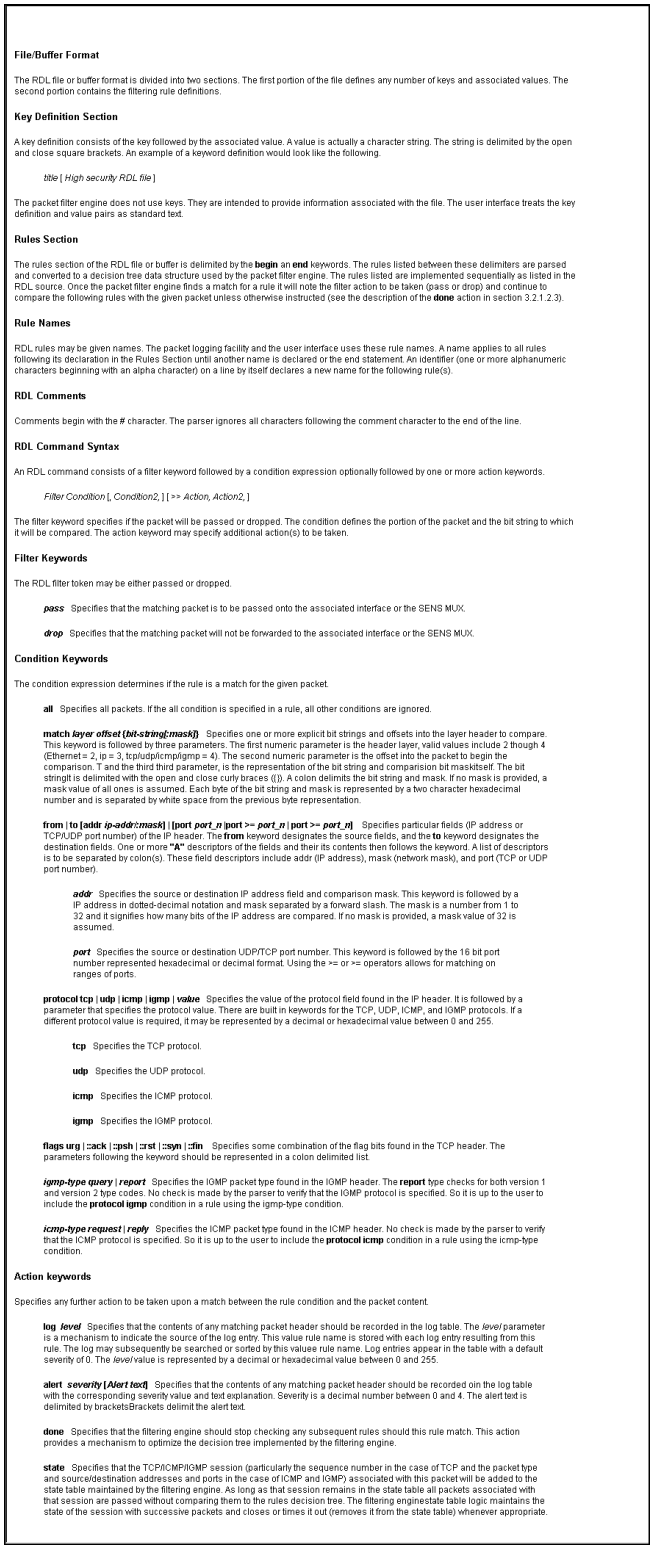
NOTE: Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset the Router to factory default settings, push the reset button on the rear of the Router.



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.



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.

title [*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** an **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 though 4 (Ethernet = 2, ip = 3, tcp/udp/icmp/igmp = 4). The second numeric parameter is the offset into the packet to begin the comparison. T and the third third parameter, is the representation of the bit string and comparision bit mask itself. The bit string it 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 *ip-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 **"A"** descriptors of the fields and their its 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 | :psh | :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.

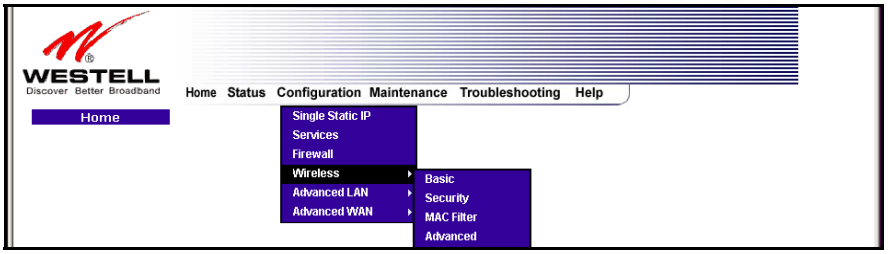
log *level* Specifies that the contents of any matching packet header should be recorded in the log table. The *level* parameter is a mechanism to indicate the source of the log entry. This value rule name is stored with each log entry resulting from this rule. The log may subsequently be searched or sorted by this valuee 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 oin 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 bracketsBrackets 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.

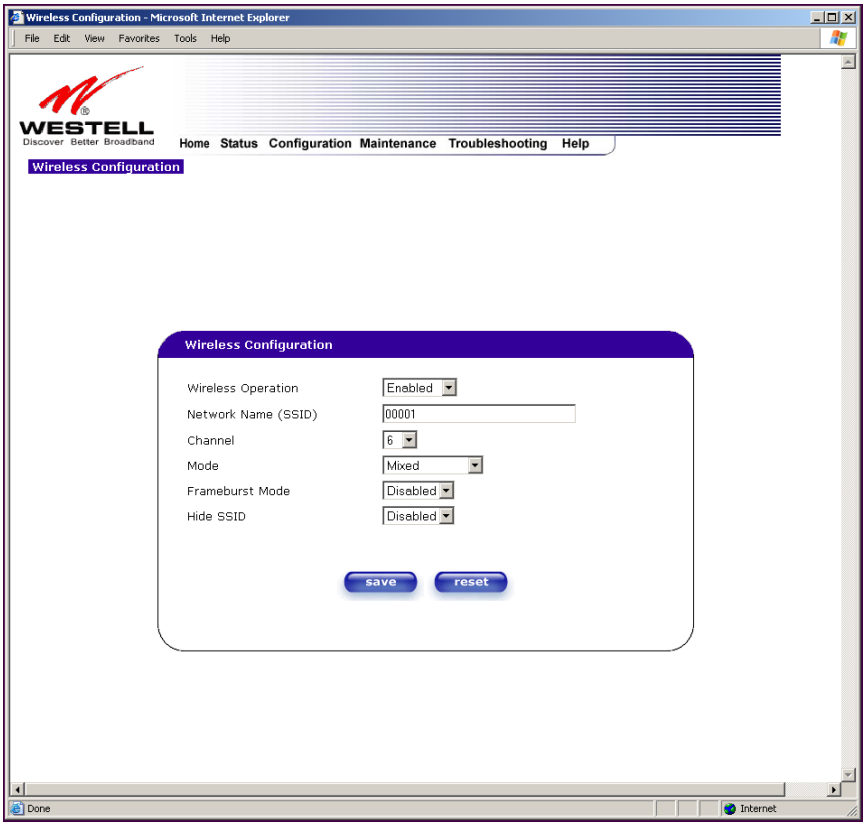
state Specifies that the TCP/ICMP/IGMP session (particularly the sequence number in the case of TCP and the packet type and source/destination addresses and ports in the case of ICMP and IGMP) associated with this packet will be added to the state table maintained by the filtering engine. As long as 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 enginestate 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 (Models 328W10, 328W11)



13.4.1 Wireless Basic

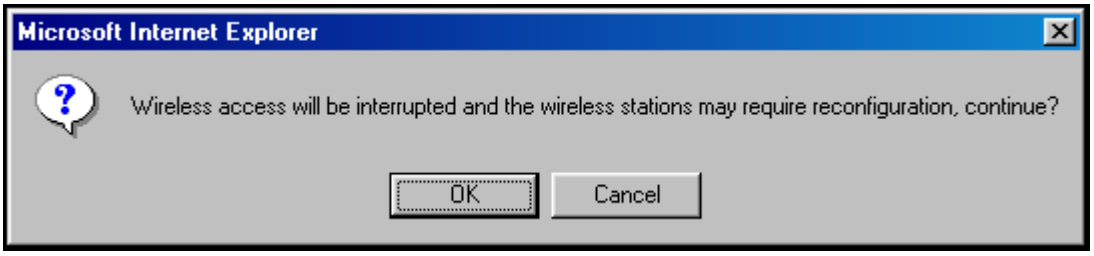
The following fields will be displayed if you select **Wireless** > **Basic** from the **Configuration** menu. If you change any settings in this screen, you must click **save** to save the settings.



IMPORTANT: If you are connecting to the Router via a wireless network adapter, the service set ID (SSID) must be the same for both the Westell Router and your PC's wireless network adapter. The default SSID for the Router 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 Router) before you begin the Router's account setup and configuration procedures. For privacy, you should change the **Network Name (SSID)** value in the **Wireless Configuration** screen to your desired value.

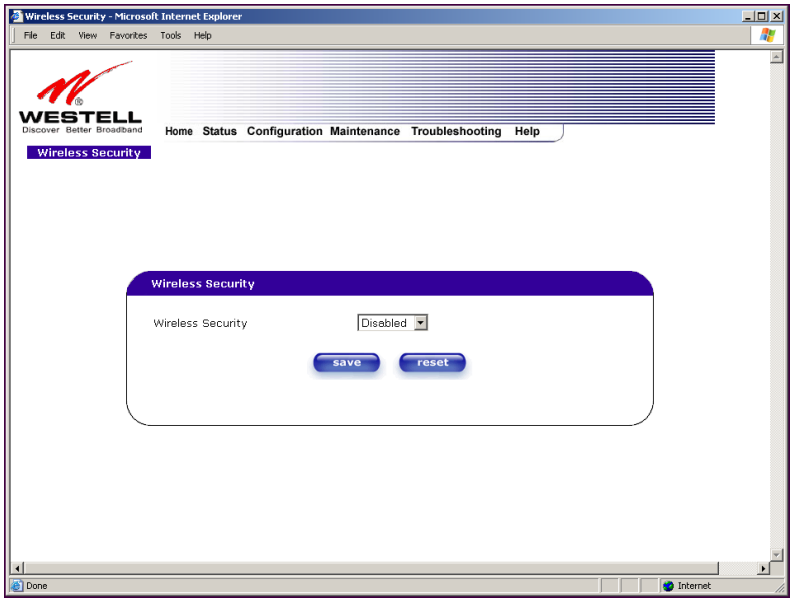
Wireless Configuration	
Wireless Operation	Factory Default = Enabled. When disabled, no stations will be able to connect to the Router.
Network Name (SSID)	This string, (32 characters or less) is the name associated with the AP. To connect to the AP, the SSID on a Station card must match the SSID on the AP card or be set to "ANY."
Channel	Factory Default = 6 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	Factory Default = Mixed This setting allows station to communicate with the Router. Possible Responses: Mixed: Station using any of the 802.11b, 802.11b+, and 802.11g rates can communicate with the Router. Legacy Mixed: Same as Mixed, but also allows older 802.11b cards to communicate with the Router. 11b only: Communication with the Router is limited to 802.11b 11b+: Stations using any of the 802.11b and 802.11b+ rates can communicate with the Router 11g only: Communication with the Router is limited to 802.11g
Frameburst Mode	Factory Default = Disabled When selected, this enables/disables the frameburst option. If enabled, additional algorithms are used for increased throughput.
Hide SSID	Factory Default = Disabled. If Enabled, the Router will not broadcast the SSID. Stations must configure the SSID to match the Network Name (SSID) to connect to the Router.

If you clicked **save** in the **Wireless Configuration** screen, the following pop-up will be displayed. Click **OK** to continue.



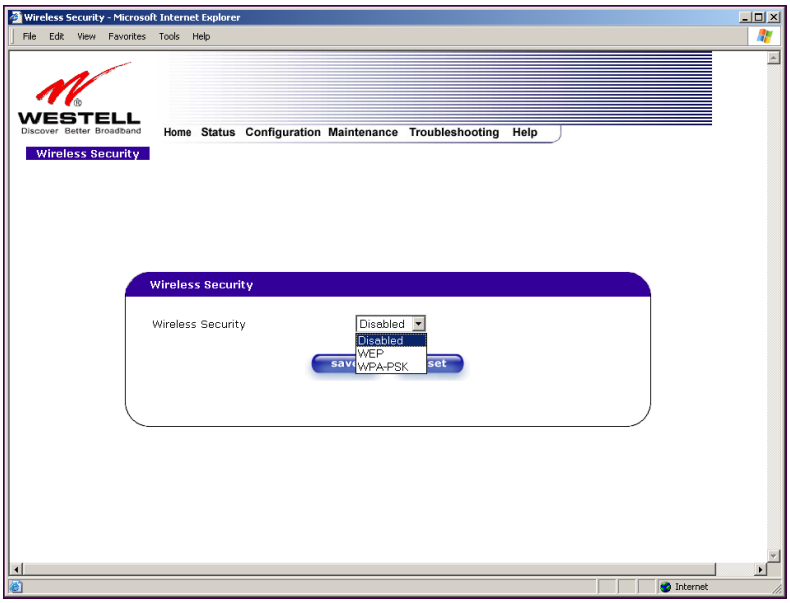
13.4.2 Wireless Security

The following screen will be displayed if you select **Wireless** > **Security** from the **Configuration** menu.



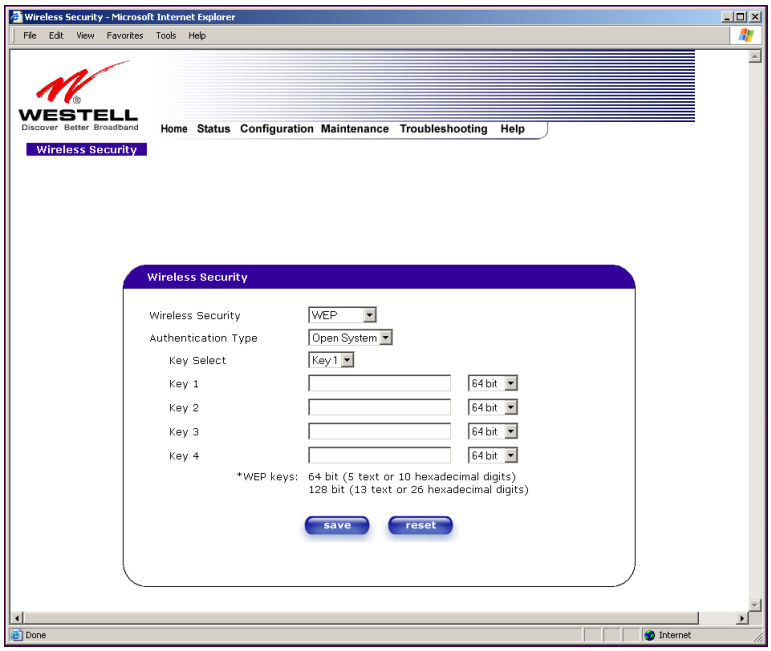
Select the desired security option from the **Wireless Security** drop-down menu.

IMPORTANT: Client PCs can use any Wireless Fidelity (Wi-Fi) 802.11b/g/g+ certified card to communicate with the Router. The Wireless card and Router must use the same security code type. **If you use WPA-PSK or WEP wireless security, you must configure your computer's wireless adapter for the security code that you use. You can access the settings in the advanced properties of the wireless network adapter.**



13.4.2.1 Enabling WEP Security

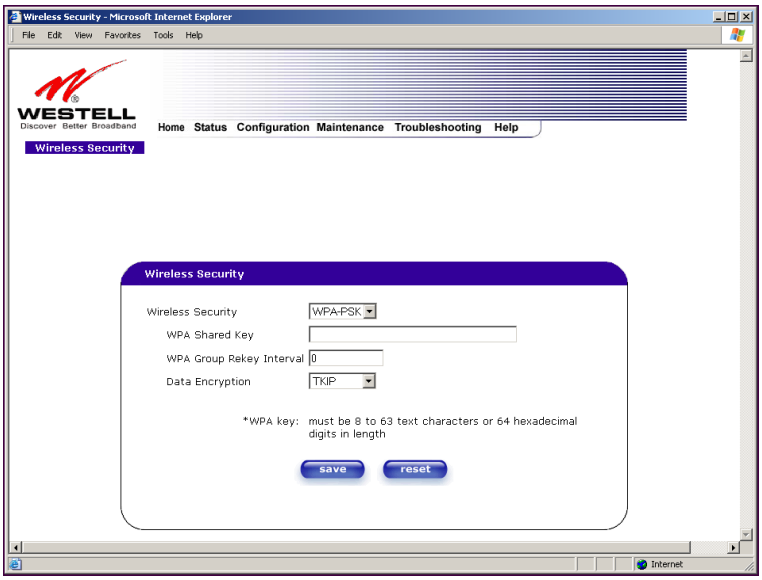
If you select **WEP** from the **Wireless Security** drop-down menu, the following screen will be displayed. After you have entered the appropriate values in the fields provided, click **save** to save the settings.



Wireless Security	
Wireless Security	Factory Default = Disabled. Possible Response: Disabled: If selected, wireless security will be disabled on the Router and any station can connect to the AP as long as its SSID matches the AP's SSID. WPA-PSK: Selecting this will enable you to set up WPA-PSK security on the Router. WEP: Selecting this will enable you to set up WEP security on the Router. The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. If WEP is selected, any station can connect to the AP (as long as its SSID matches the AP SSID). If wireless security is disabled, the risk of someone nearby accessing the AP is maximized.
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.
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 either be 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 the Router and the wireless network adapter. "Pass Phrase" is not the same as "text" and should not be used.

13.4.2.2 Enabling WPA-PSK Security

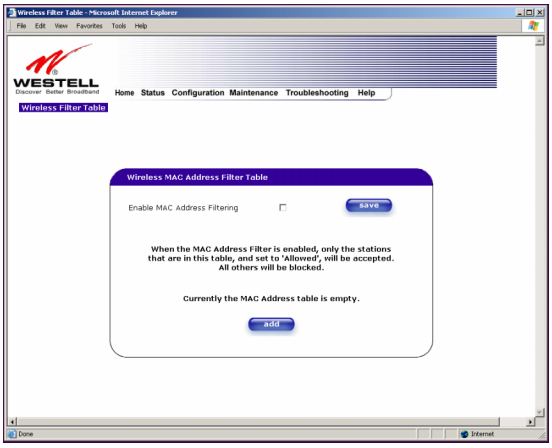
If you select **WPA-PSK** from the **Wireless Security** drop-down menu, the following screen will be displayed. After you have entered the appropriate values in the fields provided, click **save** to save the settings.



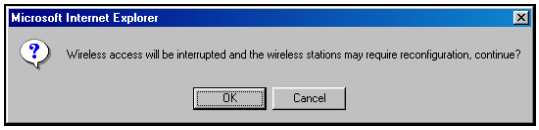
Wireless Security	
Wireless Security	Factory Default = Disabled. Possible Response: Disabled: Wireless security will be disabled on the Router. WPA-PSK: Selecting this will enable you to set up WPA-PSK security on the Router. WEP: Selecting this will enable you to set up WEP security on the Router. The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. If WEP is selected, any station can connect to the AP (as long as its SSID matches the AP SSID). If wireless security is disabled, the risk of someone nearby accessing the AP is maximized.
WPA Shared Key	This is a passphrase (also called a shared secret) that must be entered in both the wireless router and the wireless client. This shared secret can be between 8 to 63 text characters (or 64 hexadecimal characters) and can include special characters and spaces. The WPA Shared Key should be a random sequence of either keyboard characters (upper and lowercase letters, numbers, and punctuation), at lease 20 characters long, or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. The more random your WPA Shared Key, the safer it is to use.
WPA Group Rekey Interval	Factory Default = 3600 The number of seconds between rekeying the WPA group key. A zero “0” means that rekeying is disabled.
Data Encryption	Factory Default = TKIP Possible Respone: TKIP- Selecting this option enables the Temporal Key Integrity Protocol for data encryption. AES- Selecting this option enables the Advanced Encryption Standard for data encryption. TKIP/AES- Selecting this option enables the Router to accept either TKIP or AES encryption

13.4.3 Wireless MAC Filter Table

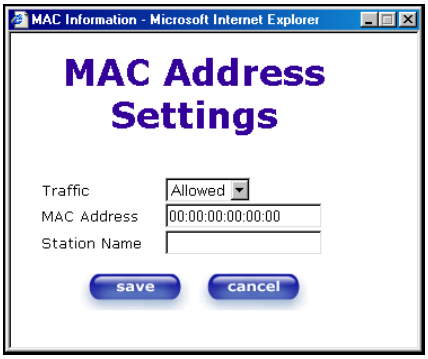
The following screen will be displayed if you select **Wireless** > **MAC Filter** from the **Configuration** menu. To enable MAC Address filtering, click the box adjacent to **Enable MAC Address Filtering**. A check mark will appear in the box. Next, click **save** to save the setting. To add or edit a MAC Address setting, click the **add** button.



If you clicked **save** in the **Wireless Filter Table** screen, following pop-up screen will be displayed. Click **OK** to continue.



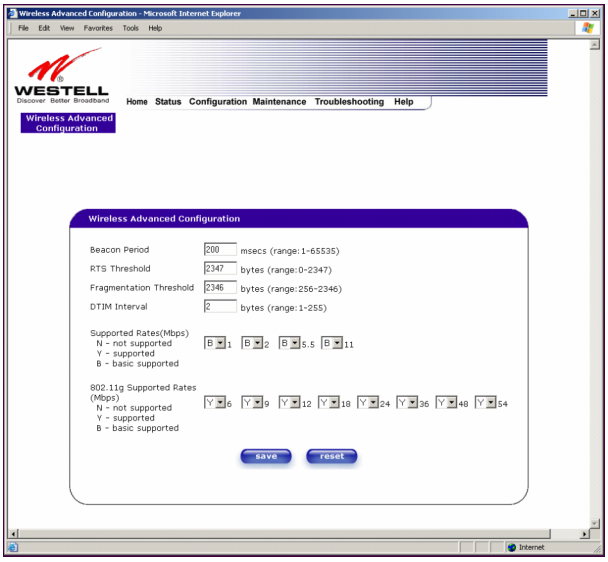
If you clicked **add** in the **Wireless Filter Table** screen, the following screen will be displayed. Enter the appropriate values for your MAC Address settings, and then click **save** to save the settings. Click **cancel** in this screen if you do not wish to add MAC Address setting.



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 Router 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.

13.4.4 Wireless Advanced Configuration

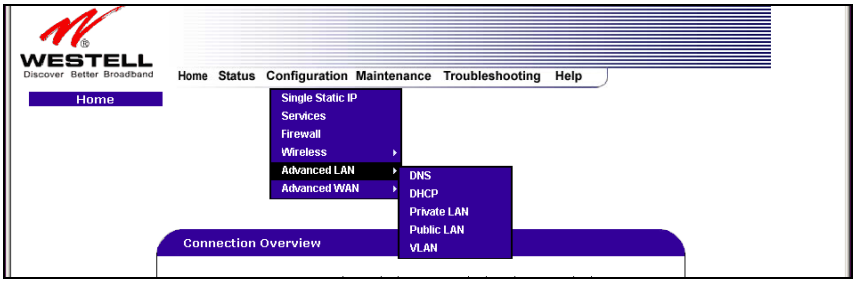
The following screen will be displayed if you select **Wireless** > **Advanced** from the **Configuration** menu. If you change the settings in this screen, you must click **save** to save the settings.



Wireless Advanced Configuration	
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.
DTIM Interval	The number of Beacon intervals between DTIM transmissions. Multicast and broadcast frames are delivered after every DTIM
Supported Rates 802.11b Rates (Mbps) 802.11g Rates (Mbps)	These are the allowable communication rates that the Router will attempt to use. The rates are also broadcast within the connection protocol as the rates supported by the Router.

If you clicked **save** in the preceding screen, the following pop-up screen will be displayed. Click **OK** to continue.

13.5 Advanced LAN

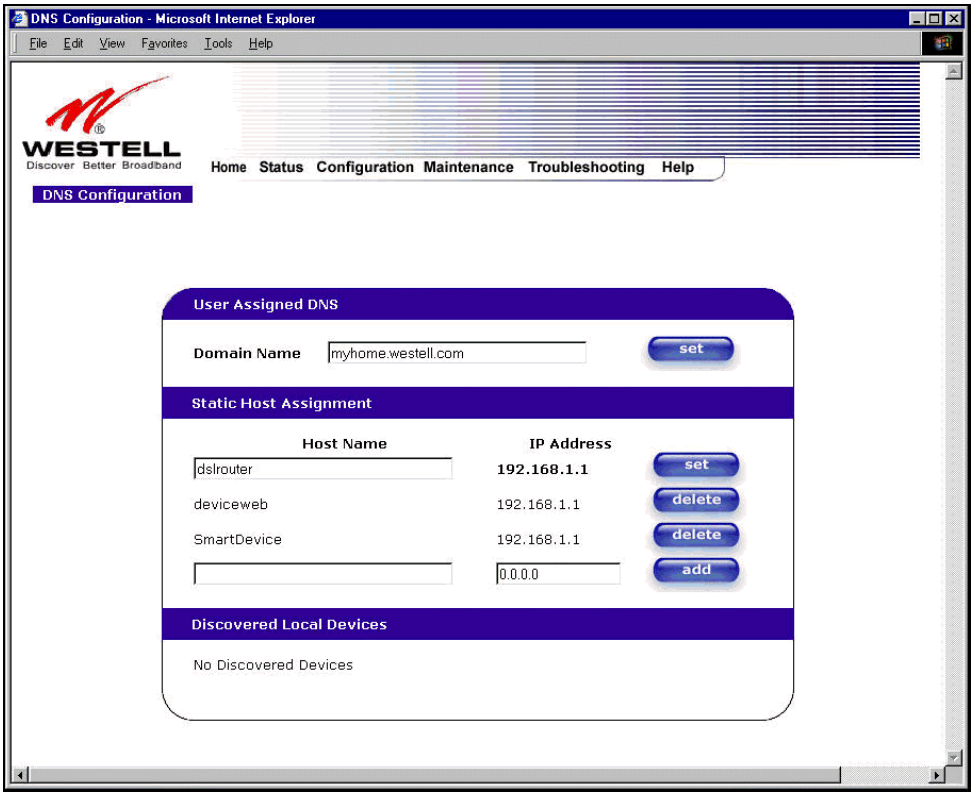


This section explains the configurable features of the Router that are available if you select **Advanced LAN** from the **Configuration** menu.

NOTE: If the Router is configured for **ETHERNET PORT 1**, **VLAN** will not be displayed. You must configure the Router for **DSLATM PORT** to access **VLAN** in the **Advanced LAN** drop-down menu. Refer to section 13.6.3.1 for details on enabling and disabling DSLATM PORT and ETHERNET PORT 1.

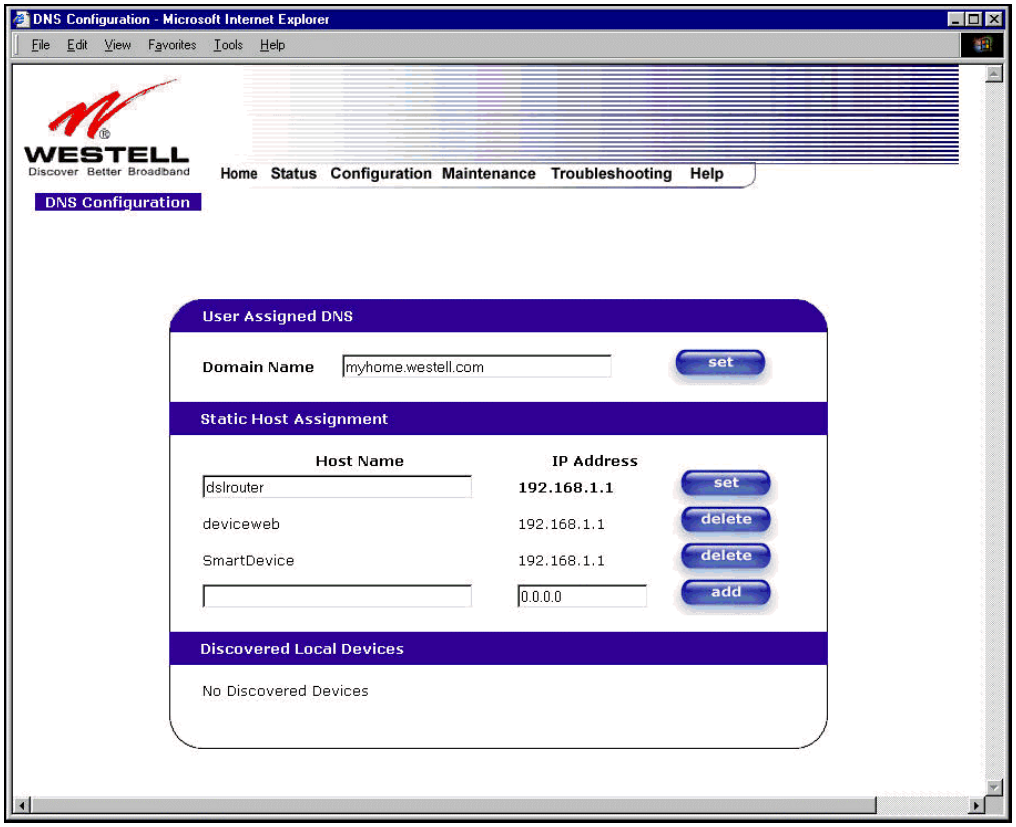
13.5.1 DNS Configuration

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

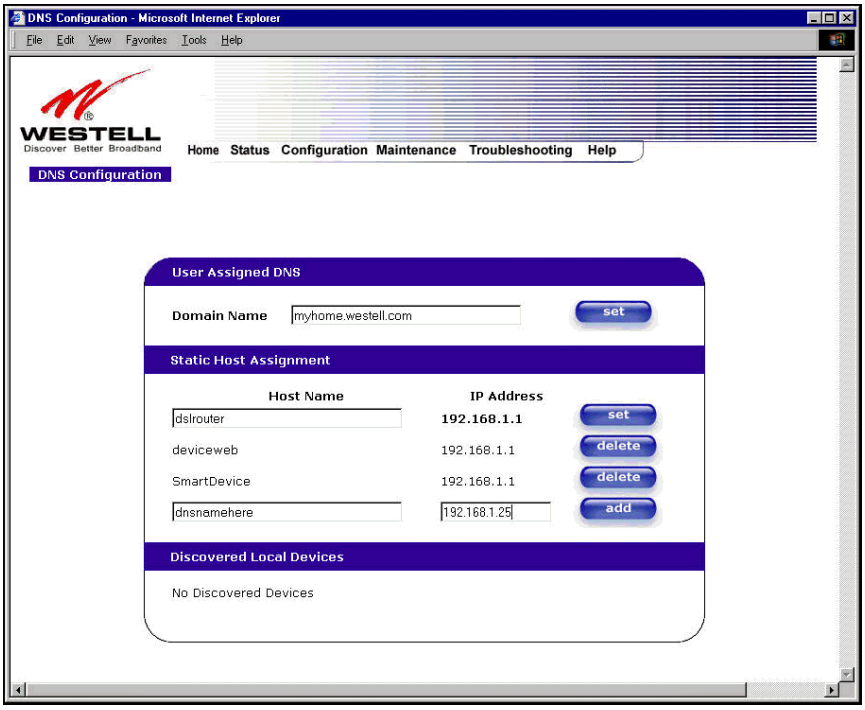


User Assigned DNS	
Domain Name NOTE: Some ISP's may require the name for identification purposes.	This field allows you to enter a Domain Name for the Router. To add a Domain Name, in the field under User Assigned DNS, type in your new domain name and click **Set.**
Static Host Assignment	
Host Name	This field allows you to enter a HOST name for the Router. To add a new Host name, in the field under Static Host Assignment, type in the Host Name and the IP address and click **Set.**
IP Address	Displays the IP address that is assigned to the Host Name.
Discover Local Devices	
This field displays a list of the computers on the LAN that were assigned a DHCP Address. The DNS name and IP address entry of each discovered device is displayed. (NOTE: The values in this field will be displayed barring any propagation delays. If 'No Discovered Devices' is displayed, manually refresh the screen.)	

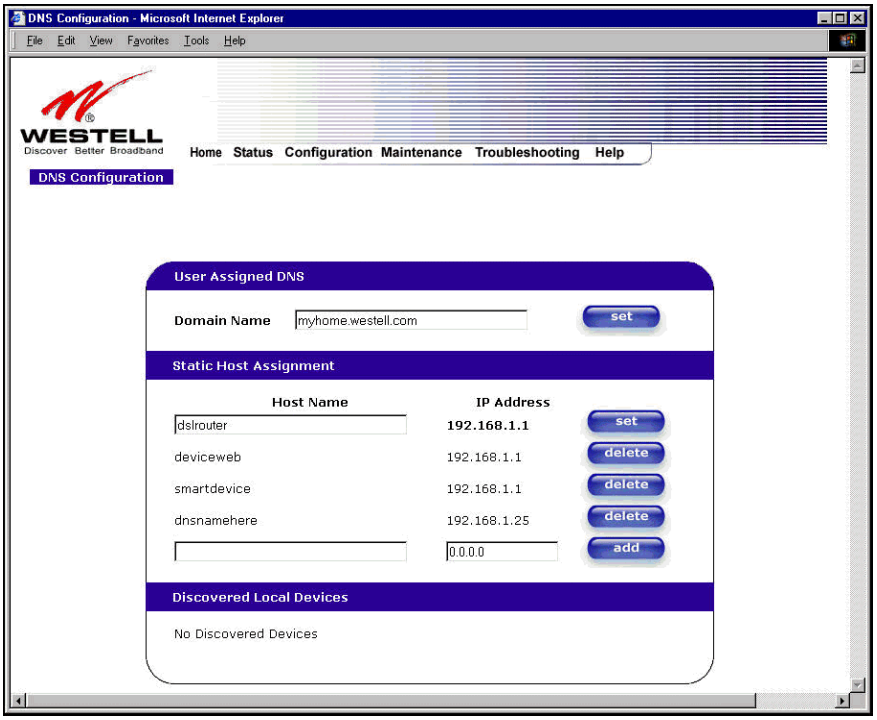
If you want to add a new Host Name and IP address to your DNS server, enter the Router's **Host Name** and **IP Address** in the fields provided in the **Static Host Assignment** section.



The following screen displays a **Host Name** and an **IP Address** in the fields. Now click on **add.**

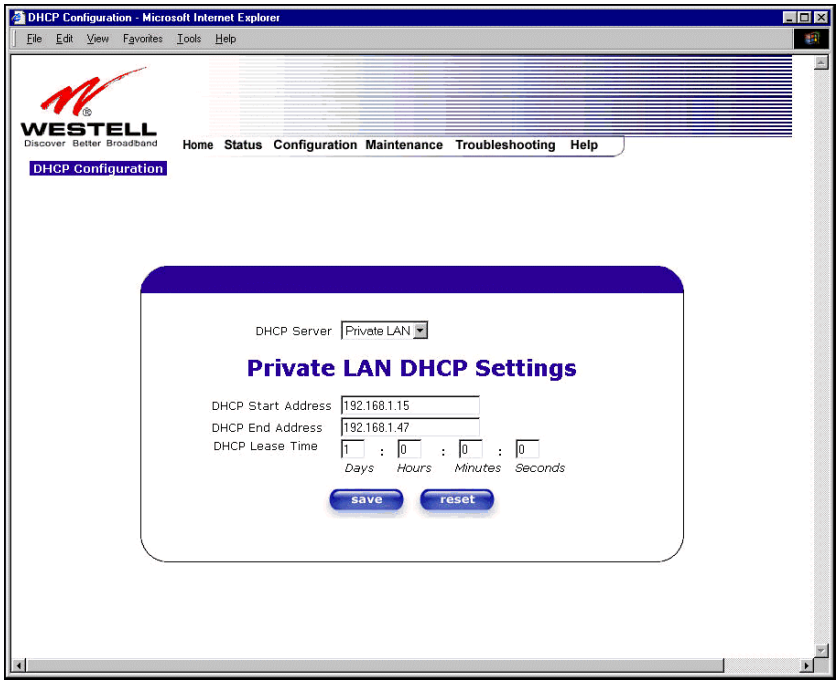


If you clicked **add**, the following screen will be displayed. The **Host Name** and **IP Address** have been added to the Static Host Assignment.



13.5.2 DHCP Configuration (Private LAN)

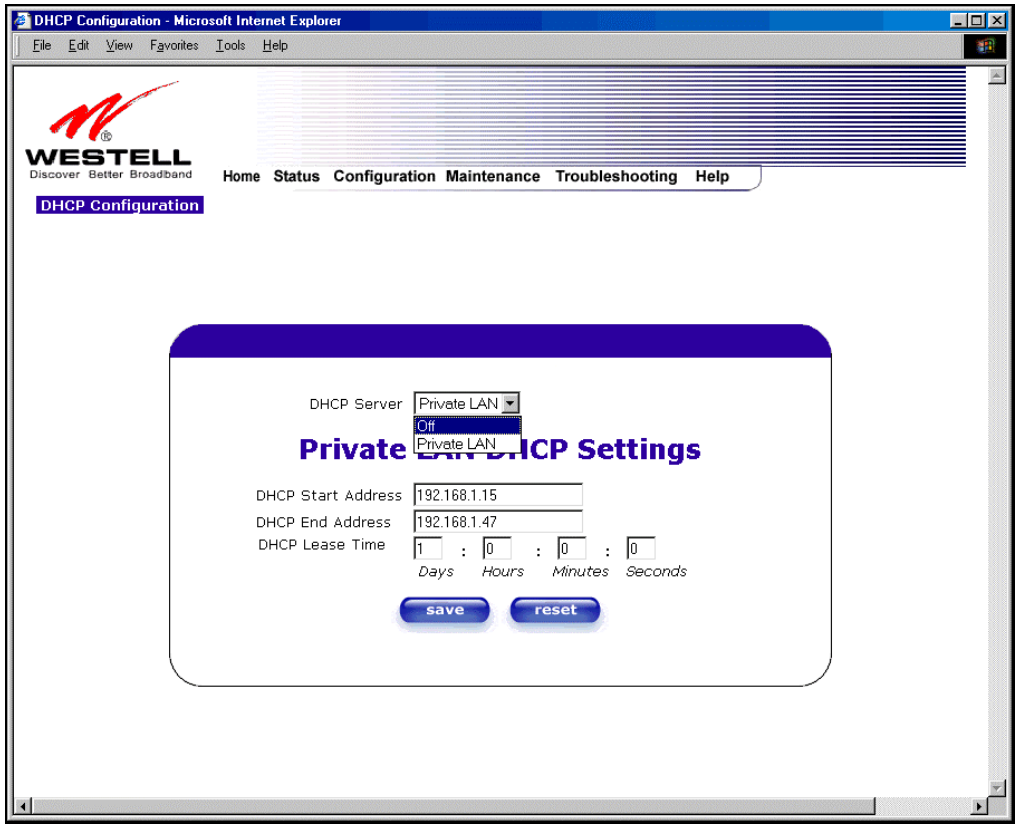
The following settings will be displayed if you select **Advanced LAN > DHCP** from the **Configuration** menu.



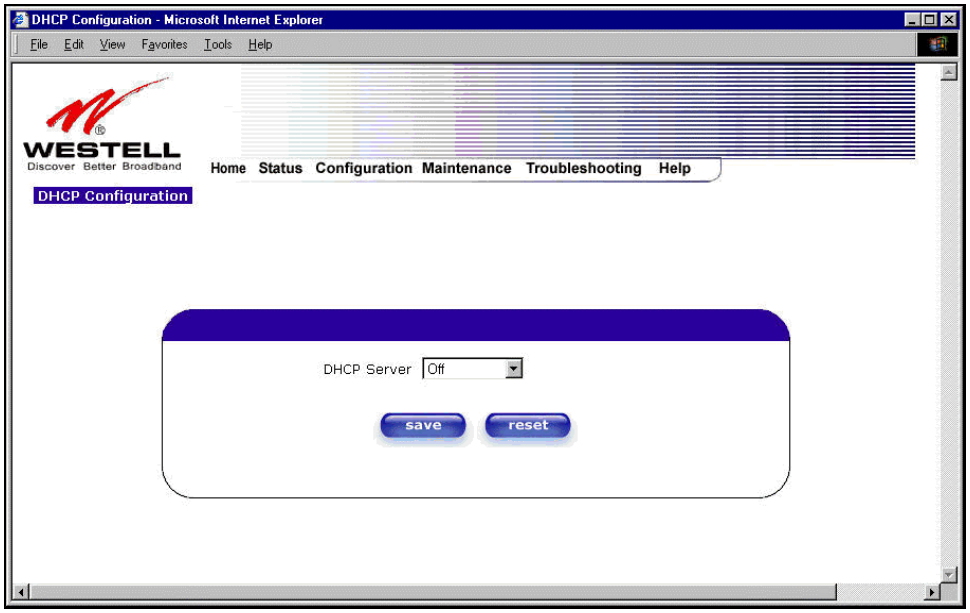
DHCP Server	This setting allows the Router to automatically assign IP addresses to local devices connected on the LAN. Westell advises setting this to enabled for the private LAN. Off = DHCP Server is disabled Private LAN = DHCP addresses will be saved into the Private LAN configuration. Public LAN = DHCP addresses will be saved into the Public LAN configuration. This option is only available if the Public LAN DHCP server is enabled. NOTE: These addresses will be overwritten if the Internet Service Provider supports dynamic setting of these values.
DHCP Start Address	Factory Default = 192.168.1.15 This field displays the first IP address that the DHCP server will provide. The DHCP Start Address must be within the IP address and lower than the DHCP End Address. You may use any number from 0 to 254 in this address.
DHCP End Address	Factory Default = 192.168.1.47 This field displays the last IP address that the DHCP server will provide. The DHCP End Address must be within the IP address and higher than the DHCP Start Address. You may use any number from 0 to 254 in this address.
DHCP Lease Time	Factory Default = 01:00:00:00 Displays the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request. NOTE: DHCP Lease Time is displayed in the format (dd:hh:mm:ss)*. This value 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. *(dd = days, hh = hours, mm = minutes, ss = seconds)

13.5.3 Disabling the DHCP Server

If you click on the drop-down arrow at **DHCP Server:,** a list of options will be displayed.
If you want to disable your DHCP server, select **Off** from the **DHCP Server** drop-down arrow. Click on **save.**



If you selected **Off** at **DHCP Server:,** the following screen will be displayed. Click on **save** to save the **DHCP Server** setting.



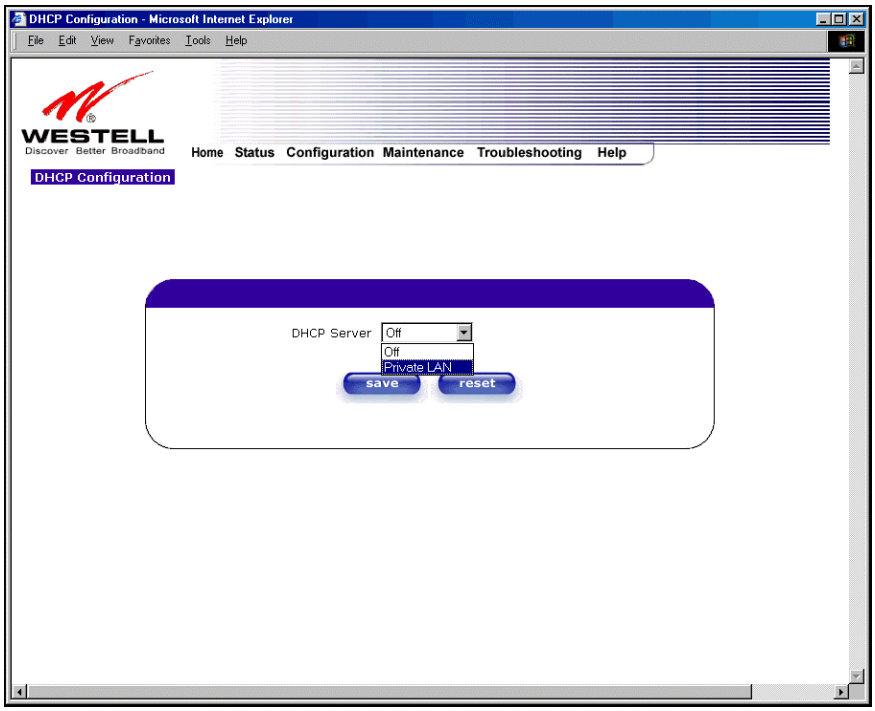
If you clicked on **save**, in the preceding **DHCP Configuration** screen**,** the following pop-up screen will appear. Click **OK.**

STOP: After you disable the DHCP server, you must reboot your PC

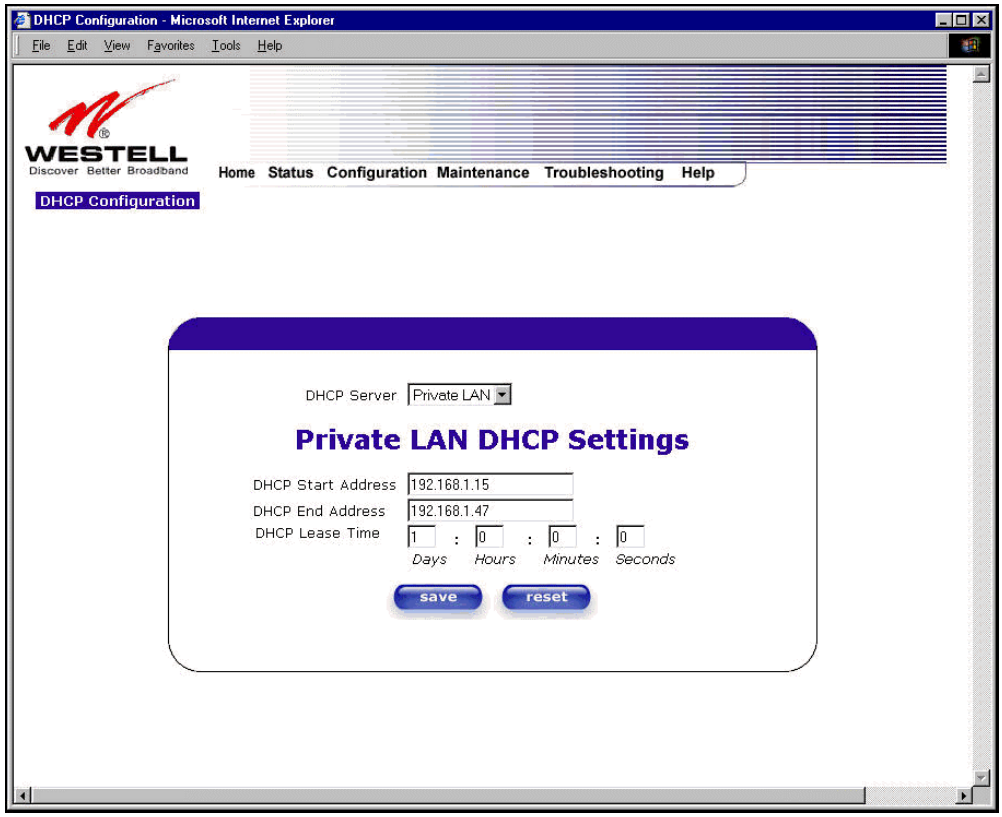
13.5.4 Enabling the DHCP Server

If you want to enable your DHCP Server settings, select **Private LAN** at the **DHCP Server** drop-down arrow.

If you have recently disabled the DHCP Server for Private LAN, select **Private LAN** while in the following screen.



If you selected **Private LAN**, the following screen will be displayed automatically. Click on **save** to save your DHCP Server setting. If you click on **reset**, your DHCP Server will be reset to factory default. (Private LAN is the factory default for the DHCP Server.)



If you clicked on **save**, the following pop-up screen will appear. Click on **OK.**

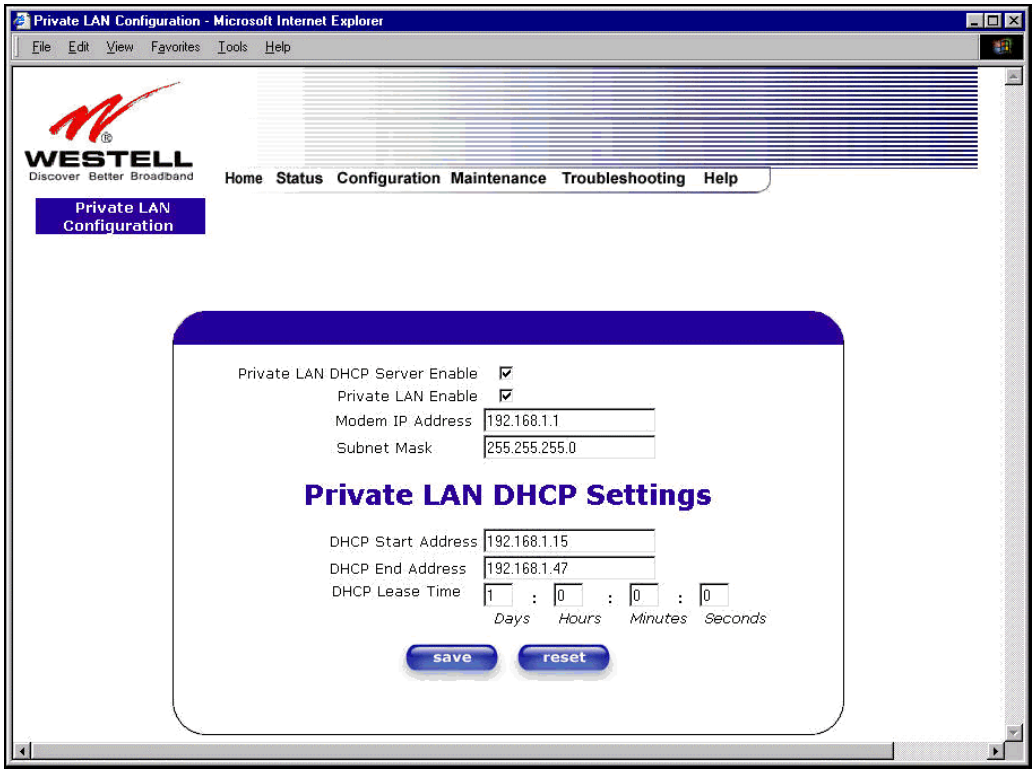
STOP: After you enable the DHCP server, you must reboot your PC

13.5.5 Private LAN Configuration – Configuring NAT

The following settings will be displayed if you select **Advanced LAN > Private LAN** from the **Configuration** menu. (Private LAN is the default configuration for the Router.)

NOTE: Private LAN allows you to set up a network behind the Router.

If you change the settings in this screen, click **save**. If you click on **reset,** the changes will not take effect.



If you made changes and clicked on **save,** the following pop-up screen will be displayed. Click on **OK**. This will save your **Private LAN Configuration** settings. If you click **Cancel**, your new settings will not take effect.

Private LAN DHCP Server Enable	Default = CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Private LAN pool.
Private LAN Enable	Default = CHECKED If this box is CHECKED, it enables the addresses from the Private LAN to use the NAT interface.
Modem IP Address	Displays the Router's IP address
Subnet Mask	Displays the Subnet Mask, which determines what portion of an IP address is controlled by the network and which portion is controlled by the host.
DHCP Start Address	Displays the first IP address that the DHCP server will provide.
DHCP End Address	Displays the last IP address that the DHCP server will provide.
DHCP Lease Time	Displays the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request.

NOTE: DHCP Lease Time is displayed in the following format: (dd:hh:mm:ss)* This value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.
*(dd = days, hh = hours, mm = minutes, ss = seconds).

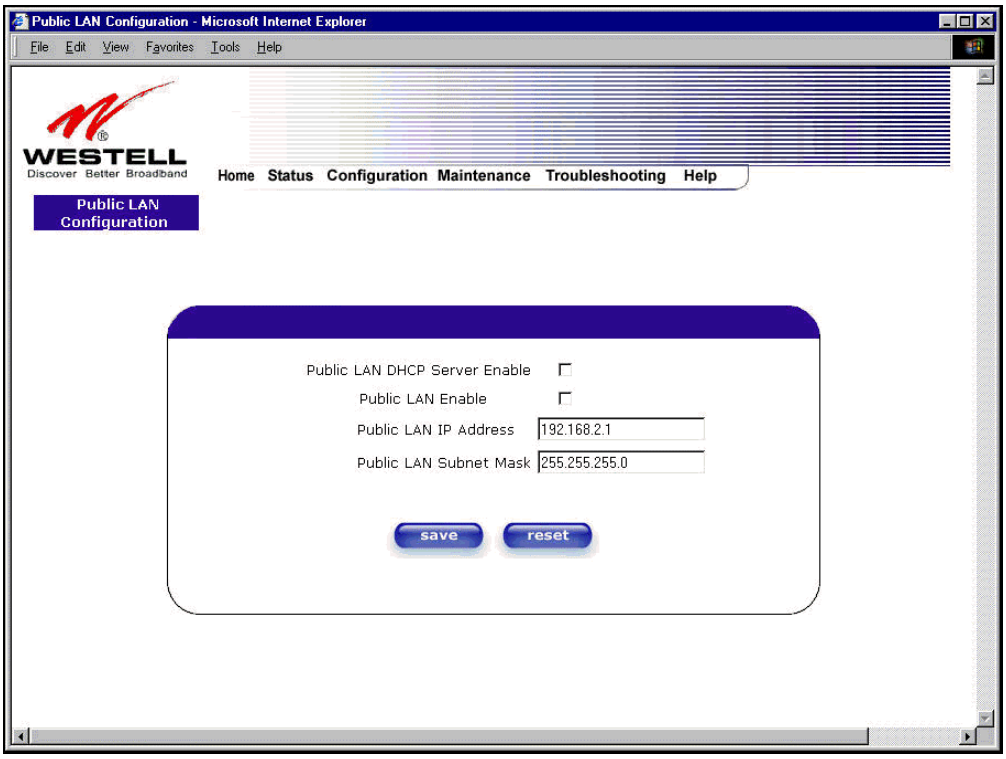
If the settings you have entered in the **Private LAN Configuration** screen are incorrect, the following warnings messages may be displayed via pop-up screens. If this occurs, check the settings in the **Private LAN Configuration** screen.

Warning Message	Check Private LAN DHCP Settings
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

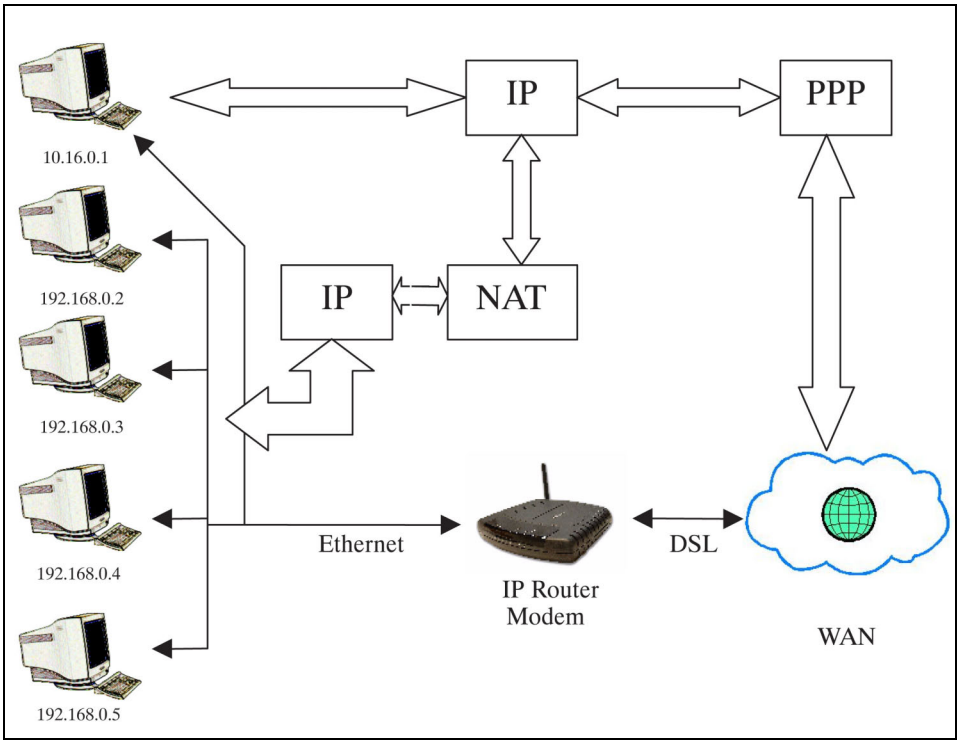
13.5.6 Public LAN Configuration – Multiple IP Address PassThrough

The following screen will be displayed if you select **Advanced LAN > Public LAN** from the **Configuration** menu. Click in the **Public LAN DHCP Server Enable** box. A check mark will appear in the box.

NOTE: The Public LAN feature, if available from your service provider, allows the Router to use LAN IP addresses that are accessible from the WAN. Public LAN allows your computer to have global address ability. To utilize the Public LAN feature on the Router, your ISP must support Public LAN and Static IP. Contact your ISP for details.



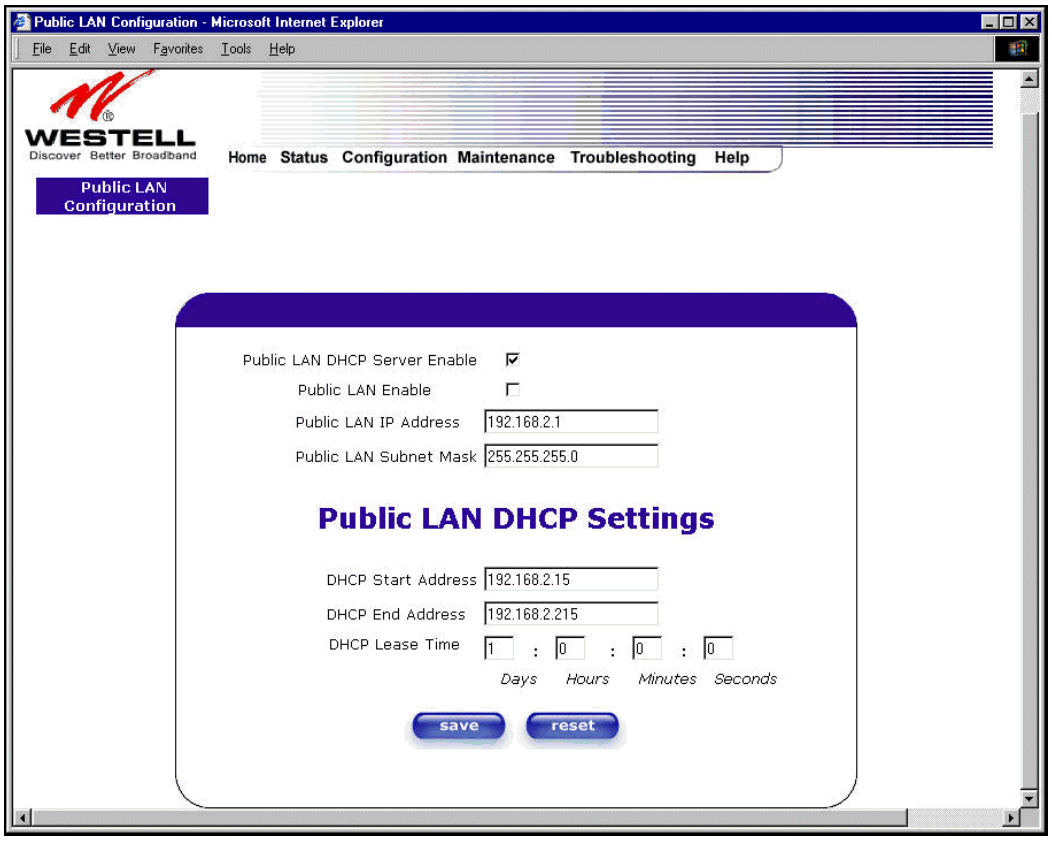
The public devices are visible on the Internet unlike a local NAT'ed PC. The example below shows four NAT'ed PCs and one global PC. The arrows show the data path for each flow.



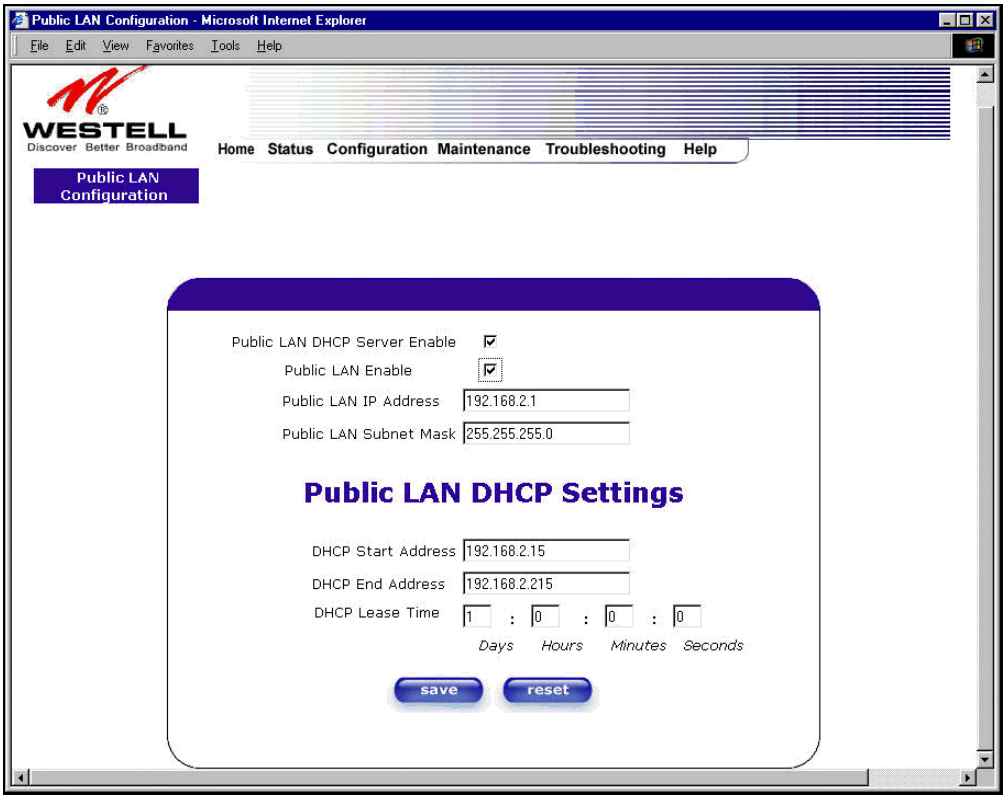
Public LAN DHCP Server Enable	Default = NOT CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Public LAN pool.
Public LAN Enable	Default = NOT CHECKED If this box is CHECKED, it enables the addresses from the Public LAN to bypass the NAT interface.
Public LAN IP Address	Provides a Public IP Address if the service provider does not automatically provide one.
Public LAN Subnet Mask	Provides a Public Subnet Mask if the service provider does not automatically provide one.

If you clicked the **Public LAN DHCP Server Enable** box, the following screen will be displayed. Click on the **Public LAN Enable** box to enable Public LAN.

NOTE: By enabling the Public LAN DHCP Server, you automatically disable the Private LAN DHCP Server on the Router.



If you clicked the **Public LAN Enable** box, the following screen will be displayed, showing the Public LAN Enable box selected. Click on **save.**



If you selected **Public LAN Enable,** or if you made other changes in the **Public LAN Configuration** screen and clicked **save**, the following pop-up screen will be displayed. Click **OK** to save the new settings. If you click on **Cancel**, your new settings will not take effect.

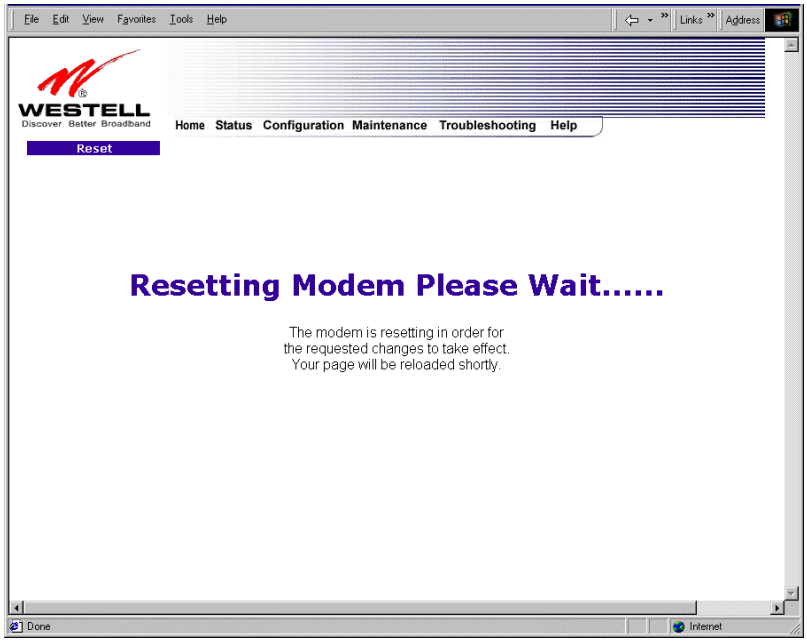
NOTE: DHCP Lease Time is displayed in the following format: (dd:hh:mm:ss)*. This value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.
*(dd = days, hh = hours, mm = minutes, ss = seconds).

If the settings you have entered in the **Public LAN Configuration** screen are incorrect, the following warnings messages may be displayed via pop-up screens. If this occurs, check settings in the **Public LAN Configuration** screen.

Warning Message	Check Public LAN DHCP Settings
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** field at DHCP Lease Time
Minutes must be between 0 and 59	Check the **Minutes** field at DHCP Lease Time
Hours must be between 0 and 23	Check the **Hours** field at DHCP Lease Time

If you clicked on **OK** in the **Load new Public LAN configuration?** screen, the following pop-up screen will be displayed. This 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. The Router will be reset and the new configuration will take effect.

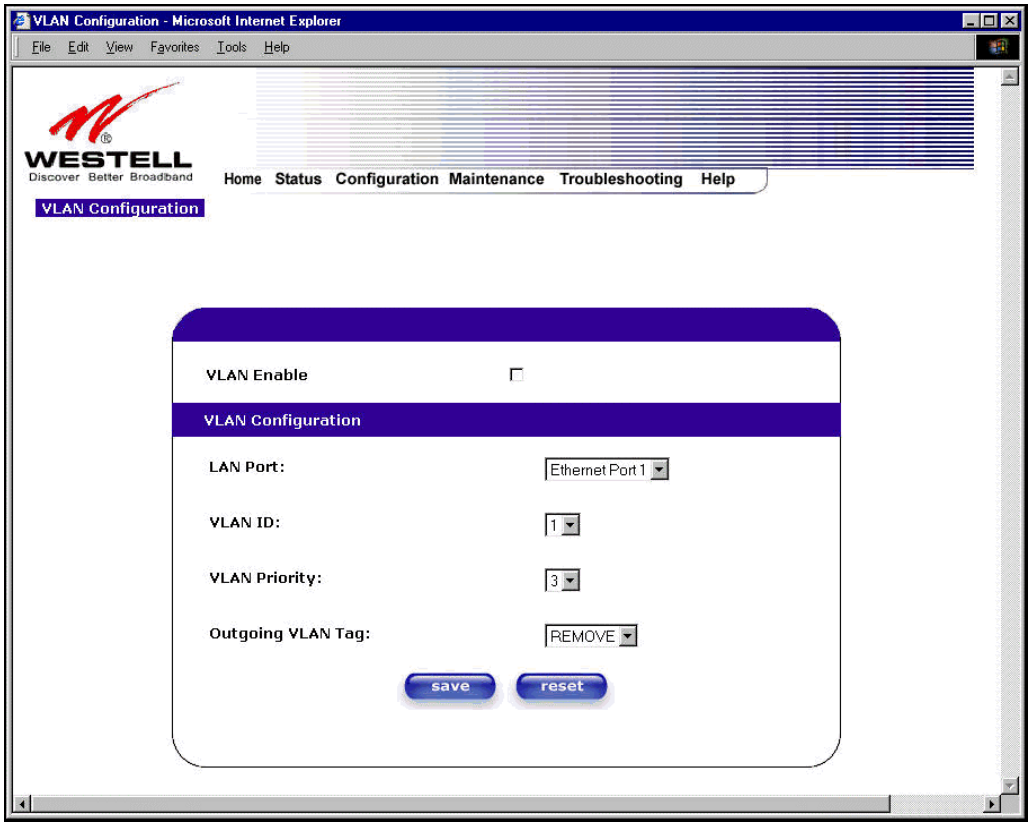


After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP.** (Click on the **connect** button to establish a PPP session).

NOTE: Whenever the PPP Status displays **DOWN,** you do not have a PPP session established. If your Router's connection setting is set to "Always On," 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 your Router's configuration.

13.5.7 VLAN

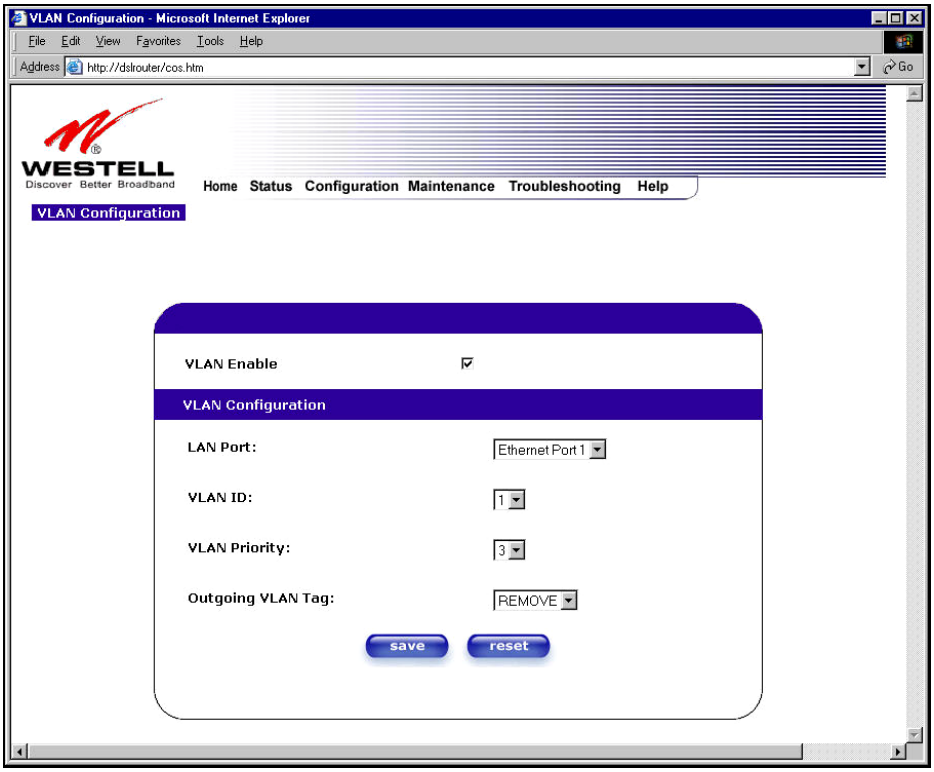
The following settings will be displayed if you select **Advanced LAN > VLAN** from the **Configuration** menu.



VLAN Enable	Factory Default = DISABLED If this box is check, VLAN will be Enabled. This will allow VLAN tagging to occur according to the data port's configuration.
LAN Port	This allows you to select the LAN port that you wish to configure. Possible response: Ethernet Port 1 Ethernet Port 2 Ethernet Port 3 Ethernet Port 4 USB Port* WLAN Port
VLAN ID	This allows you to assign a VLAN ID to the port. Possible response: 1 through 8
VLAN Priority	This allows you to set the VLAN priority for the port. Possible response: 0 through 7
Outgoing VLAN Tag	This allows you to keep or remove the VLAN tag on the port when data is outgoing.
**USB Port is available in Models 7400 and 328W10 only.*	

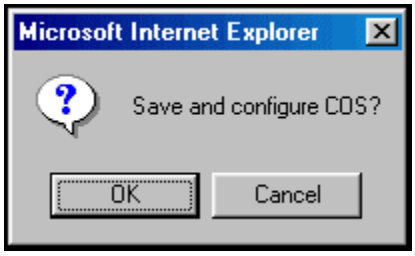
To enable VLAN, click on the box adjacent to the **VLAN Enable** field. A check mark will appear in the box. Click **save** to save the settings.

NOTE: For VLAN to function properly, the VLAN ID must be set to a value other than '1' in **VLAN Configuration** screen and in the **VC 1 Configuration** screen when the you are using the Bridge (VLAN Bridge) protocol. See Advanced WAN section for configuring VC's (refer to section 13.6.6).



NOTE: If you change the values in the **VLAN Configuration** screen and click the **reset** button, the screen will display the previously set values for the LAN Port you have selected. If you change the settings in this screen, you must click **save** to save the new settings.

If you click on **save**, the following pop-up screen will appear. Click **OK** in the pop-up screen to allow the new settings to take effect.

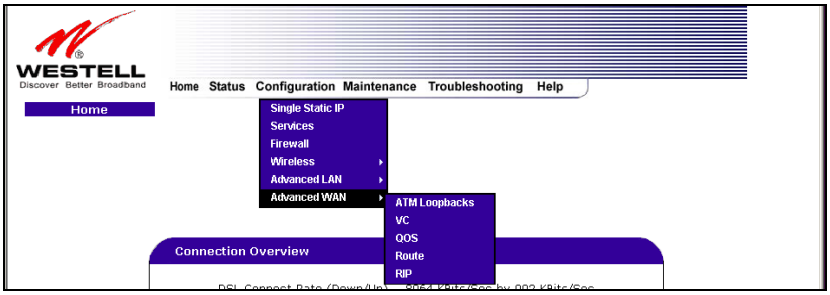


13.6 Advanced WAN

This section explains the configurable features of the Router that are available if you select **Advanced WAN** from the **Configuration** menu.

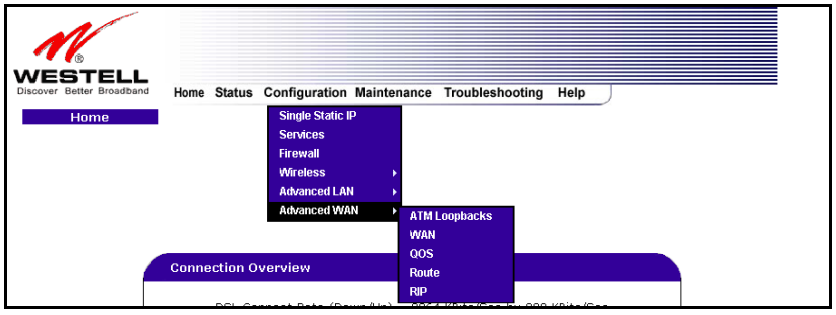
NOTE: If you are using Model 328W10 or 328W11, options in the **Advanced WAN** drop-down menu may or may not be displayed depending on the Router's WAN Configuration (DSLATM PORT or ETHERNET PORT 1). However, all menu options are displayed if the Router is configured for DSLATM PORT 1. The following sections provide further details on the Troubleshooting menu.

If you are using Models 7400, 7401, the following **Advanced WAN** menu options will be displayed.



If you are using Models 328W10, 328W11, the following **Advanced WAN** menu options will be displayed.

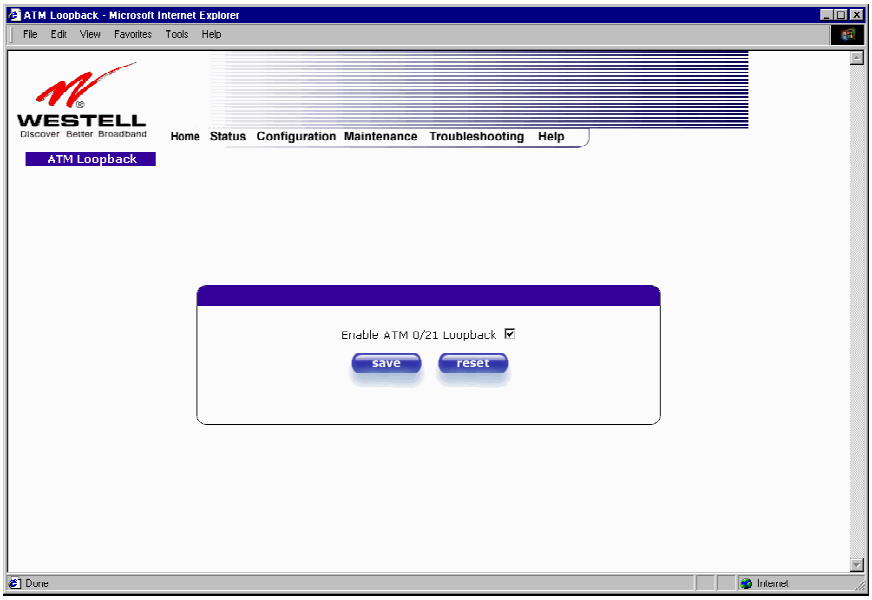
NOTE: If Model 328W10, or 328W11 is configured for **ETHERNET PORT 1**, the **QOS** option will not be displayed in the **Advanced WAN** drop-down menu. You must configure the Router for **DSLATM PORT** to access **QOS**. Refer to section 13.6.3.1 for details on enabling and disabling DSLATM PORT and ETHERNET PORT 1.



13.6.1 ATM Loopbacks

The following settings will be displayed if you select **Advanced WAN > ATM Loopbacks** from the **Configuration** menu.

NOTE: When the **Enable ATM 0/21** box is checked, this feature is enabled. If the box does not display a check mark, this feature is disabled. If you change the setting in this screen, you must click **save** to save the setting. **Westell does not recommend that you change this setting.**



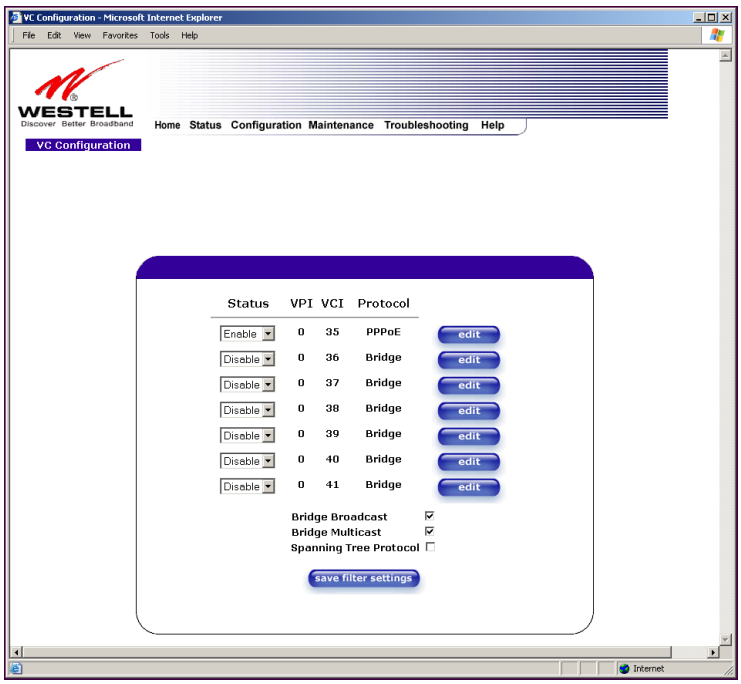
Enable ATM 0/21 Loopback:	Factory Default = ENABLED This option enables the 0/21 loopback, which is used by your ISP. NOTE: Westell does not recommend that you change this setting.

13.6.2 VC Configuration (Models 7400, 7401)

The following screen will be displayed if you select **Advanced WAN > VC** from the **Configuration** menu. If you change the **Bridge Broadcast, Bridge Multicast,** or **Spanning Tree Protocol** configurations in this screen, click on the **save filter settings** button to allow these changes to take effect. If you change any of the **Status** configurations, a pop-up screen will prompt you to reset the Router. After the Router has been reset, the **Status** configurations will take effect. The **edit** button allows you to change the VC configuration settings of the Router. Details on the **edit** button are explained later in section 13.6.4.

NOTE: The actual information displayed in this screen may vary, depending on the network connection established.

If you are using Model 7400 or Model 7401, the following screen will be displayed.



Status	Allows you to enable or disable your VC (Virtual Connection)
VPI	Displays the VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	Displays the VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
Protocol NOTE: The configuration specified by your Service Provider will determine which Protocols are available to you.	Displays the Protocol for each VC, which is specified by your Service Provider. Possible Response: PPPoA = Point to Point Protocol over ATM (Asynchronous Transfer Mode) PPPoE = Point to Point Protocol over Ethernet Bridge = Bridge Protocol Classical IPoA = Internet Protocol over ATM (Asynchronous Transfer Mode). This is an ATM encapsulation of the IP protocol.

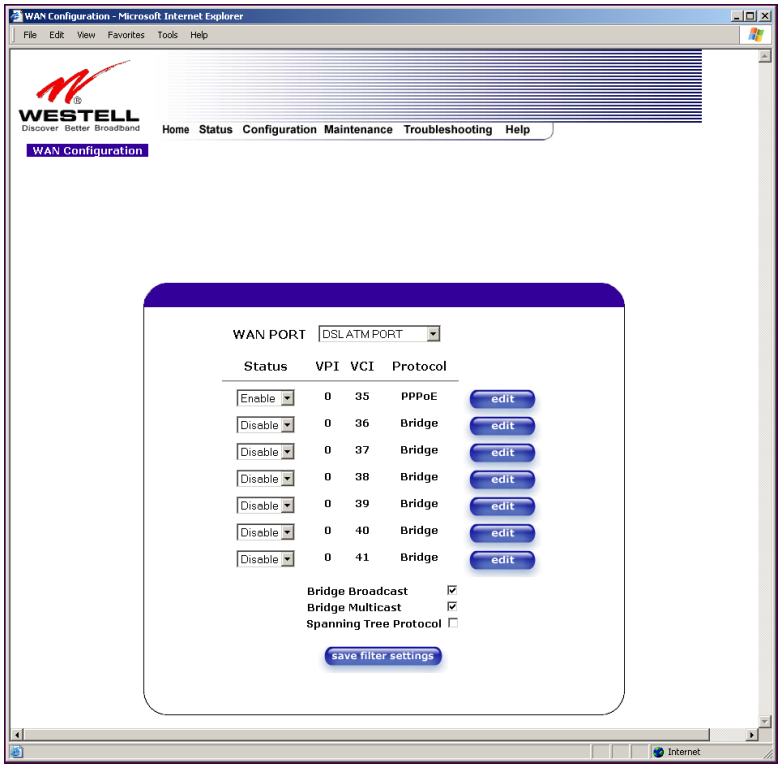
Bridge Broadcast	Factory Default = CHECKED When this setting is CHECKED, the Router will allow Broadcast IP packets to/from the WAN. When this setting is NOT CHECKED, the Router will block Broadcast IP packets to/from the WAN. This setting is only valid if one of the Virtual Channels is configured for Bridge mode.
Bridge Multicast	Factory Default = CHECKED When this setting is CHECKED, the Router will allow Multicast IP packets to/from the WAN. When this setting is NOT CHECKED, the Router will block Multicast IP packets to/from the WAN. This setting is only valid if one of the Virtual Channels is configured for Bridge mode.
Spanning Tree Protocol	Factory Default = DISABLED Spanning Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For Ethernet network to function properly, only one active path can exist between two stations. When ENABLED, two bridges are used to interconnect the same two computer network segments. Spanning Tree Protocol will allow the bridges to exchange information so that only one of them will handle a given message that is being sent between two computers within the network. NOTE: Spanning Tree can't be enabled if VLAN is enabled.
Status	Allows you to enable or disable your VC (Virtual Connection)

13.6.3 WAN Configuration (Models 328W10, 328W11)

The following screen will be displayed if you select **Advanced WAN > WAN** from the **Configuration** menu. If you change the **Bridge Broadcast, Bridge Multicast,** or **Spanning Tree Protocol** configurations in this screen, click on the **save filter settings** button to allow these changes to take effect. If you change any of the **Status** configurations, a pop-up screen will prompt you to reset the Router. After the Router has been reset, the **Status** configurations will take effect. The **edit** button allows you to change the VC configuration settings of the Router. Details on the **edit** button are explained later in section 13.6.4.

NOTE: The actual information displayed in this screen may vary, depending on the network connection established.

If you are using Model 328W10 or Model 328W11, the following screen will be displayed.



WAN PORT	Factory Default = DSLATM PORT Possible Responses: DSLATM PORT - Selecting this will enable the Router's DSL transceiver. This will disable the WAN Ethernet port and allow the WAN interface to use the DSL port. ETHERNET PORT 1 – Selecting this will disable the Router's DSL transceiver. This will enable the WAN Ethernet port and allow the WAN interface to use the UPLINK/E1 Port.
Status	Allows you to enable or disable your VC (Virtual Connection)
VPI	Displays the VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	Displays the VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.

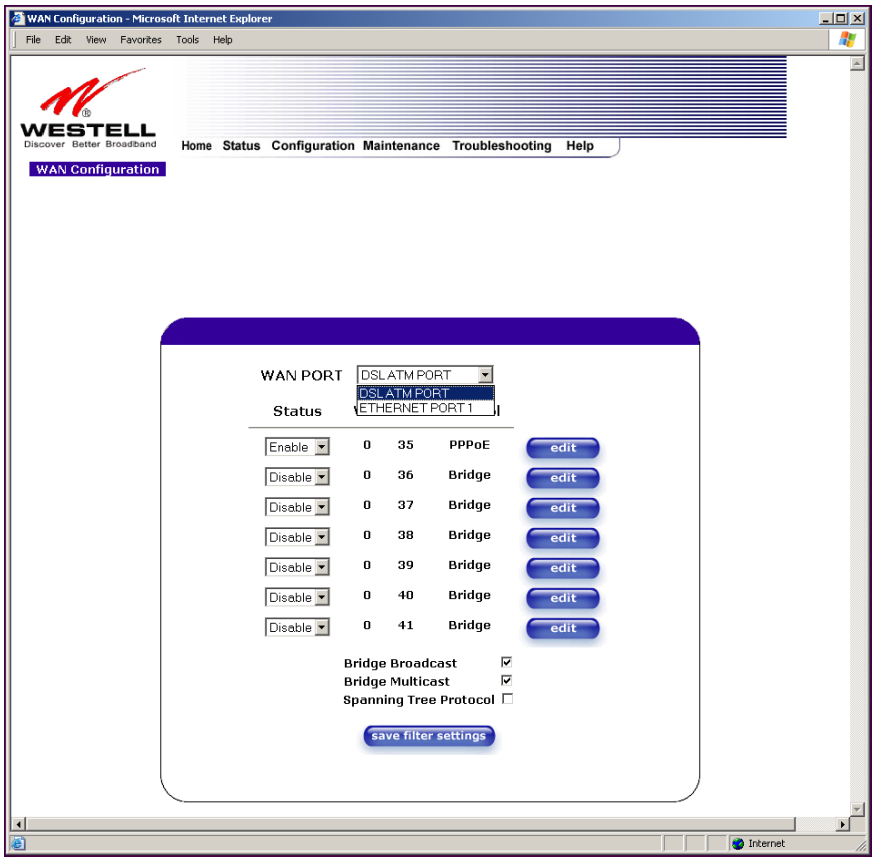
Protocol NOTE: The configuration specified by your Service Provider will determine which Protocols are available to you.	Displays the Protocol for each VC, which is specified by your Service Provider. Possible Response: PPPoA = Point to Point Protocol over ATM (Asynchronous Transfer Mode) PPPoE = Point to Point Protocol over Ethernet Bridge = Bridge Protocol Classical IPoA = Internet Protocol over ATM (Asynchronous Transfer Mode). This is an ATM encapsulation of the IP protocol.
Bridge Broadcast	Factory Default = CHECKED When this setting is CHECKED, the Router will allow Broadcast IP packets to/from the WAN. When this setting is NOT CHECKED, the Router will block Broadcast IP packets to/from the WAN. This setting is only valid if one of the Virtual Channels is configured for Bridge mode.
Bridge Multicast	Factory Default = CHECKED When this setting is CHECKED, the Router will allow Multicast IP packets to/from the WAN. When this setting is NOT CHECKED, the Router will block Multicast IP packets to/from the WAN. This setting is only valid if one of the Virtual Channels is configured for Bridge mode.
Spanning Tree Protocol	Factory Default = DISABLED Spanning Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For Ethernet network to function properly, only one active path can exist between two stations. When ENABLED, two bridges are used to interconnect the same two computer network segments. Spanning Tree Protocol will allow the bridges to exchange information so that only one of them will handle a given message that is being sent between two computers within the network. NOTE: Spanning Tree can't be enabled if VLAN is enabled.

13.6.3.1 Enabling DSLATM PORT – Disabling ETHERNET PORT 1 (Models 328W10 and 328W11 only)

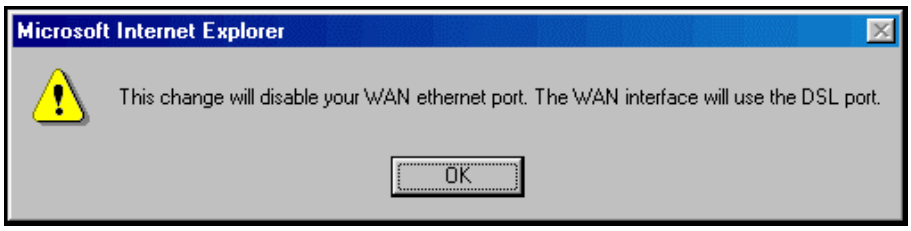
NOTE: When using the optional UPLINK/E1 port, Ethernet LAN connection is limited to E2, E3, and E4. The UPLINK feature is optional. If UPLINK is not enabled, the Router will use DSL and wireless only.

To configure the Router so that it uses the DSL port, select **DSLATM PORT** from the **WAN PORT** drop-down arrow. By selecting **DSLATM PORT**, you will enable the Router's DSL transceiver. This will disable the WAN Ethernet port and allow the WAN interface to use the DSL port.

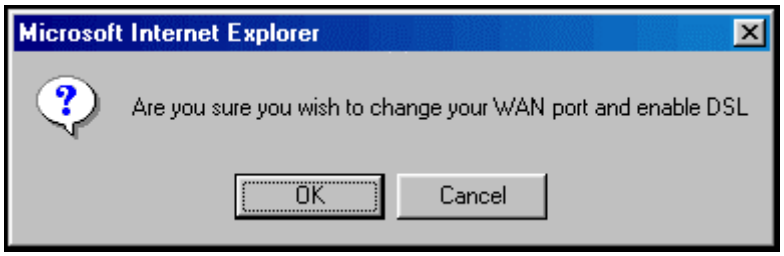
NOTE: All of the Router's menu options are displayed if the Router is configured for **DSLATM PORT**.



If you select **DSLATM PORT** from the **WAN Port** drop-down arrow, the following screen will be displayed. Click **OK.**

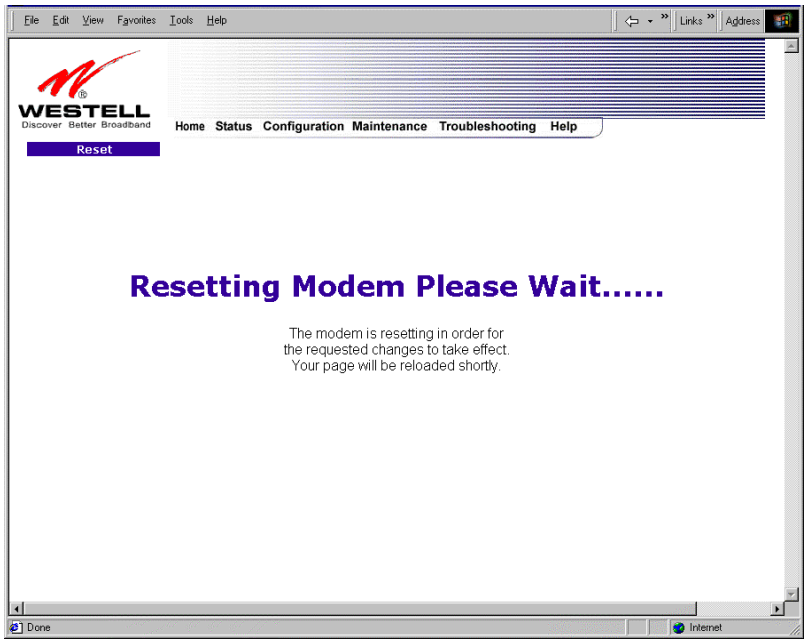


If you click **OK** in the preceding pop-up screen, the following screen will be displayed. Click on **OK.** If you click on **Cancel,** the change will not take effect.



If you clicked on **OK** in the preceding pop-up screen, the following pop-up screen will appear. The Router 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. The Router will be reset and the new configuration will take effect.



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

13.6.3.2 Disabling DSLATM PORT – Enabling ETHERNET PORT 1 (Models 328W10 and 328W11 only)

To configure the Router so that it uses the WAN Ethernet Port, select **ETHERNET PORT 1** from the **WAN PORT** drop-down arrow. By selecting **ETHERNET PORT 1**, you will disable the Router's DSL transceiver. This will disable the DSL Port and allow the WAN interface to use the WAN Ethernet Port.

NOTE: If ETHERNET PORT 1 is configured, the Router's menu options may or may not be displayed. The sections explained throughout this document will indicate when a menu item is unavailable. The UPLINK feature is optional, and if UPLINK is not enabled in the .ini file, the Router will use DSL and Wireless only.

NOTE: If you experience any problems, please reset the Router via the external hardware reset button or via the procedure defined in section 15.1(Backup/Restore) from the **Maintenance** menu. Click the **restore** button adjacent to 'Factory defaults become Current configuration'.