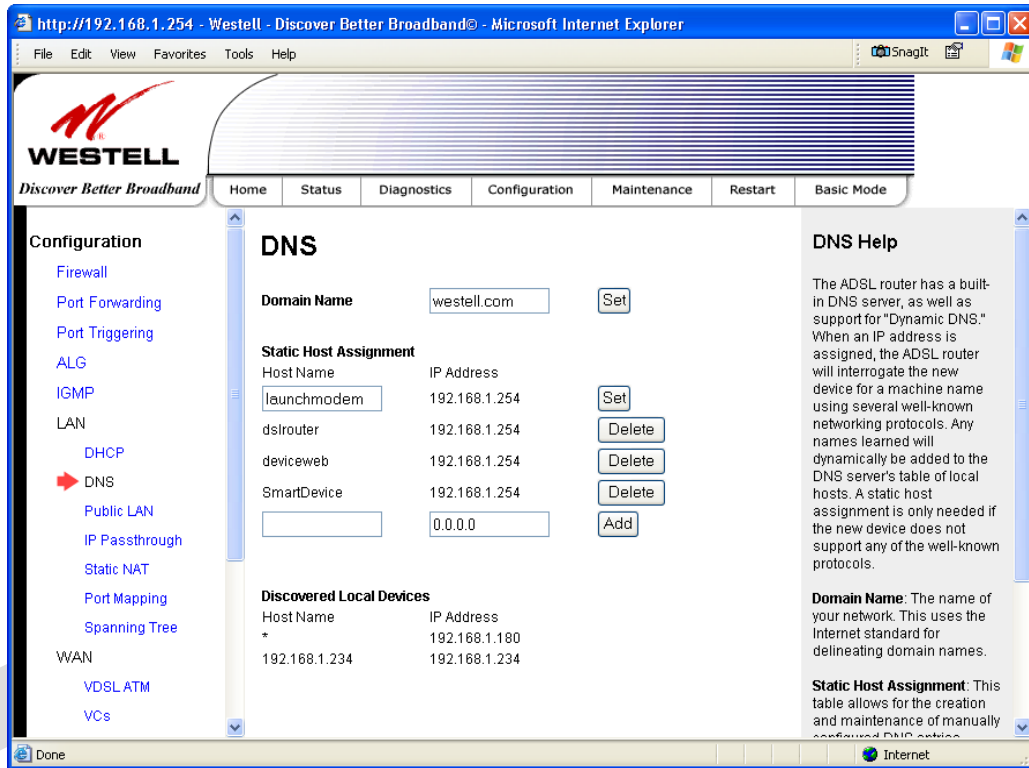


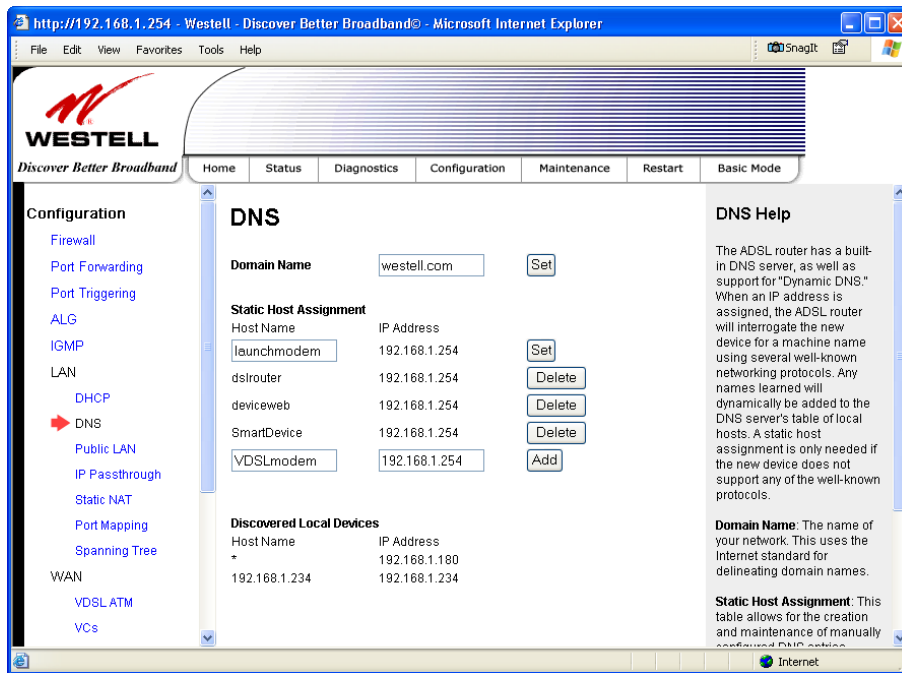
15.6.2 DNS

The following screen will be displayed if you select **Configuration > LAN > DNS** from the menu options. The DNS screen allows you add static host names along with their IP addresses to your Gateway's DNS server.

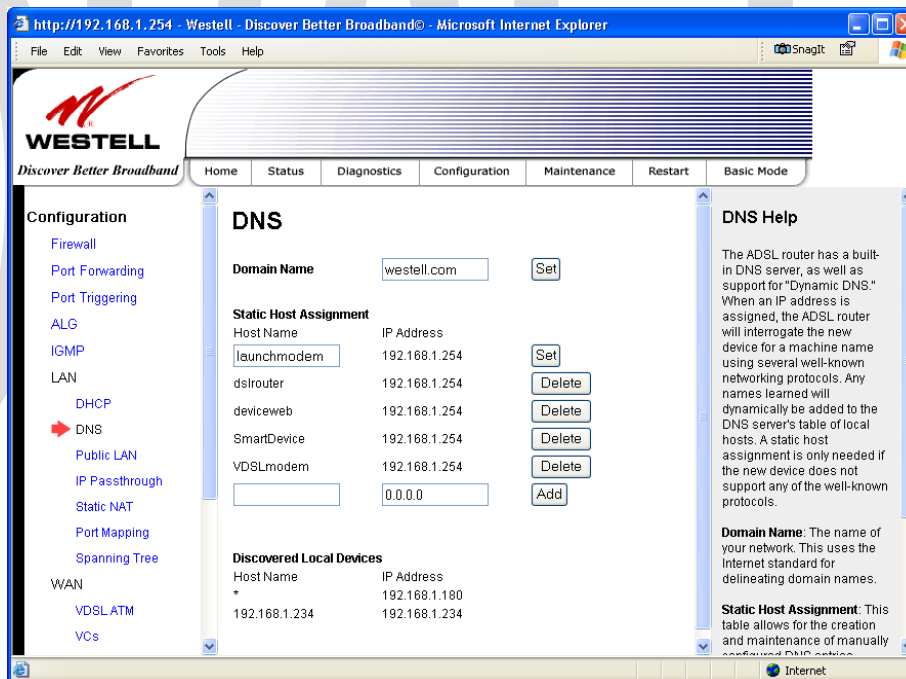


DNS	
Domain Name Note: Some ISP's may require the name for identification purposes.	This field allows you to enter a Domain Name for the Gateway. To add a Domain Name, in the field under User Assigned DNS, type in your new domain name and click Set .
Static Host Assignment	
Host Name	This field allows you to enter a HOST name for the Gateway. To add a new Host name, in the field under Static Host Assignment, type in the Host Name and the associated IP address and then click Add . To delete a Host name, click the Delete button adjacent to the Host Name and IP Address you want to delete.
IP Address	Displays the IP address that is assigned to the Host Name.
Discovered Local Devices	
This field displays a list of the computers on the LAN that have been 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.)	

To add a static host assignment, enter a Host Name and IP Address in the fields provided, and then click **Add**.



After you have entered the desired values and clicked **Add**, the following screen will be displayed. If you want to delete a Static Host Assignment, click the adjacent **Delete** button of the Host Name/IP address you want to delete.



15.6.3 Public LAN—Multiple IP Address Passthrough

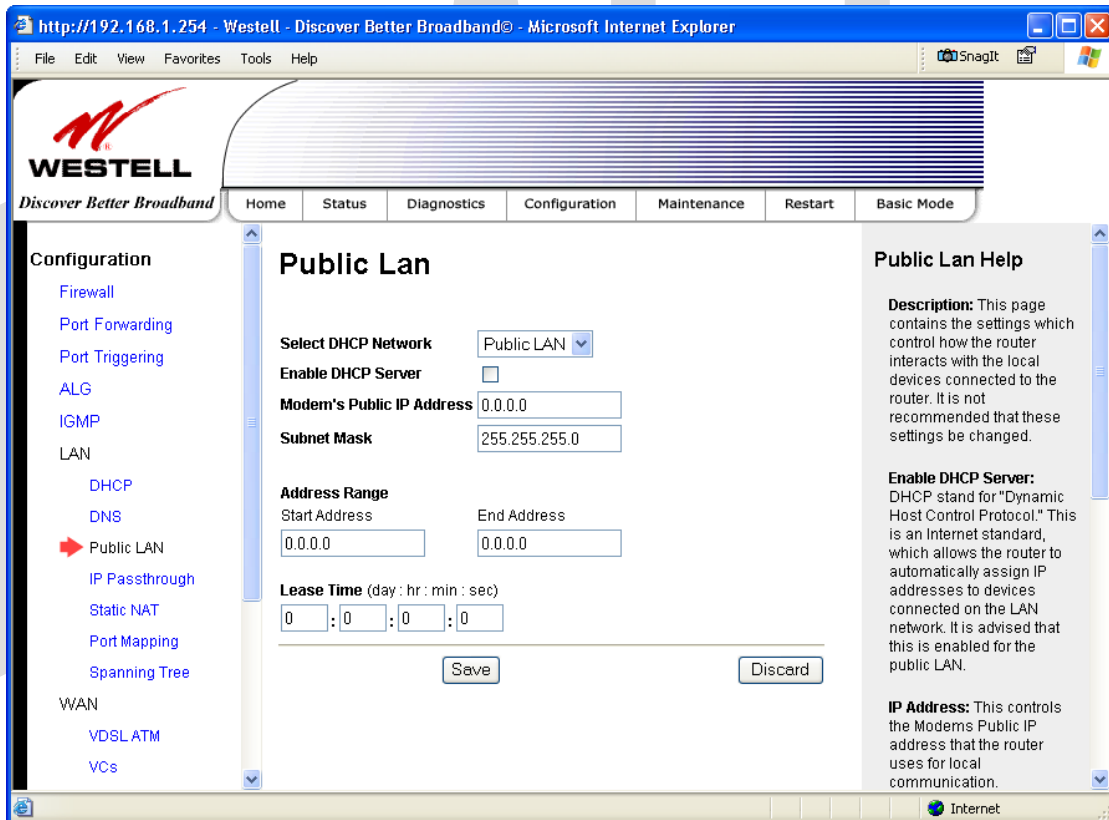
The following screen will be displayed if you select **Configuration > LAN > Public LAN** from the menu options. This screen contains the settings that control how the Gateway interacts with the local devices to which it is connected.

NOTE:

1. Selecting Public LAN will enable your computer to have global address ability. To use the Public LAN feature, your ISP must support Public LAN and Static IP. Contact your ISP for details.
2. Westell recommends that you do not change these settings unless your service provider instructs you to do so.

To enable Public LAN, do the following:

1. Click the **Enable DHCP Server** check box (a check mark will appear in the box). Note: By factory default this box will already contain a check mark.
2. Enter the appropriate address values in the fields provided. (Refer to the following table for information about the Private LAN settings.)
3. Enter the desired lease time values.
4. Click **Save** to save the settings.



Alternate LAN - Public LAN Settings	
Select DHCP Network	Displays the DHCP Network that you have selected.
Enable DHCP Server	Factory Default = Disable Possible Responses: If Enabled (box is checked), this will enable the Public LAN DHCP server and allow IP address to be server from the DHCP Public LAN pool. If Disabled (box is unchecked), this will disable the Public LAN DHCP server.

Modem's Public IP Address	The Gateway's public IP address
Subnet Mask	The Subnet Mask, which determines what portion of an IP address is controlled by the network and which portion is controlled by the host.
Address Range	
DHCP Start Address	This value is provided by your Internet service provider and functions as the first IP address that the Public LAN DHCP Server will provide. The DHCP Start Address must be within the IP address and lower than the DHCP End Address.
DHCP End Address	This value is provided by your Internet service provider and functions the last IP address that the Public LAN DHCP Server will provide. The DHCP End Address must be within the IP address and higher than the DHCP Start Address.
DHCP Lease Time	Factory Default = 00:00:00:00 Displays the amount of time the provided addresses will be valid, after which time the Public LAN DHCP client will usually re-submit a request. Note: DHCP Lease Time is displayed in the format (day:hour:min:sec). This value must be greater than 10 seconds. (Hours must be between 0 and 23; Minutes must be between 0 and 59; and Seconds must be between 0 and 59.)

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

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

15.6.4 IP Passthrough—Single IP Address Passthrough

The following screen will be displayed if you select **Configuration > LAN > IP Passthrough** from the menu options.

IP Passthrough enables you to select one device on your LAN that will share your WAN-assigned IP address. This configuration allows the device with the single static IP address to become visible on the Internet. Network Address Translation (NAT) and Firewall rules do not apply to the device configured for IP Passthrough.

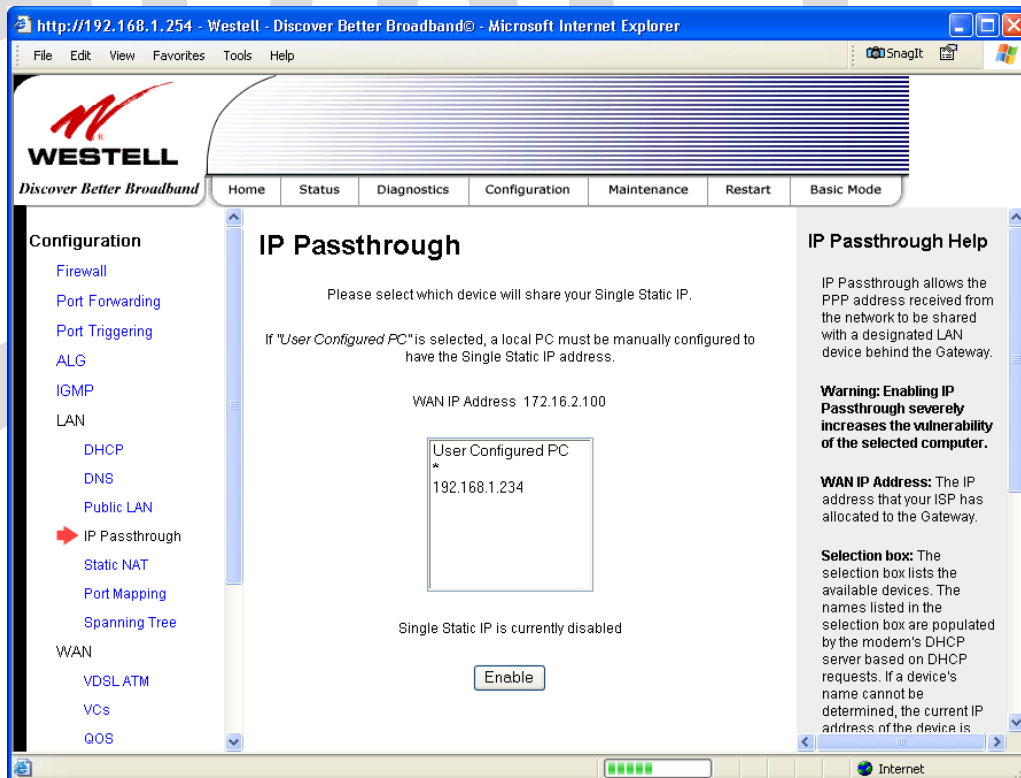
IMPORTANT:

1. Before you begin this section, configure your PC settings to obtain an IP address from your Gateway automatically. (Refer to your computer's Microsoft® Windows® Help screen for instructions.)
2. Static NAT and Single Static IP are mutually exclusive features. Before you enable Single Static IP, be sure to disable Static NAT (if it has been previously enabled). To disable Static NAT, select **Configuration > LAN > Static NAT** from the menu options. Next, click the **disable** button. After you have disabled Static NAT, you can configure IP Passthrough.
3. If you are using Routed IP protocol, IP Passthrough configuration will not be available.

15.6.4.1 Enabling IP Passthrough – Single IP Address PassThrough (Applicable for PPPoE Connections Only)

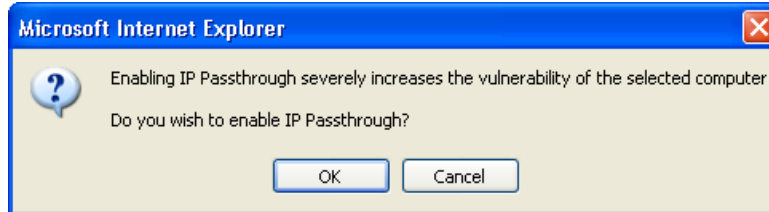
To enable IP Passthrough, select a device that will share your Single Static IP from the options listed in the window. Click **Enable**.

NOTE: The actual device names may differ from those displayed in this screen.

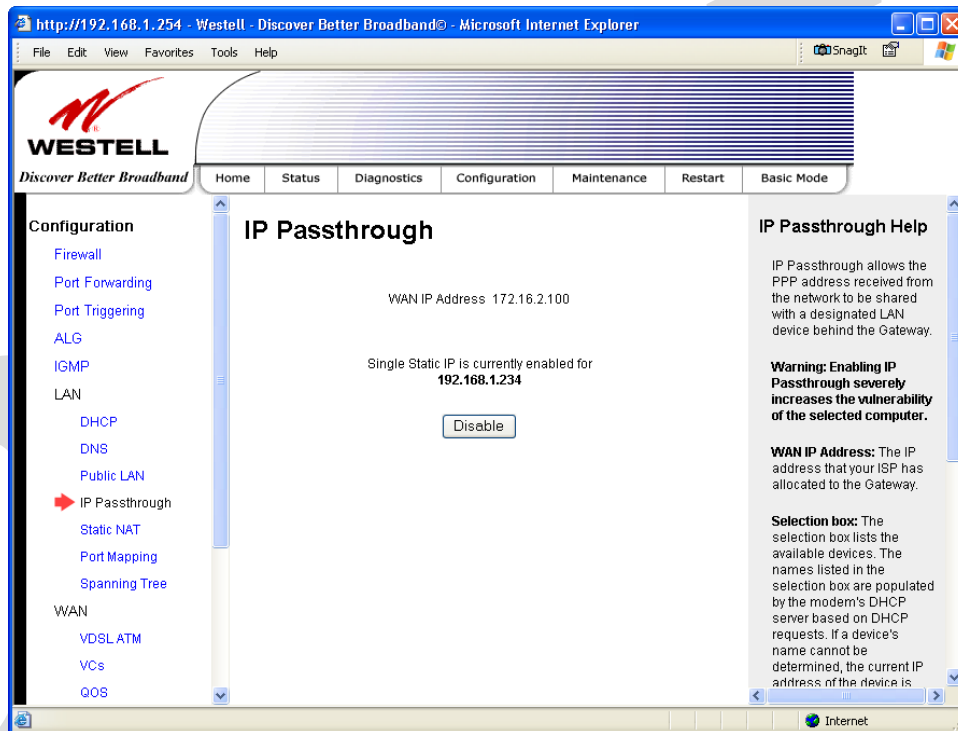


If you clicked **Enable**, the following pop-up screen will be displayed. Click **OK** to continue.

WARNING: Enabling IP Passthrough severely increases the vulnerability of the selected computer.



If you clicked **OK** in the preceding pop-up screen, the Gateway will be reset and the new configuration will take effect, as shown in the following screen.

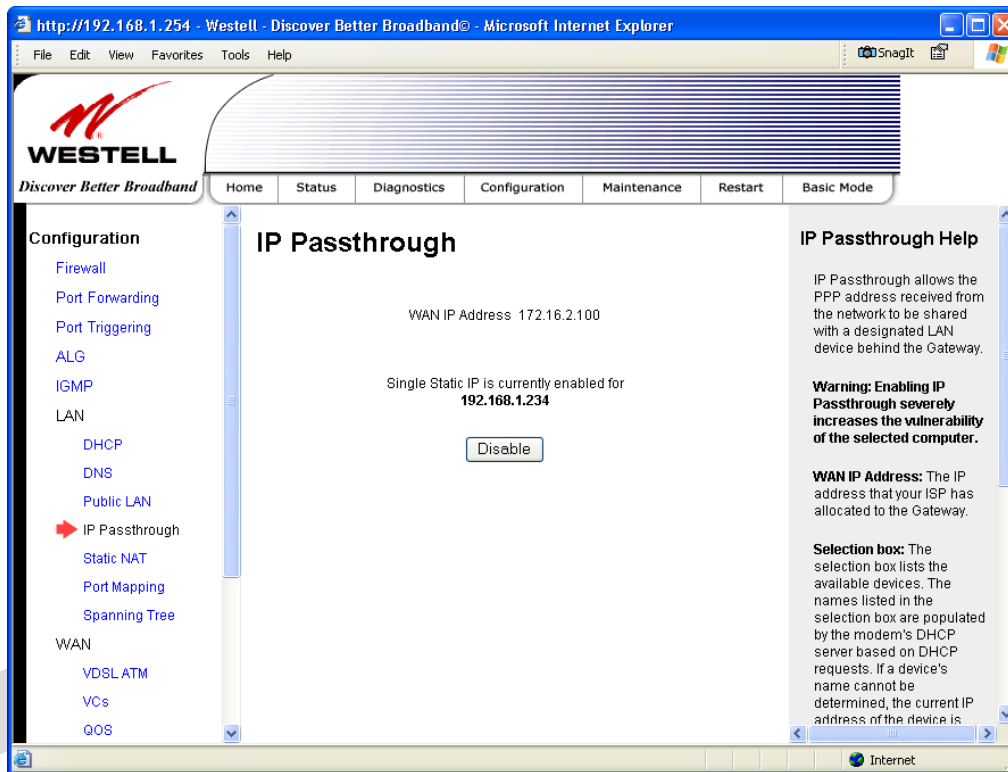


STOP! After you enable IP Passthrough, you must reboot your computer.

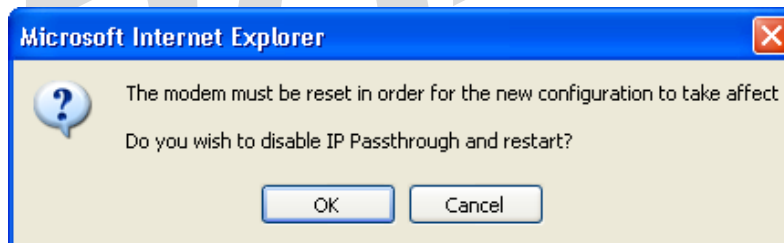
IMPORTANT: If you chose to enable **User Configured PC**, wait for the Gateway to reset and then manually enter the WAN IP, Gateway, and Subnet mask addresses you obtained from your Internet service provider into a PC.

15.6.4.2 Disabling IP Passthrough—Single IP Address PassThrough

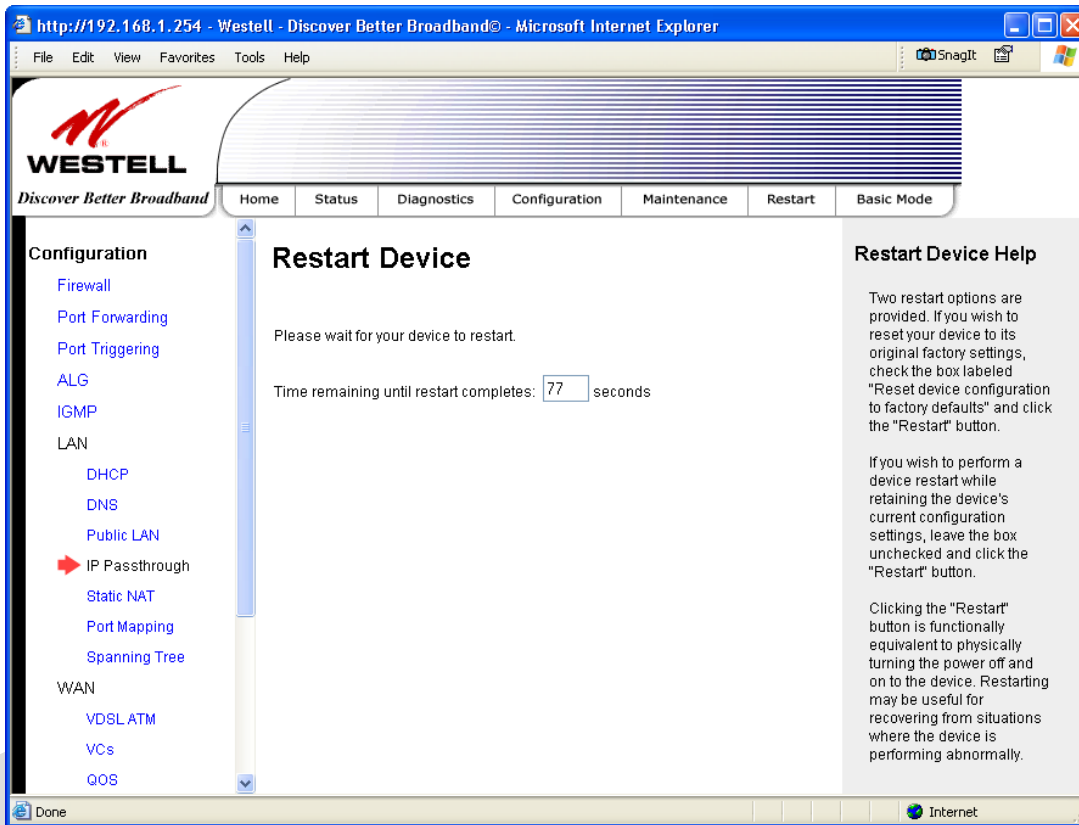
To disable IP Passthrough (if previously enabled), select **Configuration > LAN > IP Passthrough** from the menu options. Next, click **Disable**.



If you clicked **Disable** following pop-up screen will be displayed. Click **OK** to continue.



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



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

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

15.6.5 Static NAT

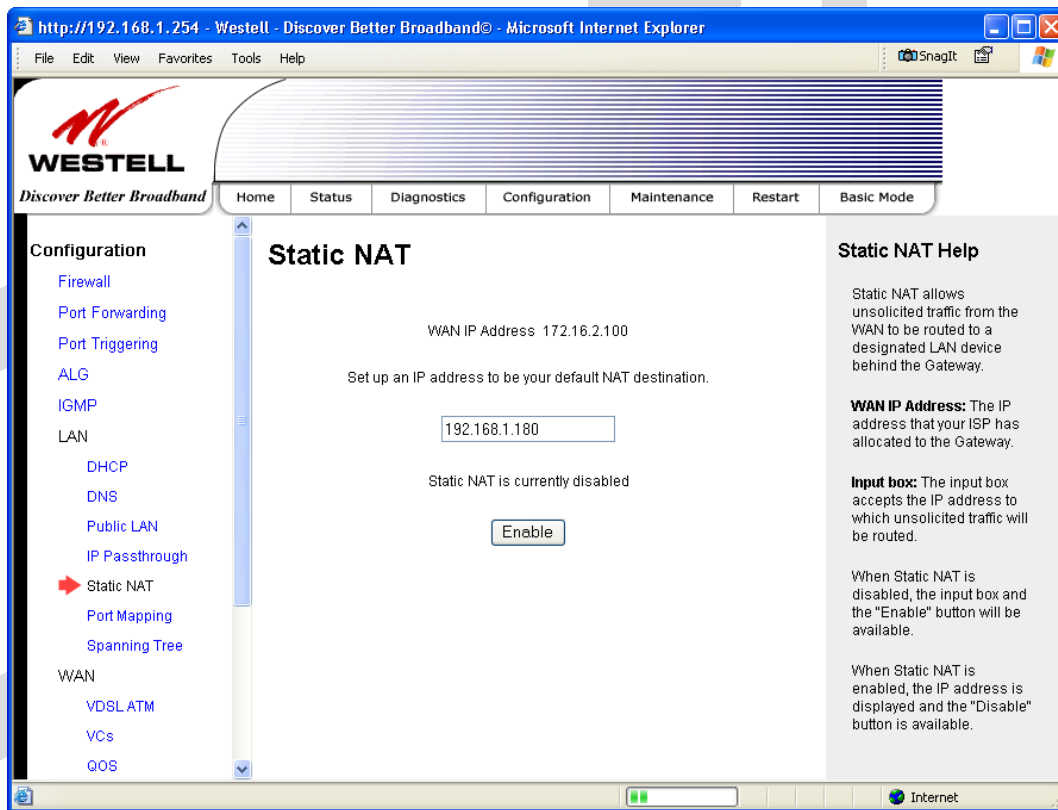
The following screen will be displayed if you select **Configuration > LAN > Static NAT** from the menu options. This screen enables you to configure your Gateway to work with the special NAT services. When your Gateway is configured for Static NAT, any unsolicited packets arriving at the WAN would be forwarded to this device. This feature is used in cases where the user wants to host a server for a specific application.

IMPORTANT: IP Passthrough must be disabled (if it has been previously enabled) before you enable **static NAT**. Refer to section 15.6.4.2 for instructions on disabling IP Passthrough.

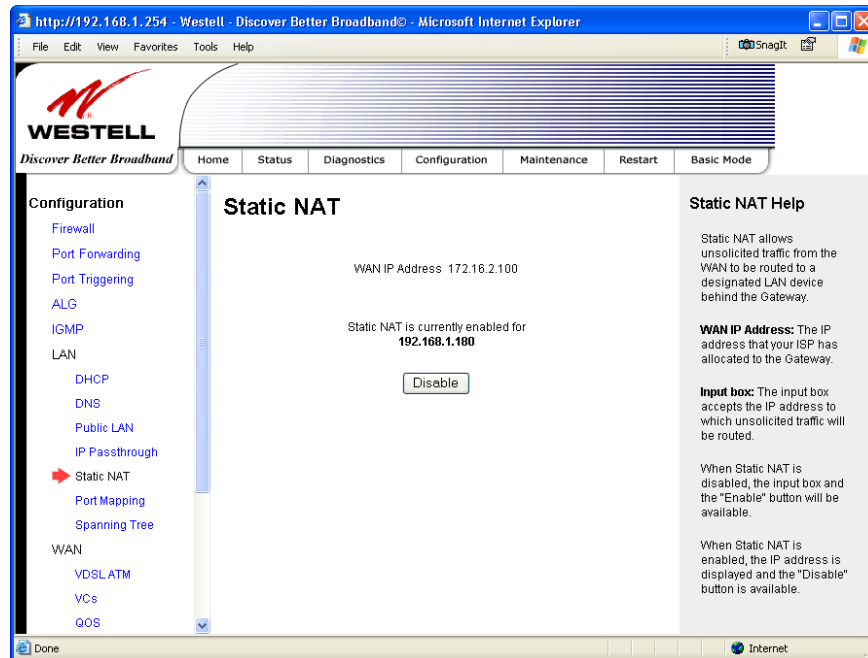
15.6.5.1 Enabling Static NAT

To enable Static NAT, type the desired IP address in the **Static NAT** screen and then click **Enable**.

NOTE: The actual IP addresses or device names may differ from those displayed in the following screen.

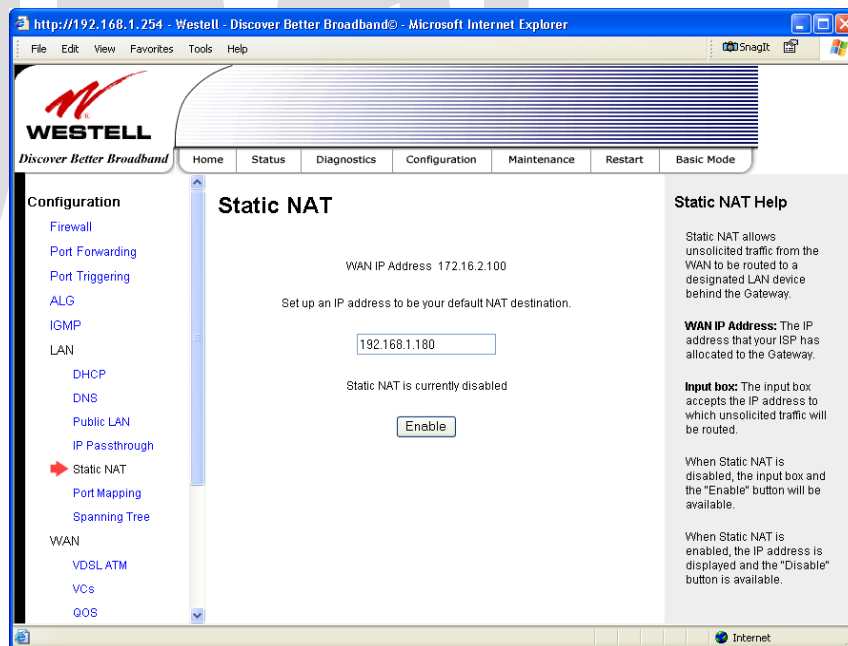


If you clicked **Enable**, the following screen will be displayed. It shows that Static NAT enabled for the IP address or device name you selected.



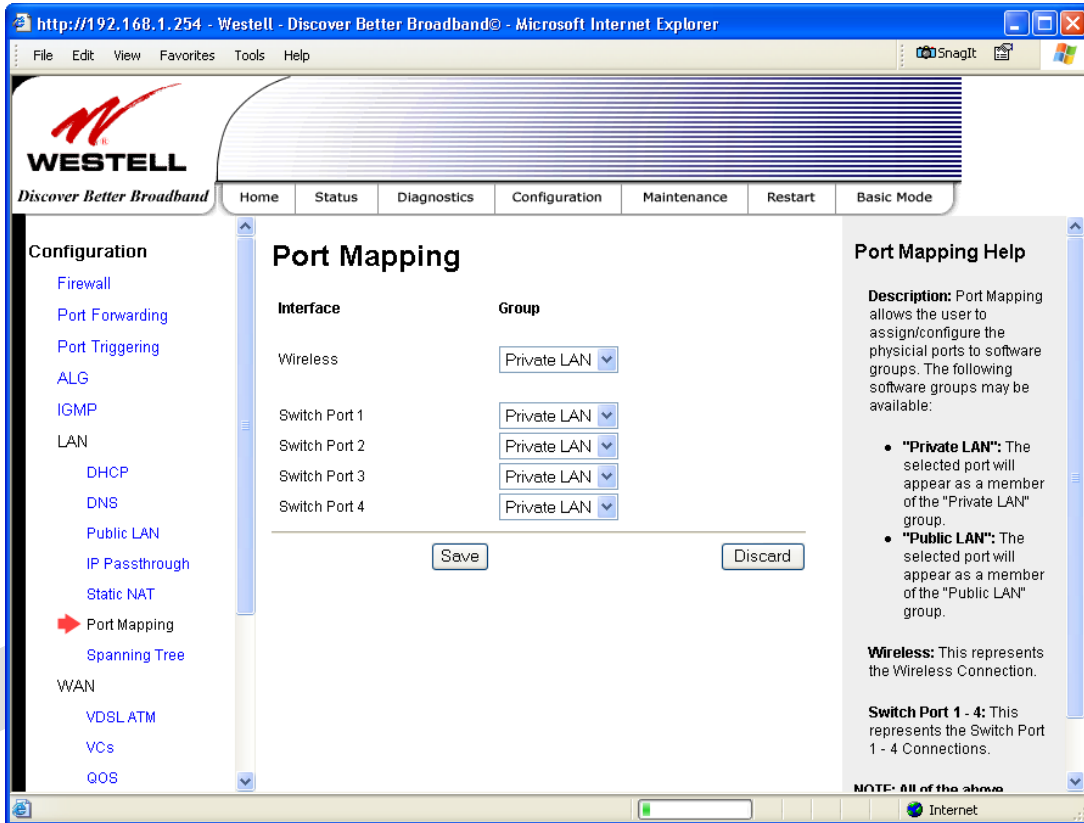
15.6.5.2 Disabling Static NAT

To disable Static NAT, click **Disable** in the **Static NAT** screen. After you have clicked **Disable**, the following screen will be displayed.



15.6.6 Port Mapping

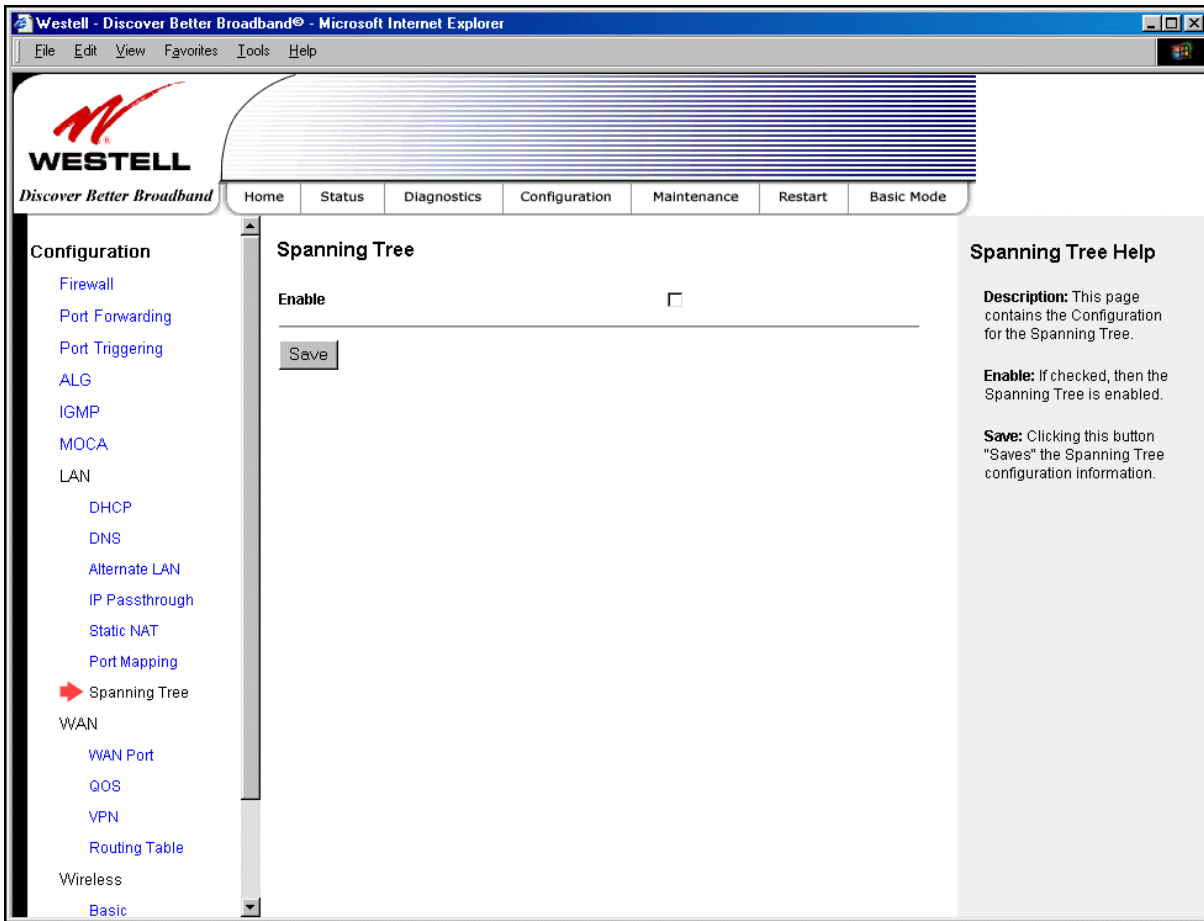
The following screen will be displayed if you select **Configuration > LAN > Port Mapping** from the menu options. This screen enables you to assign the physical ports to software groups. Select the appropriate options from the drop-down menus, and then click **Save** to save your settings.



Interface	The physical ports available for mapping.
Group	<p>Factory Default: Private LAN</p> <p>The software defined virtual LAN group to which the port should be assigned:</p> <p>Possible Responses:</p> <p>Private LAN – The selected port will appear as a member of the Private LAN group.</p> <p>Public LAN – The selected port will appear as a member of the Public LAN group.</p>

15.7 Spanning Tree

The following screen will be displayed if you select **Configuration > LAN > Spanning Tree** from the menu options. This screen enables you to assign the Gateway's physical ports to software groups. To enable Spanning Tree functionality for your Gateway, click the box adjacent to **Enable** (a check mark will appear in the box). Next, click **Save** to save your settings.



Spanning Tree	
Enable	Factory Default = Disabled When this box is checked Spanning Tree is enabled. If the box is unchecked, Spanning Tree is disabled.

15.8 WAN Configuration

This section explains how to configure your Gateway's WAN connections.

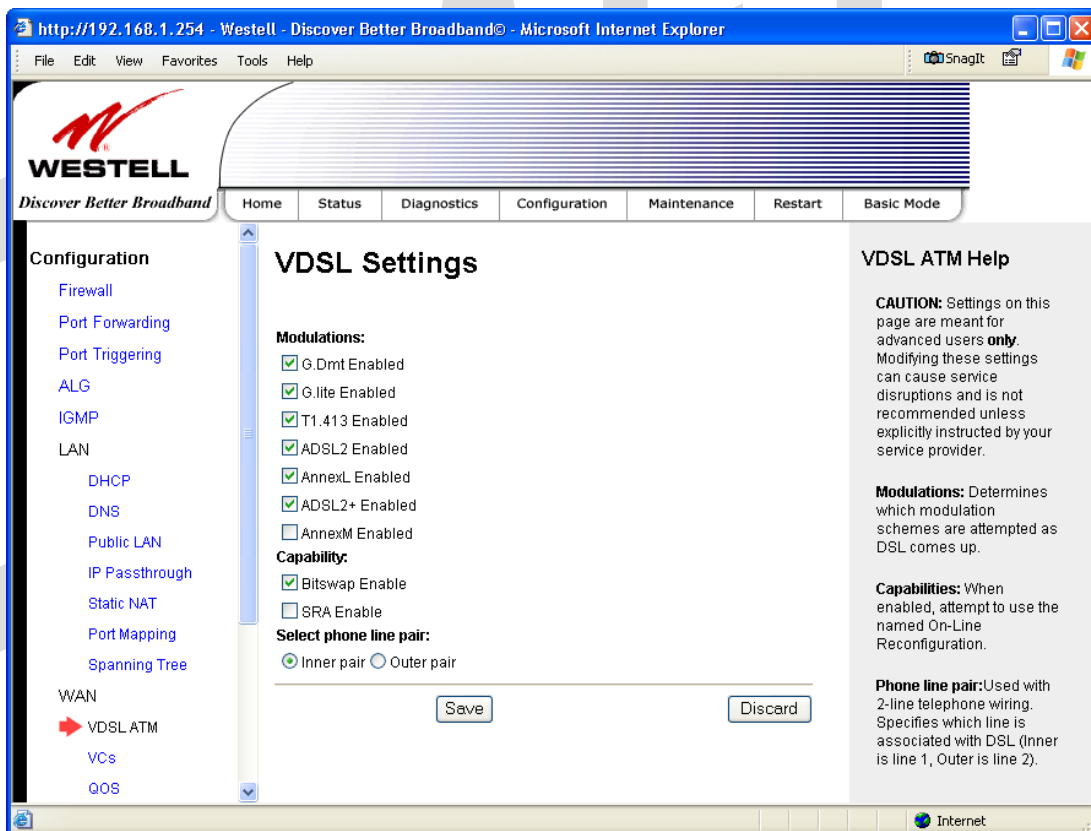
15.8.1 VDSLATM

The following screen will be displayed if you select **Configuration > WAN > WAN Port** from the menu options. This screen allows you to select the VDSL services that you want to use.

CAUTION: Settings on this page are meant for advanced users only. Modifying these settings can cause service disruptions and is not recommended unless your service provider instructs you to do so.

To configure your VDSL settings, do the following:

1. Click the check box of each modulation service that you want to activate (a check mark will appear in the box if it is not already checked).
2. Select which capability settings you want activated. If desired, you can activate both.
3. Select the radio button of the phone line you want to use.
4. Click **Save** to save the settings.



VDSL Settings	
Modulations	This determines which modulations schemes are attempted as DSL comes up. To enable a modulation, put a check mark in the box of each modulation you want to activate. If the box is clear (unchecked), the setting will not be activated.
Capability	Factory Default = Bitswap

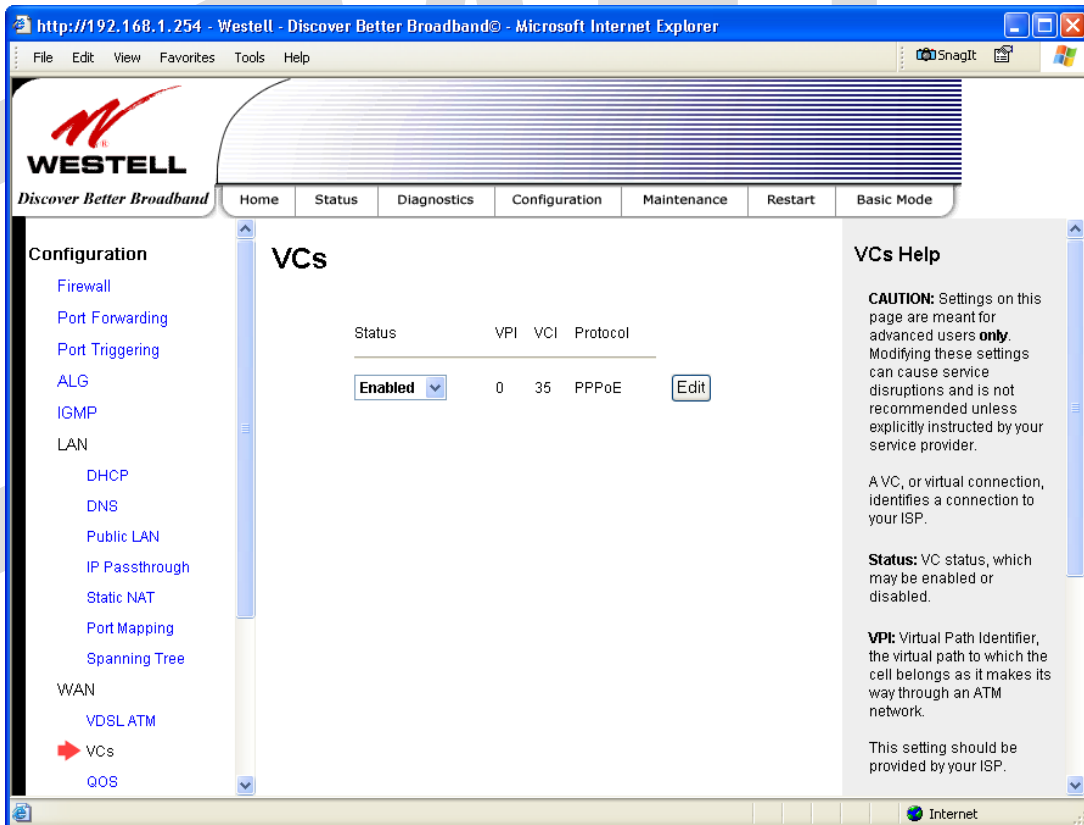
	<p>This allow you to activate the on-line reconfiguration that you want to use; you can use both, if desired. If a box is unchecked, the configuration will not be activated.</p> <p>Possible Responses: Bitswap – If this box is checked, Bitswap will be the activated. SRA – If this box is checked, SRA will be activated.</p>
Select phone line pair	<p>Factory Default = Inner Pair This feature is used with 2-line telephone wiring. It specifies which line is associated with the DSL. Select the desired radio button.</p> <p>Possible Responses: Inner – Represents Line 1. Outer – Represents Line 2.</p>

15.8.2 VCs

The following screen will be displayed if you select **Configuration > WAN > VCs** from the menu options. Click **Edit** to change the VC configuration settings.

NOTE:

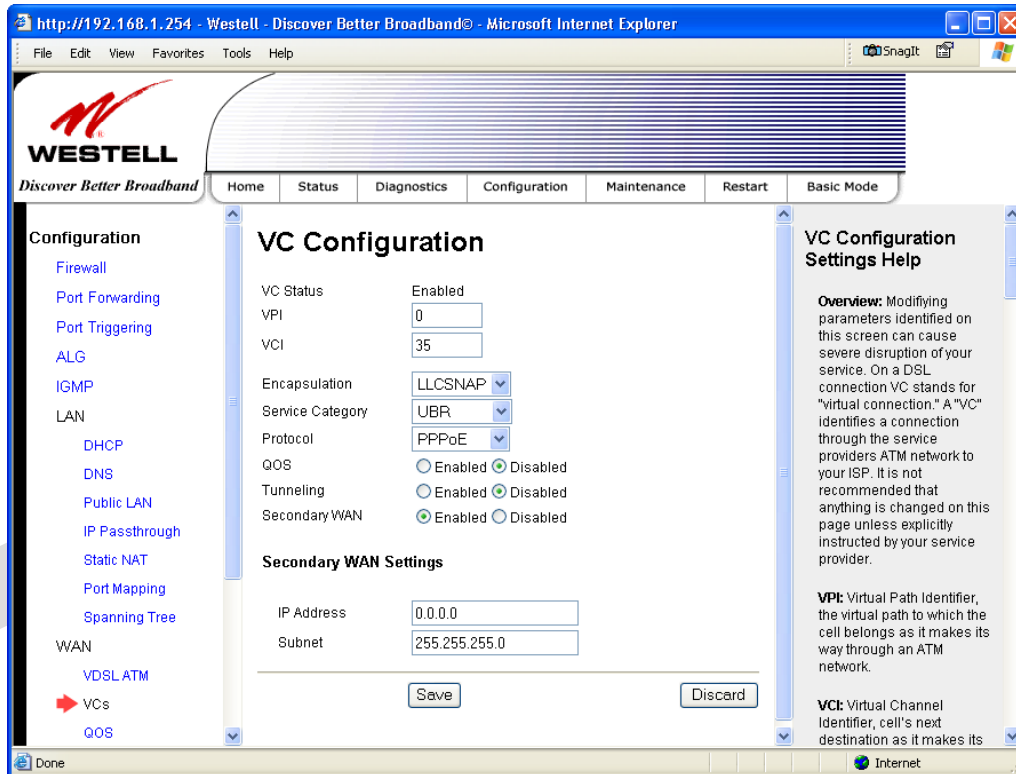
1. The protocol status must display **Enabled** to allow edits to its VC configuration.
2. If you experience any problems with your VC configuration, you can reset your Gateway by pressing the external hardware reset button on the rear of the Gateway.



If you clicked **Edit**, the following **VC Configuration** screen will appear. The **VC Configuration** screen allows you to edit your virtual connection (VC). A virtual connection identifies a connection through the service provider's ATM network to your ISP. Unlike physical hardware connections, virtual connections are defined by data.

If you change any settings in the **VC Configuration** screen, click the **Save** button to save the settings.

NOTE: If you experience any problems, you can reset your Gateway by pressing the external hardware reset button on the rear of the Gateway.



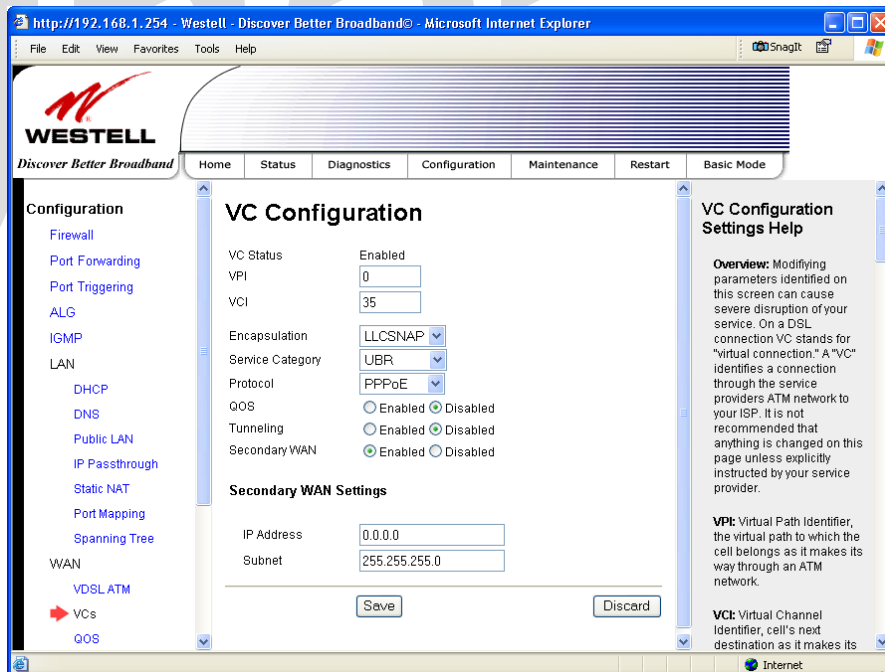
VC Configuration	
VC Status	Displays the status of your VC. The status must display Enabled in order to change the VC settings.
VPI	This setting allows you to change your VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	This setting allows you to change your VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
Encapsulation	Factory Default = LLCSNAP The encapsulation protocol used. Possible Responses: LLCSNAP VCMUX
Service Category	Factory Default = UBR Possible Responses: UBR-Unspecified Bit Rate UBR-PCR – Unspecified Bit Rate-Peak Cell Rate CBR – Constant Bit Rate rt-VBR – RealTime Variable Bit Rate nrt-VBR – Non-RealTime Variable Bit Rate
Protocol	Factory Default = PPPoE

	<p>This is a specific format used for transmitting data on your ISP’s network to access the Internet. You ISP will inform you of the protocol to use for your Internet connection.</p> <p>Possible Responses: PPPoE – Point-to-Point protocol over Ethernet Bridge – Bridging protocol Routed IP – Routed IP protocol</p>
QoS	<p>Factory Default = Disabled</p> <p>Quality of Service, which is determined by your Service Provider.</p> <p>To enable this feature, select the radio button labeled Enabled.</p>
Tunneling	<p>Factory Default = Disabled</p> <p>If Enabled, this option enables PPP traffic from the LAN to be bridged to the WAN. This feature enables you to use a PPPoE shim on the host computer to connect to the Internet service provider, by bypassing the Gateway’s capability to do this.</p> <p>Note: Tunneling is available in PPPoE mode only.</p>
Secondary WAN	<p>Factory Default = Enabled</p> <p>The secondary WAN interface is used for multicast traffic. This feature applies only when you are using PPPoE as the Primary WAN protocol.</p>
Secondary WAN Settings	
IP Address	The IP address of the secondary WAN.
Subnet	The subnet address of the secondary WAN.

NOTE: The values for IP Address and Subnet are all “Override of the value obtained from the PPP connection,” They default to “0.0.0.0,” in which case the override is ignored. Westell recommends that you do not change the values unless your ISP instructs you to change them.

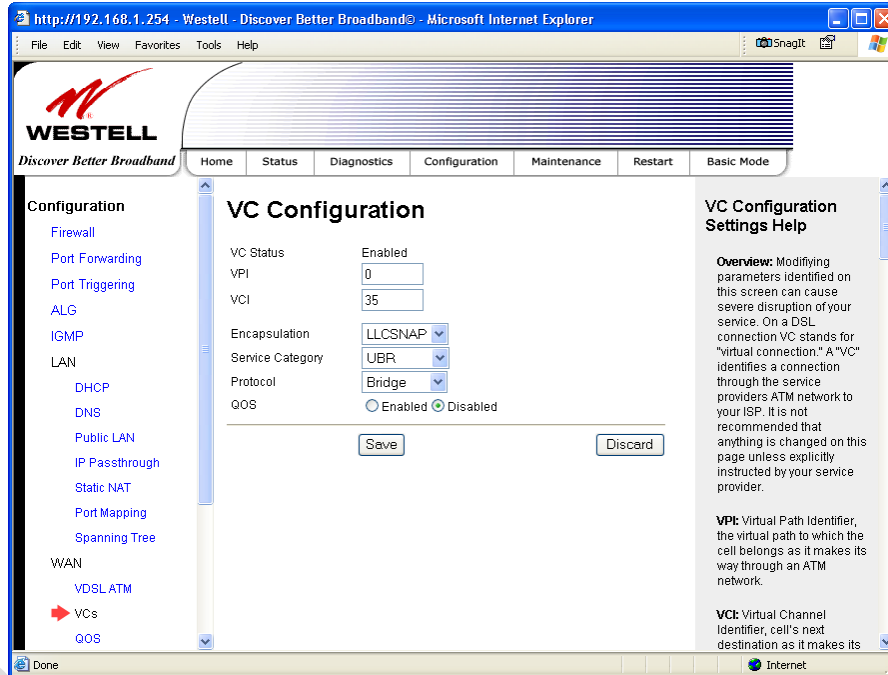
15.8.2.1 Configuring WAN Protocol for PPPoE Mode

To configure the WAN Protocol for PPPoE mode, select **PPPoE** from the **Protocol** drop-down menu; the following screen will be displayed. Enter the appropriate values, and then click **Save** to save your settings.



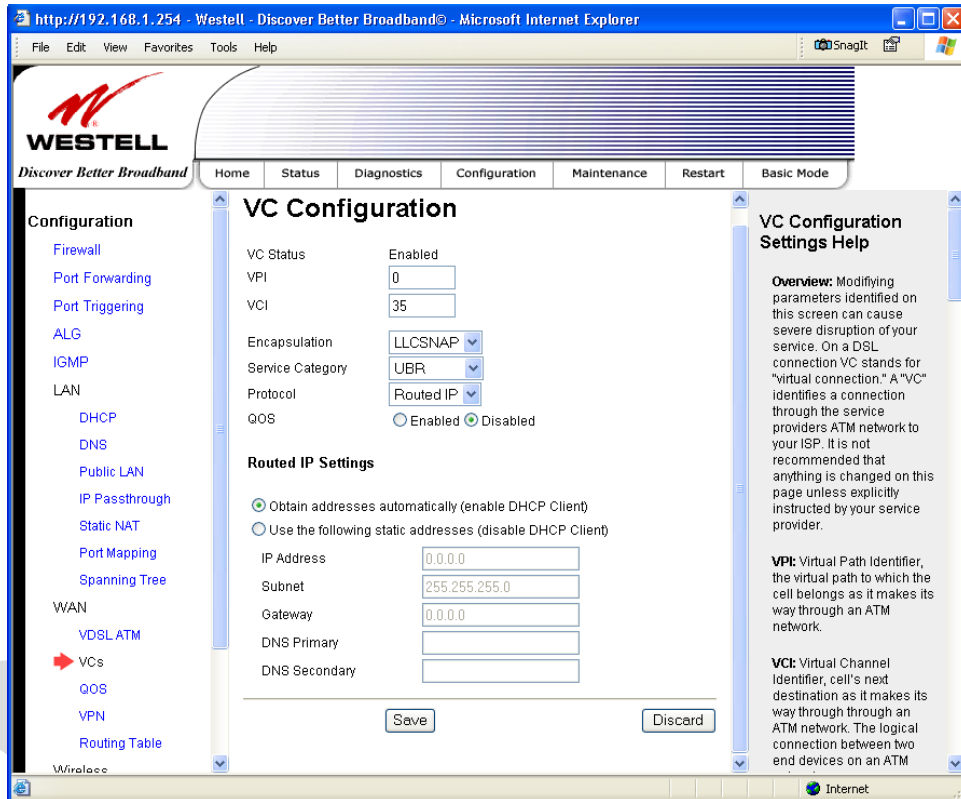
15.8.2.2 Configuring WAN Protocol for Bridge Mode—(MAC Bridge)

To configure the WAN Protocol for Bridge mode, select **Bridge** from the **Protocol** drop-down menu; the following screen will be displayed. Enter the appropriate values, and then click **Save** to save your settings.



15.8.2.3 Configuring WAN Protocol for Routed IP Mode

To configure the WAN Protocol for Routed IP mode, select **Routed IP** from the **Protocol** drop-down menu; the following screen will be displayed. Enter the appropriate values, and then click **Save** to save your settings.

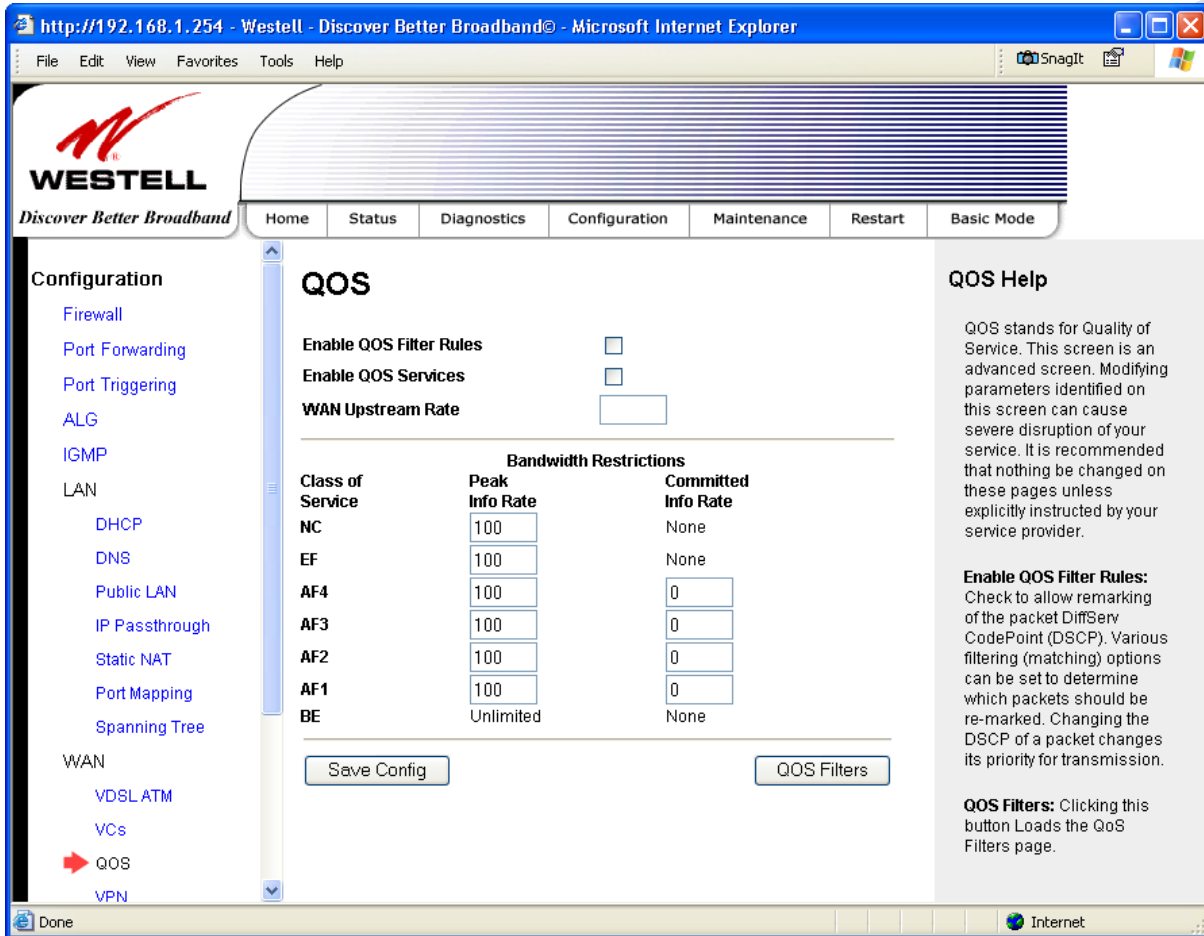


Routed IP Settings	
DHCP Client (enable DHCP Client) (disable DHCP Client)	Factory Default = Enable Possible Response: If (enable DHCP Client) is selected, the Gateway's DHCP client will be activated, and the Gateway will obtain its IP address, gateway address and DNS addresses automatically from the network. If (disable DHCP Client) is selected, this will deactivate the Gateway's DHCP client you must manually enter the IP address values that are provided by your ISP.
IP Address	Displays the Gateway's IP network address.
Subnet	Displays the Gateway's subnet mask settings.
Gateway	Displays the Gateway's IP gateway address.
DNS Primary	Displays the IP address of primary Domain Name Service (DNS) server your Gateway is using.
DNS Secondary	Displays the IP address of secondary DNS server your Gateway is using.

15.8.3 QOS

The following screen will be displayed if you select **Configuration > WAN > QOS** from the menu options. This screen enables you to configure the QOS services for your Gateway. If you change the settings in this screen, you must click **Save Config** to save the settings.

CAUTION: Changing the parameters on this screen could cause severe disruption of your service. It is recommended that you do not change any settings in this screen unless instructed by your service provider.

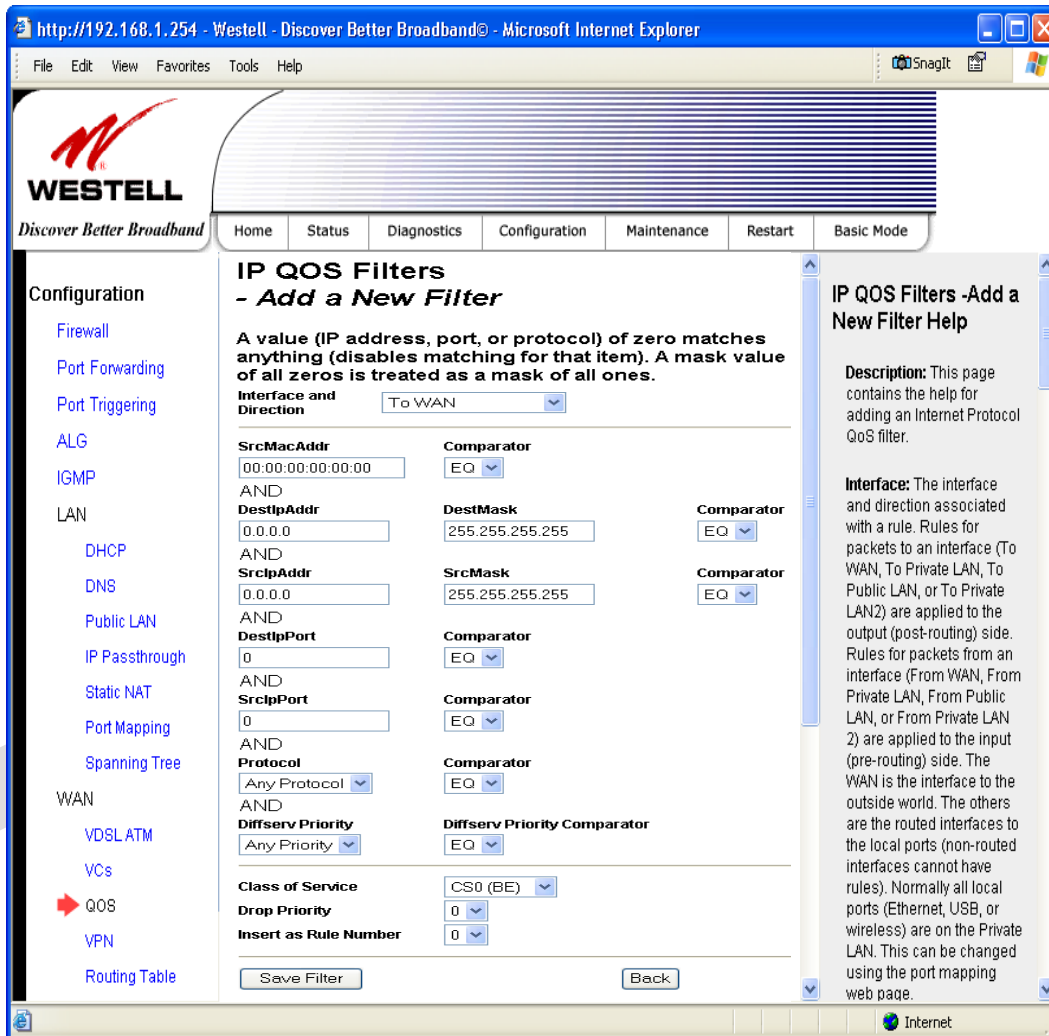


QOS	
Enable QOS Services	Factory Default = Enabled If Enabled (box is checked) this function will be activated. If Disabled, this function will be deactivated.
Class of Service	This enables you to partition network traffic into multiple priority levels or classes or service.
Peak Info Rate	The maximum allow rate for this priority.
QOS Services Committed Info Rate	The committed rate for this priority.
Max Queue Size	The number of packets that can be queued for this priority.

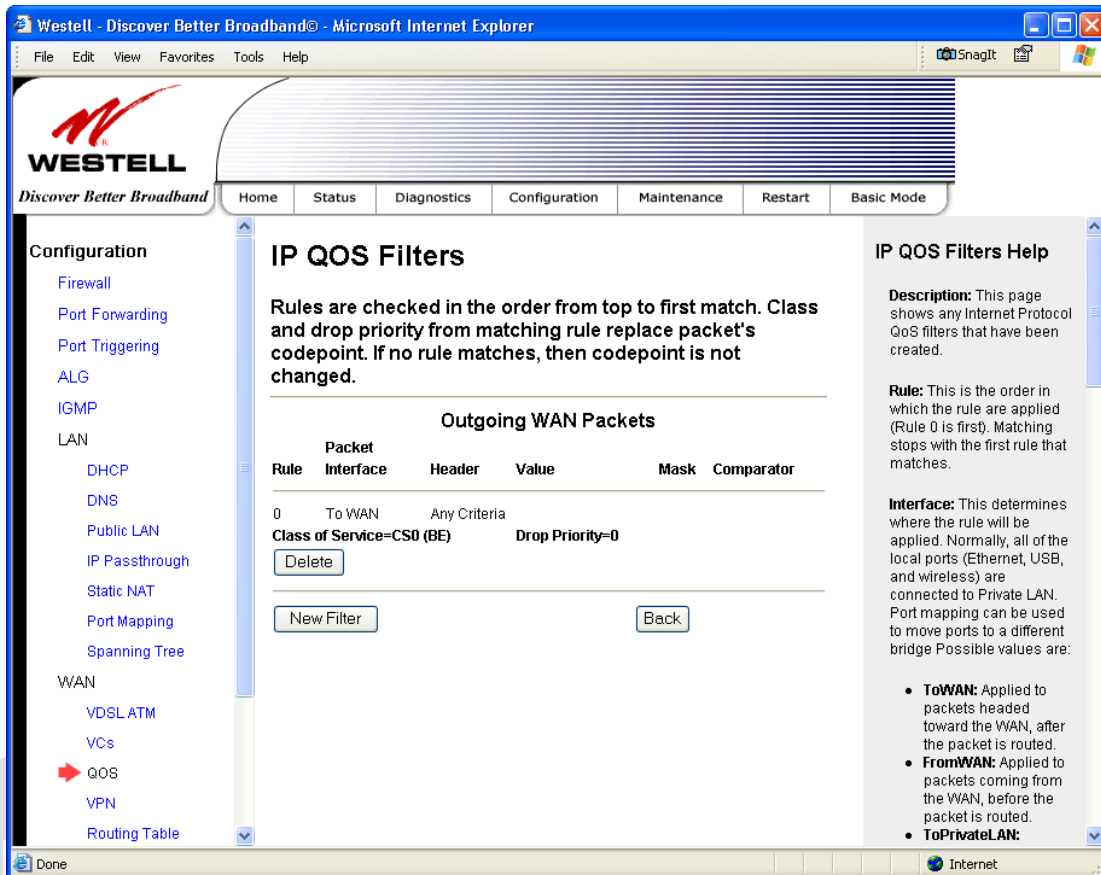
If you click **QOS filters**, the following screen will be displayed. Click **New Filter** to continue.



If you clicked **New Filter**, the following screen will be displayed. Select or enter your desired values and click **Save Filter** to save the settings.

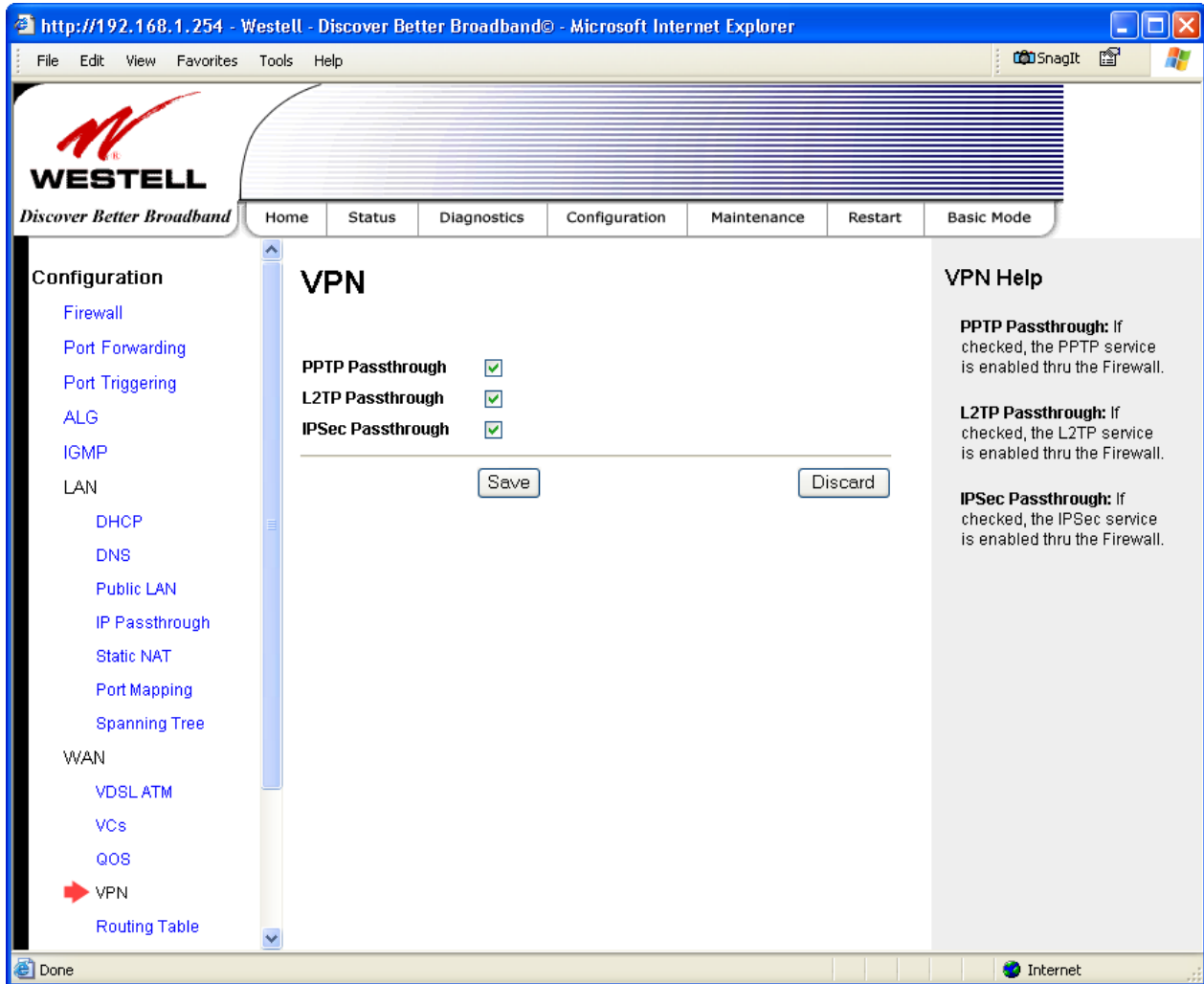


If you clicked **Save Filter**, the following screen will be displayed. To add a filter, click **New Filter**. If you want to delete a filter click **Delete**. To return to the previous screen, click **Back**.



15.8.4 VPN

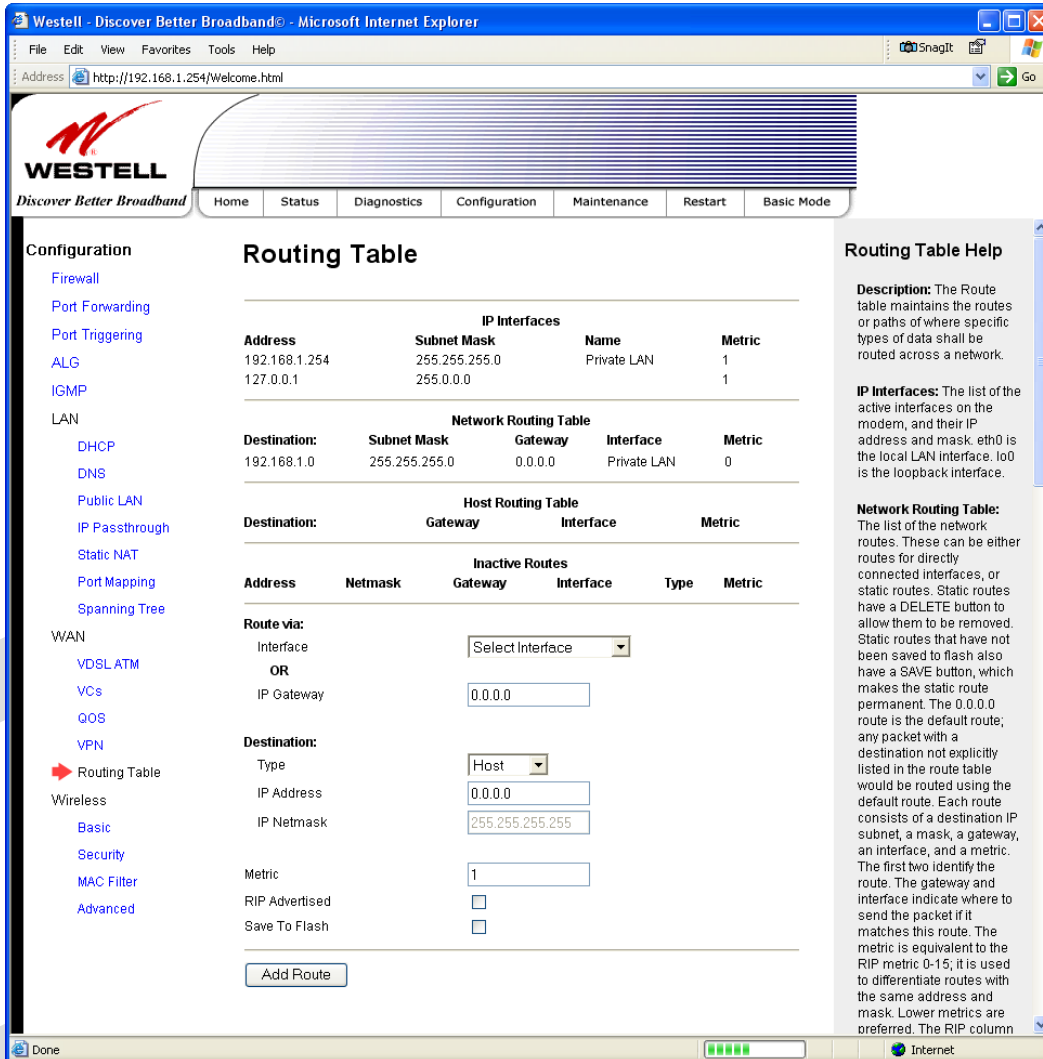
The following screen will be displayed if you select **Configuration > WAN > VPN** from the menu options. This screen enables you to configure the VPN services for your Gateway. If you change the settings in this screen, you must click **Save** to save the settings.



VPN	
PPTP Passthrough	When this box is checked, PPTP service is enabled through the firewall.
L2TP Passthrough	When this box is checked, PPTP service is enabled through the firewall.
IPSec Passthrough	When this box is checked, IPSec service is enabled through the firewall.

15.8.5 Routing Table

The following screen will be displayed if you select **Configuration > WAN > Routing Table** from the menu options. To add a route to the Network Routing Table, select the desired options from the drop-down menus, and then enter the appropriate values in the fields provided. Next, click **Add Route**.



The screenshot shows the Westell web interface for the Routing Table configuration. The main content area contains the following tables:

IP Interfaces			
Address	Subnet Mask	Name	Metric
192.168.1.254	255.255.255.0	Private LAN	1
127.0.0.1	255.0.0.0		1

Network Routing Table				
Destination:	Subnet Mask	Gateway	Interface	Metric
192.168.1.0	255.255.255.0	0.0.0.0	Private LAN	0

Host Routing Table			
Destination:	Gateway	Interface	Metric

Inactive Routes					
Address	Netmask	Gateway	Interface	Type	Metric

The 'Route via' section includes the following fields:

- Interface: Select Interface (dropdown)
- OR
- IP Gateway: 0.0.0.0 (text input)
- Destination:
 - Type: Host (dropdown)
 - IP Address: 0.0.0.0 (text input)
 - IP Netmask: 255.255.255.255 (text input)
- Metric: 1 (text input)
- RIP Advertised:
- Save To Flash:

An **Add Route** button is located at the bottom of the configuration area.

IP Interfaces	
The list of active interfaces on the Gateway, their IP addresses and subnet masks.	
Address	The IP interface address of the interface.
Subnet Mask	The subnet mask of the interface.
Name	The name assigned to the interface. Possible Names are: Private LAN – The main Ethernet interface. Public LAN – The interface for Private LAN mode. lo – The local loopback interface.
Metric	The numeric value assigned to this interface, used to calculate the best route to a destination address.

Networking Routing Table	
The list of the network routes. These can be either routes for directly connected networks, or static routes that have been entered.	
Destination	The IP subnet of the destination network.
Subnet Mask	The subnet mask of the destination network.
Gateway	The IP address of the default gateway for this route.
Interface	Indicates the name of the router's interface to use for this route.
Metric	The numeric value assigned to this route, used to calculate the best route to a destination network.
Host Routing Table	
The list of host routes. A host route is an IP route with a 32-bit mask.	
Destination	The IP address of the destination host.
Gateway	The IP address of the default gateway for this route.
Interface	Indicates the name of the router's interface to use for this route.
Metric	The numeric value assigned to this route, used to calculate the best route to a destination network.
Inactive Routes	
The list of routes whose interface is currently not in service.	
Address	The IP address of the destination network.
Netmask	The subnet mask of the destination network.
Gateway	The IP address of the default gateway for this route.
Interface	The name of the router's interface associated with this route.
Type	Indicates if this route is a network route, a host route, or a default route.
Metric	The numeric value assigned to this route used to calculate the best route to a destination network.
The following sections allow you to add static routes to the gateway's routing table.	
Route Via	
Allows you to specify either the interface or the default gateway that the router should use for this static route. If an interface is not specified, the correct interface will be automatically chosen, based on the gateway addresses.	
Interface	Select the interface that will be used for this static route. If you enter an interface, you cannot specify a default gateway.
IP Gateway	Enter the IP address of the default gateway used for this static route. The specified gateway must be reachable; this means that the Gateway must have a route to the gateway. You must specify either an interface or a gateway for each static route.
Destination	
Allows you to specify the destination network or host.	
Type	Factory Default = Host Possible Responses: Host – The static route is assigned to a single IP host. Network – The static route is assigned to a network. Default – The static route is assigned to a default route.
IP Address	The IP subnet of the destination network or host.
IP Netmask	The subnet mask of the destination network. If the route type was a host, a 32-bit subnet mask will be automatically populated.
Metric	The numeric value assigned to this route, used to calculate the best route to a destination network.
RIP Advertised	This determines whether or not to advertise the static route using RIP. (RIP must also be enabled before the route will be advertised.) If Enabled (box is checked), RIP Advertised will be activated. If Disabled, RIP Advertised will not be activated.
Save to Flash	If Enabled (box is checked), the route will be made permanent by saving it to flash memory. If Disabled, the route will disappear the next time the Gateway restarts.
Add Route	This button enables you to add a new static route in the Gateway. Note: When adding a route, you can need to reload the page for the route to appear in the "active" Routes.

15.9 Wireless Configuration

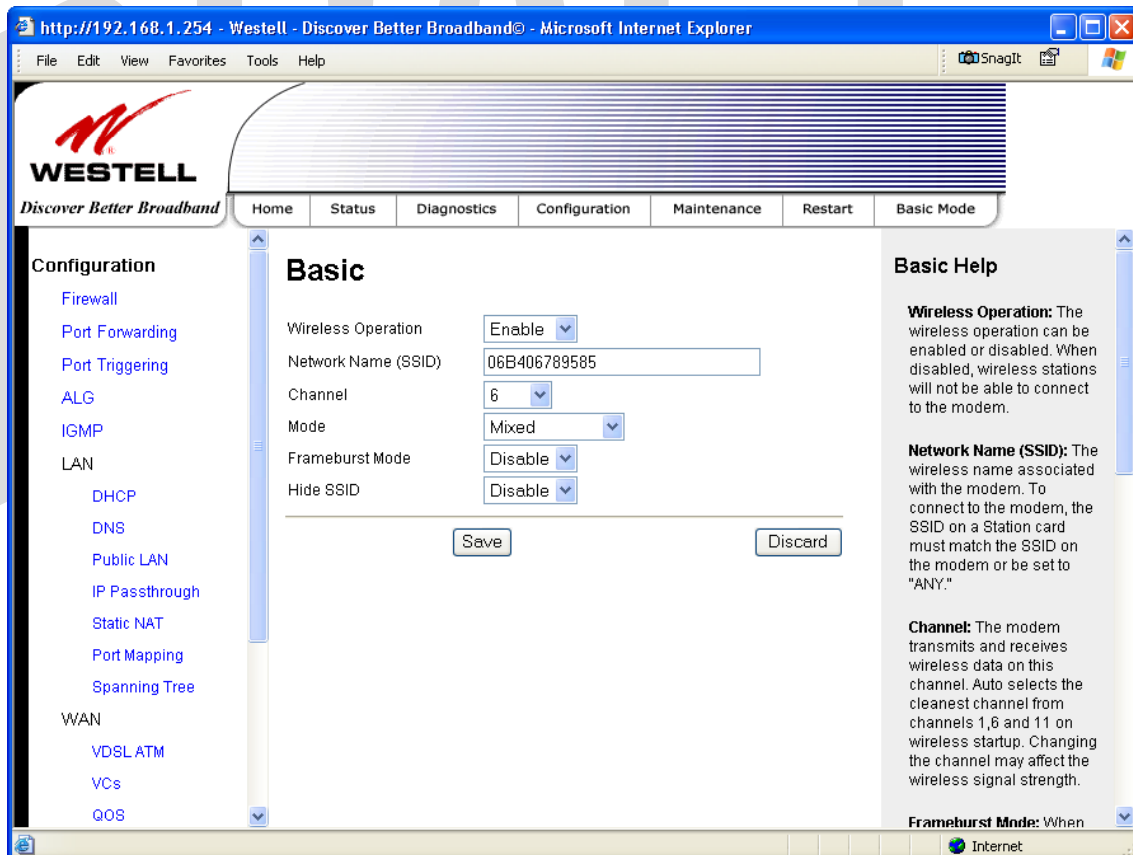
This section explains how to configure your Gateway's Wireless settings.

IMPORTANT:

1. If you are connecting to the Gateway via a wireless network adapter, the SSID must be the same for both the Gateway and your PC's wireless network adapter. The default SSID for the 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 Gateway) before you begin the account setup and configuration procedures. Later, for privacy you can change the SSID.
2. Client PCs can use any wireless 802.11b/g certified card to communicate with the Modem. The Wireless card and Gateway 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 your wireless network adapter.**
3. Be sure to enter the default WEP key into your wireless adapter. The WEP key is located below the barcode on the bottom of your Gateway.

15.9.1 Basic

The following screen will be displayed if you select **Configuration > Wireless > Basic** from the menu options. Select the desired settings, and then click **Save** to save your settings.



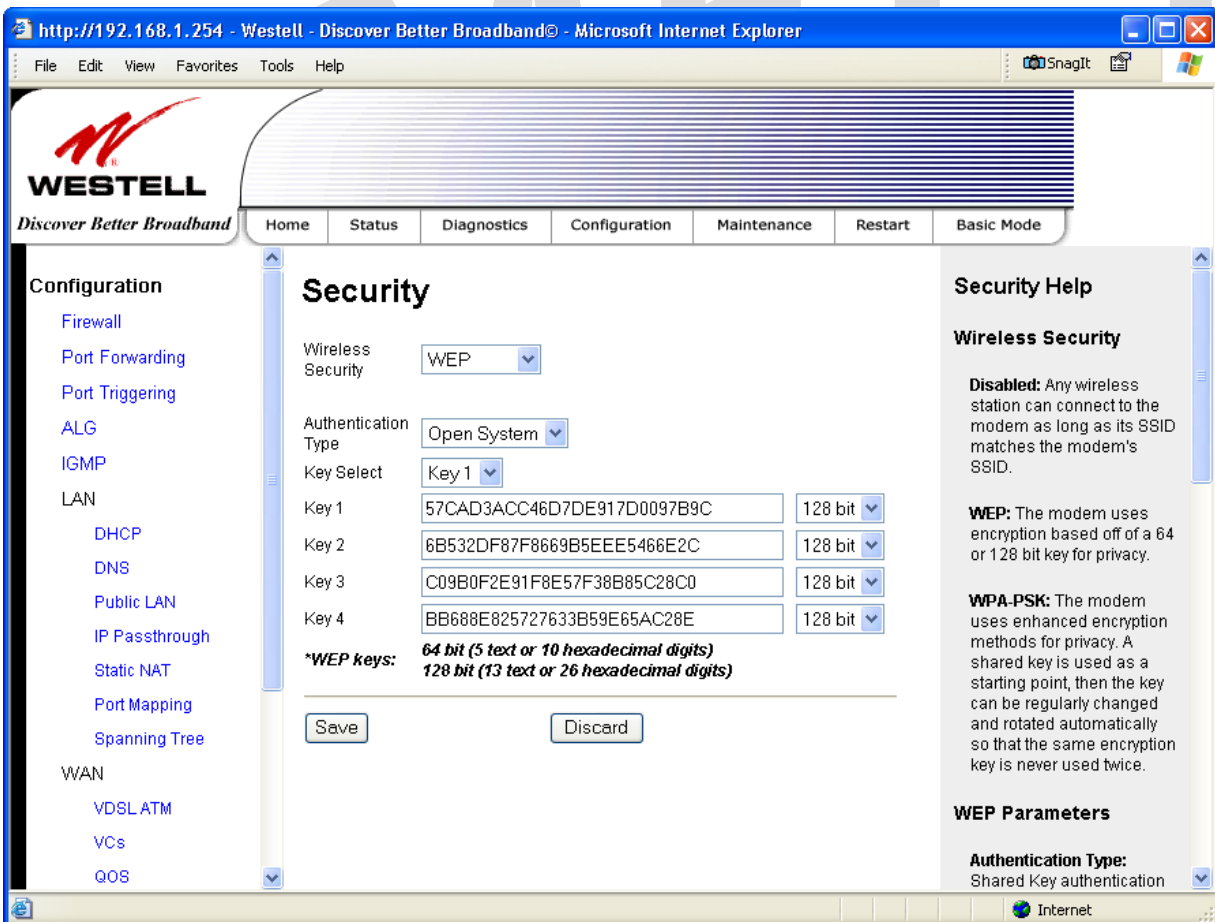
Wireless Basic Configuration	
Wireless Operation	Factory Default = Enabled Displays the current setting of the Gateway’s wireless operation. When disabled, no wireless stations will be able to connect to the Gateway.
Network Name (SSID)	This string (32 characters or less) is the name associated with the Gateway. To connect to the Gateway, the SSID on a Station card must match the SSID on the Gateway card or be set to “ANY.” (Note: If the SSID on a Gateway is hidden, at the station card you must manually type the SSID of the Gateway to which you are trying to connect.)
Channel	The AP transmits and receives data on this channel. The number of channels to choose from is pre-programmed into the AP card. The Gateway transmits and receives data on this channel. Station cards do not have to be set to the same channel as the AP; the station cards scan all channels and look for the Gateway with the correct SSID. Possible Responses: 1 through 11
Mode	This setting allows station to communicate with the Gateway. Possible Responses: Mixed: Station using any of the 802.11b and 802.11g rates can communicate with the Gateway. Legacy Mixed: Same as Mixed, but also allows older 802.11b cards to communicate with the Gateway. 11b only: Communication with the Gateway is limited to 802.11b 11g only: Communication with the Gateway is limited to 802.11g
Frameburst Mode	If enabled, additional algorithms are used for increased throughput. If Disabled, this feature will not be activated.
Hide SSID	If enabled, the Gateway will not broadcast the SSID. To connect to the Gateway, each Station must configure its SSIDs so that it matches the Gateway’s Network Name (SSID). If Disabled, this function will not be activated.

15.9.2 Wireless Security

The following screen will be displayed if you select **Configuration > Wireless > Security** from the menu. Select the desired security option from the **Wireless Security** drop-down menu. After you have configured your wireless security settings, click **Save** and then click **OK** in the pop-up screen to save the settings.

IMPORTANT:

1. If you are connecting to the Gateway via a wireless network adapter, the SSID must be the same for both the Gateway and your PC's wireless network adapter. The default SSID for the 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 Gateway) before you begin the account setup and configuration procedures. Later, for privacy you can change the SSID.
2. Client PCs can use any wireless 802.11b/g certified card to communicate with the Modem. The Wireless card and Gateway 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 your wireless network adapter.**
3. Be sure to enter the default WEP key into your wireless adapter. The WEP key is located below the barcode on the bottom of your Gateway.



The screenshot shows the Westell Gateway web interface in Microsoft Internet Explorer. The browser address bar shows 'http://192.168.1.254 - Westell - Discover Better Broadband© - Microsoft Internet Explorer'. The page title is 'Discover Better Broadband'. The navigation menu includes Home, Status, Diagnostics, Configuration, Maintenance, Restart, and Basic Mode. The 'Configuration' menu is expanded, showing options like Firewall, Port Forwarding, Port Triggering, ALG, IGMP, LAN, DHCP, DNS, Public LAN, IP Passthrough, Static NAT, Port Mapping, Spanning Tree, WAN, VDSL ATM, VCs, and QOS. The 'Security' page is displayed, showing the following settings:

- Wireless Security: WEP (selected)
- Authentication Type: Open System (selected)
- Key Select: Key 1 (selected)
- Key 1: 57CAD3ACC46D7DE917D0097B9C (128 bit)
- Key 2: 6B532DF87F8669B5EEE5466E2C (128 bit)
- Key 3: C09B0F2E91F8E57F38B85C28C0 (128 bit)
- Key 4: BB688E825727633B59E65AC28E (128 bit)

*WEP keys: 64 bit (5 text or 10 hexadecimal digits)
128 bit (13 text or 26 hexadecimal digits)

Buttons: Save, Discard

Security Help

Wireless Security

Disabled: Any wireless station can connect to the modem as long as its SSID matches the modem's SSID.

WEP: The modem uses encryption based off of a 64 or 128 bit key for privacy.

WPA-PSK: The modem uses enhanced encryption methods for privacy. A shared key is used as a starting point, then the key can be regularly changed and rotated automatically so that the same encryption key is never used twice.

WEP Parameters

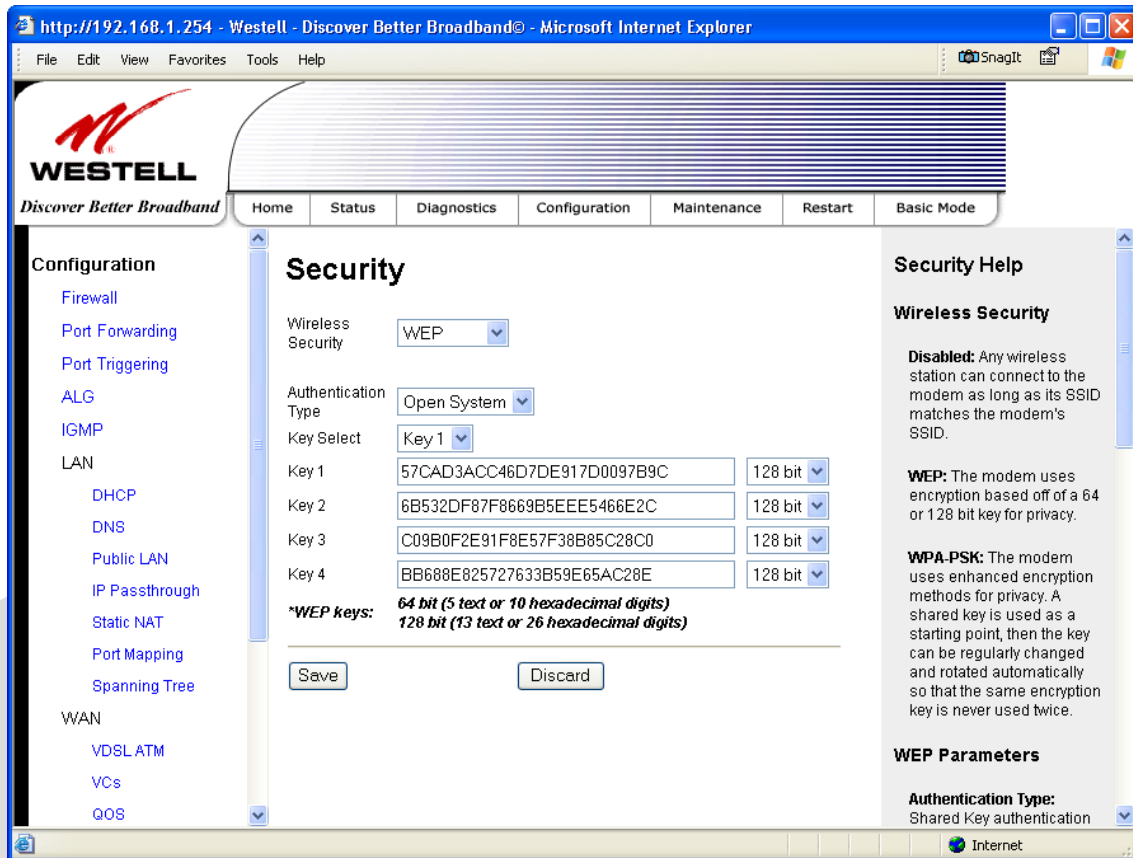
Authentication Type: Shared Key authentication (selected)

Wireless Security	
Wireless Security	<p>Factory Default = WEP</p> <p>Possible Responses:</p> <p>Disabled: No security is used.</p> <p>WEP: WEP encryption used to secure the data being sent to and from the Gateway; when WEP is enabled, the risk of someone nearby accessing the Gateway is minimized.</p> <p>WPA-PSK: This setting is used to encrypt and secure the connection and the data being sent to and from the Gateway.</p> <p>This string (8 to 63 characters of 64 hex characters) is the key used for encrypting packets being sent to and from the Gateway. This key must be the same in both the Gateway and the station.</p>
Authentication Type	<p>Factory Default = Open System</p> <p>Possible Responses:</p> <p>Open System: Open System authentication allows any station to associate with the wireless network but only stations with the valid WEP key can send or receive data from the Gateway. Open System authentication is considered to be more secure than Shared Key authentication.</p> <p>Shared Key: Shared Key authentication requires the station to authenticate with the Gateway using the WEP key before it can associate with the wireless network.</p>
Key Select	<p>Factory Default = Key 1</p> <p>Select Key 1 to Key 4 as the WEP key to be used. Note: The key position must be the same in both the Gateway and the wireless station.</p>
Key n (where n is 1 - 4 for WEP and is blank for WPA-PSK)	<p>The WEP key is treated as either text or hexadecimal (hex) characters. The number of characters is based on the key size selected. The key size 64-bit is either 5 text or 10 hex characters, 128-bit is either 13 text or 26 hex characters. Hexadecimal characters are 0-9 and A-F (or a-f). This key must be the same in both the Gateway and the wireless station.</p>

15.9.2.1 Enabling WEP Security

If you selected **WEP** from the **Wireless Security** drop-down menu, the following screen will be displayed. Enter the appropriate values, and then click **Save** to save the settings.

NOTE: The WEP key must be 64 bit (5 text characters or 10 hexadecimal digits in length) or 128 bit (13 text characters or 26 hexadecimal characters in length).

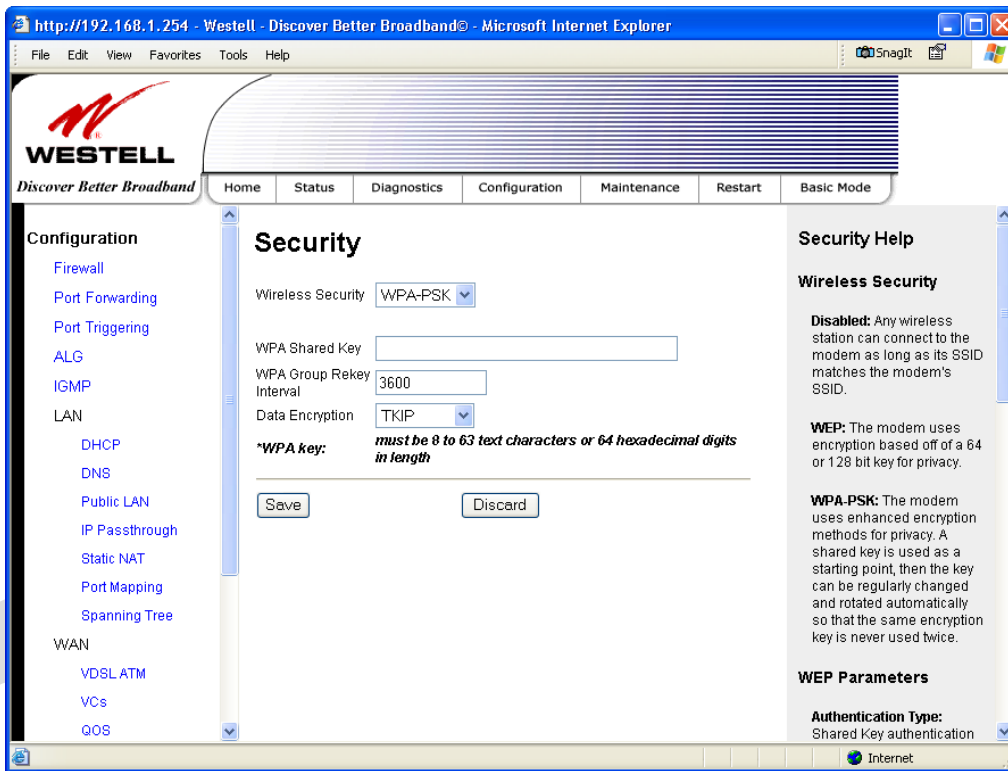


Wireless Security (WEP)	
Wireless Security	WEP has been selected as the wireless security method used.
Authentication Type	Factory Default = Open System Possible Responses: Open System: Open System authentication allows any station to associate with the wireless network but only stations with the valid WEP key can send or receive data from the Gateway. Open System authentication is considered to be more secure than Shared Key authentication. Shared Key: Shared Key authentication requires the station to authenticate with the Gateway using the WEP key before it can associate with the wireless network.
Key Select	Factory Default = Key 1 Select Key 1 to Key 4 as the WEP key to be used. Note: The key position must be the same in both the Gateway and the wireless station.
Key n (where n is 1 - 4 for WEP and is blank for WPA-PSK)	The WEP key is treated as either text or hexadecimal (hex) characters. The number of characters is based on the key size selected. The key size 64-bit is either 5 text or 10 hex characters, 128-bit is either 13 text or 26 hex characters. Hexadecimal characters are 0-9 and A-F (or a-f). This key must be the same in both the Gateway and the wireless station.

15.9.2.2 Enabling WPA-PSK Security

If you selected **WPA-PSK** from the **Wireless Security** drop-down menu, the following screen will be displayed. Enter the appropriate values, and then click **Save** to save the settings.

NOTE: The WPA key must be 8 to 63 characters or 64 hexadecimal digits in length.

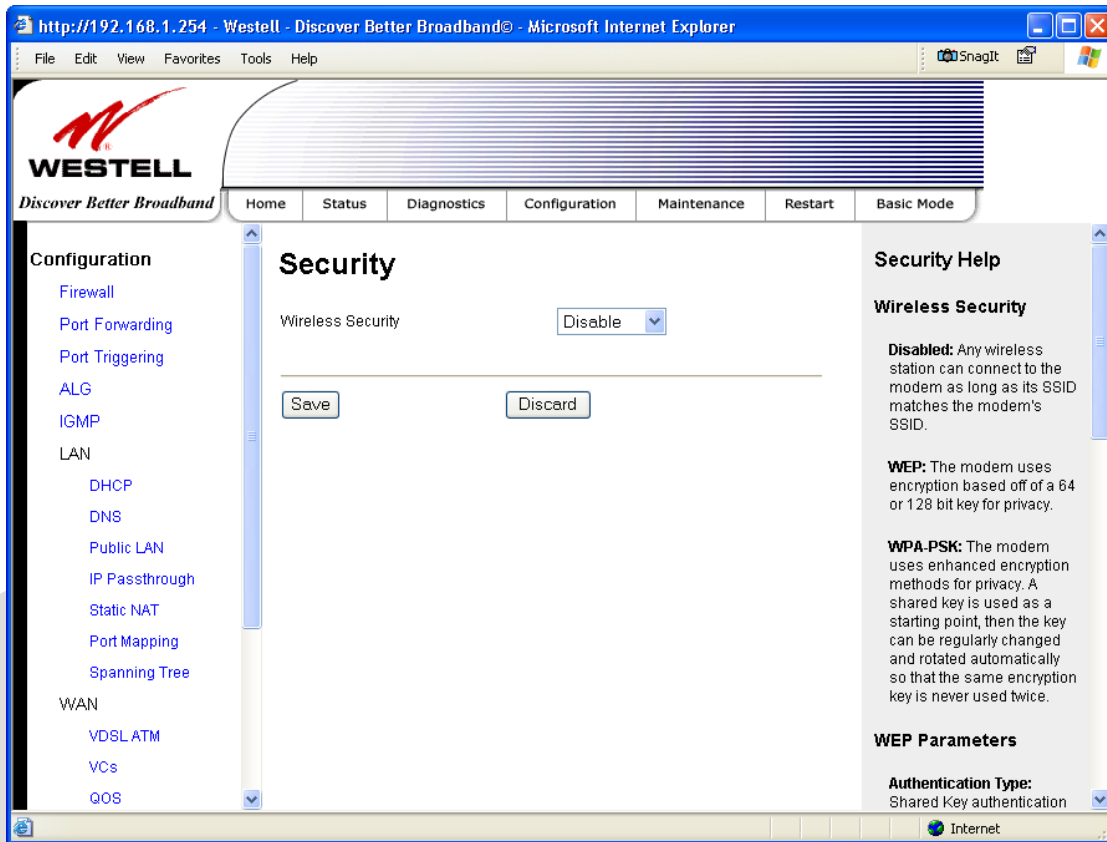


Wireless Security (WPA-PSK)	
Wireless Security	WPA-PSK has been selected as the wireless security method used.
WPA Shared Key	This string (8 to 63 characters of 64 hex characters) is the key used for encrypting packets being sent to and from the Gateway. Hexadecimal characters are 0-9 and A-F (or a-f). The key must be entered in both the Gateway and the wireless station. Using random characters in your WPA Shared Key increases the security of your wireless connection.
WPA Group Rekey Interval	The number of seconds between rekeying the WPA group key. A value of "0" means that rekeying is disabled. The Shared Key is the initial key and new keys are created and used, based on that key, at each Rekey Interval.
Data Encryption	Factory Default = TKIP Possible Responses: 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 Gateway to accept either TKIP or AES encryption

15.9.2.3 Disabling Wireless Security

If you selected **Disable** from the **Wireless Security** drop-down menu, the following screen will be displayed. Click **Save** to save the setting.

IMPORTANT: When wireless security is disabled, any wireless station can connect to your Gateway as long as its SSID matches your Gateway's SSID.

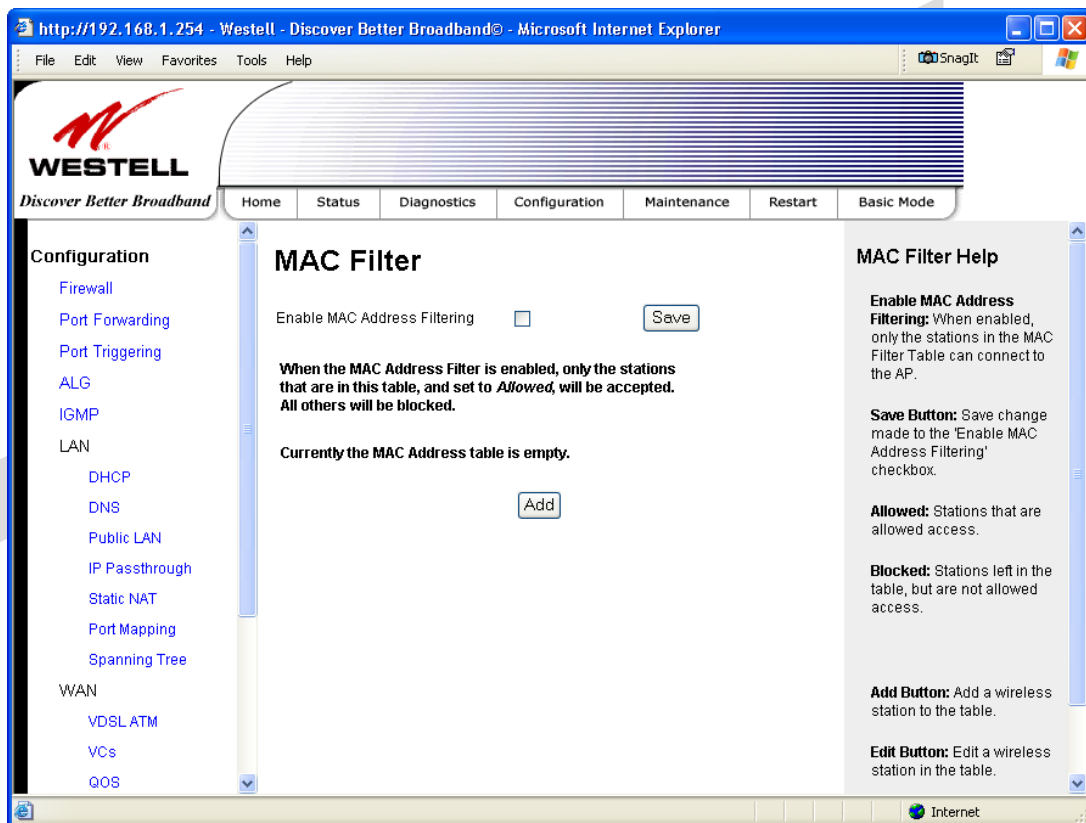


15.9.3 MAC Filter

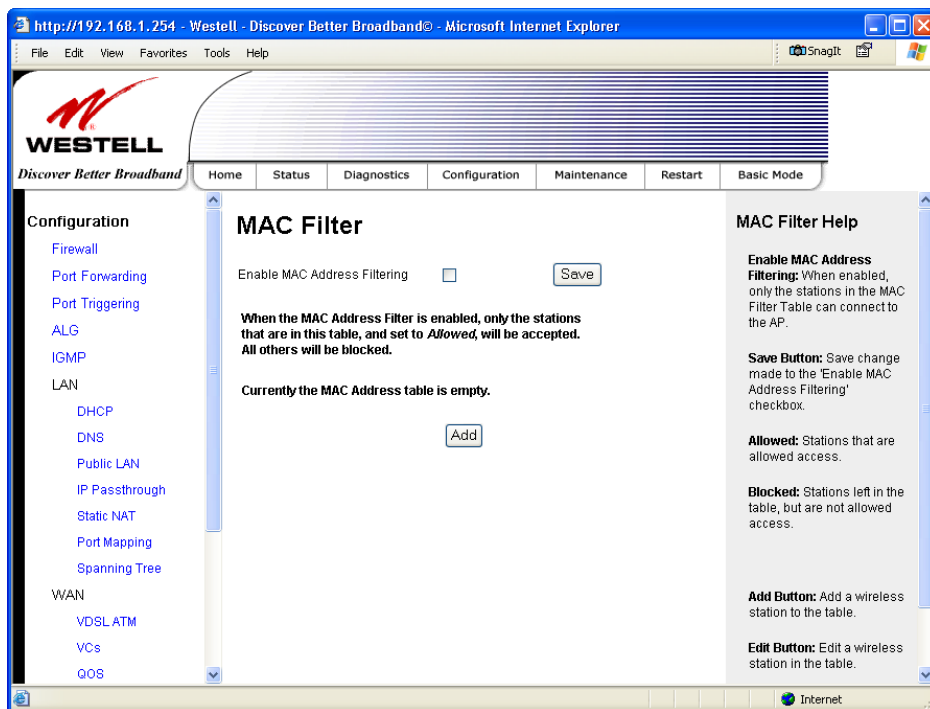
The following screen will be displayed if you select **Configuration > Wireless > MAC Filter** from the menu options. This screen enables you to configure the MAC filter settings for your Gateway.

After you have finished adding MAC addresses from the MAC Filter table, as explained in the following paragraphs, click the box adjacent to **Enable MAC Address Filtering** (a check mark will appear in the box). Next, click **Save** to save your settings.

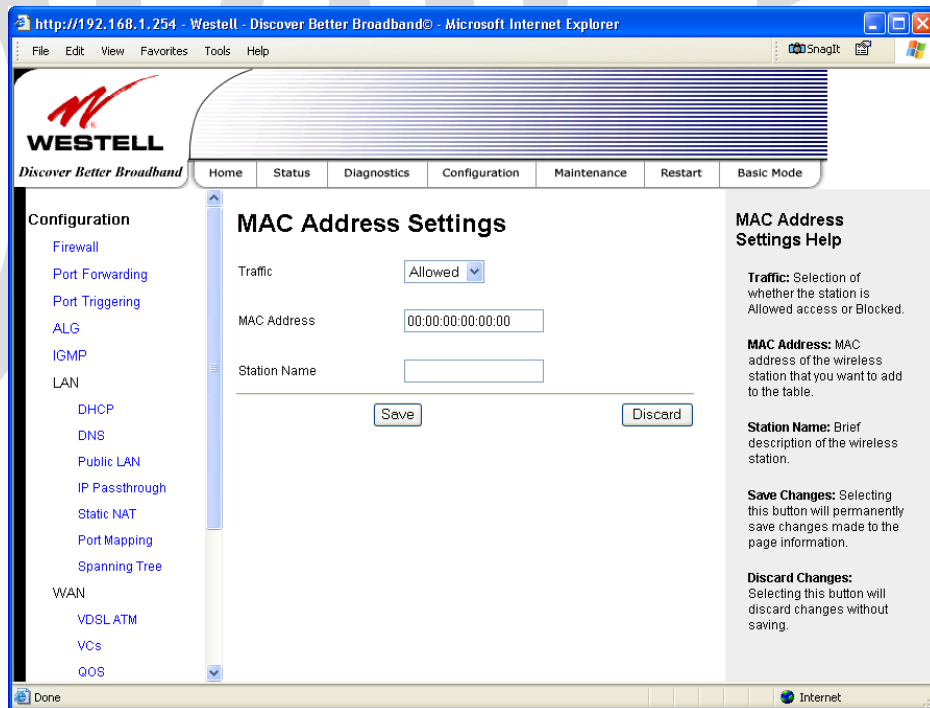
NOTE: When the MAC address Filter is enabled (box is checked), only the stations that are in the MAC Filter table and that are set to **Allowed** will be accepted by the Gateway. All other stations will be blocked.



To add stations to the MAC Address table, click the **Add** button.



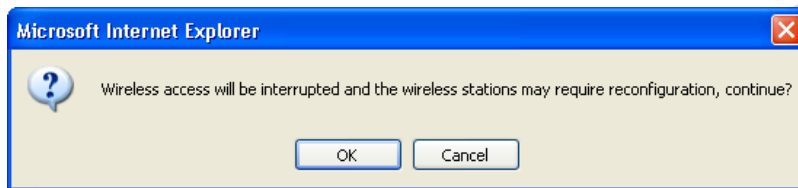
If you clicked **Add**, the following screen will be displayed. Select the desired traffic setting, and then enter the appropriate values in the fields provided. Click **Save** to save the settings.



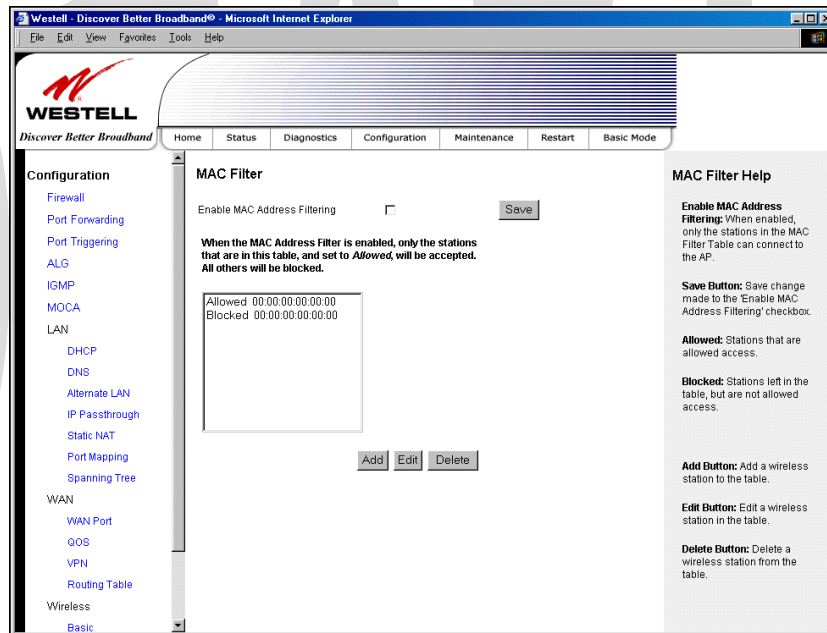
MAC Address Settings	
Traffic	Factory Default = Allowed If Blocked is selected, the station will be blocked (it cannot access the Gateway).
MAC Address	Factory Default = 00:00:00:00:00:00 The MAC address of the wireless station you want to add.
Station Name	The name of the wireless station you want to add.

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

NOTE: When you add a MAC address, wireless access will be interrupted and wireless stations may require reconfiguration.



If you clicked **OK**, in the preceding pop-up screen, the following screen will be displayed. The screen displays the list of MAC addresses added to the **MAC Address Filter Table**. You may now add, edit, or delete MAC addresses from the table by clicking on the desired MAC address (displayed in the window) and then by clicking the desired button. Click **OK** in the pop-up screen to continue.

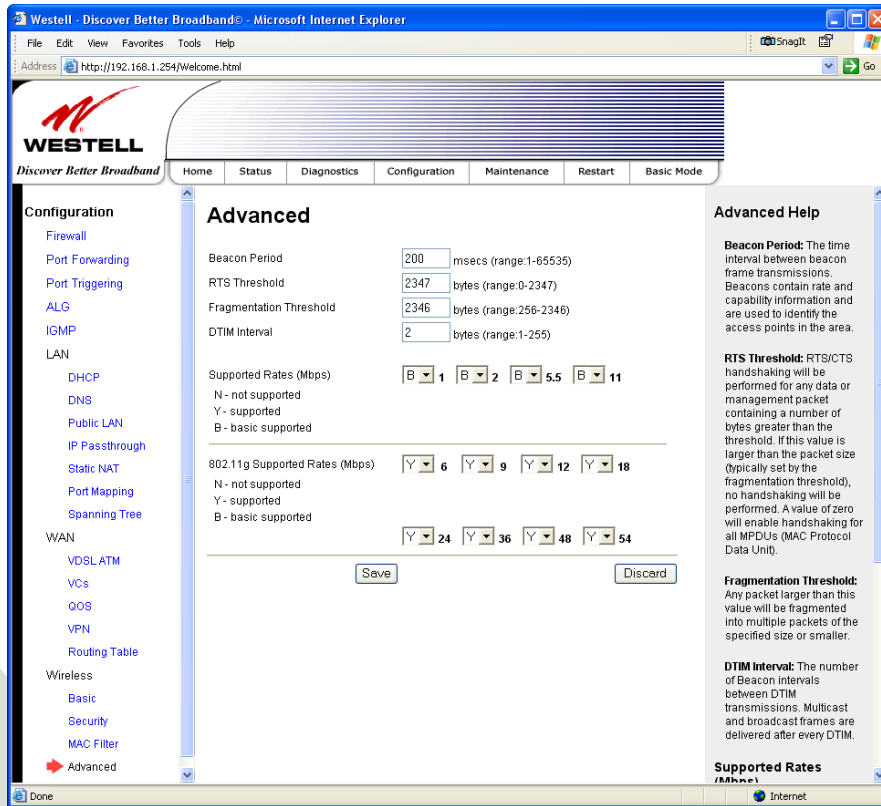


After you have finished adding MAC addresses to the MAC Filter table, click the box adjacent to **Enable MAC Address Filtering** (a check mark will appear in the box). Next, click **Save** to save your settings.

NOTE: When the MAC address Filter is enabled (box is checked), only the stations that are in MAC Filter table and that are set to **Allowed** will be accepted by the Gateway. All other stations will be blocked.

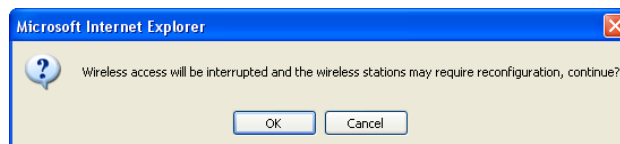
15.9.4 Advanced Wireless Settings

The following screen will be displayed if you select **Configuration > Wireless > Advanced** from the menu options. Enter the appropriate values, and then 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 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 MPDU 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 Gateway will attempt to use. The rates are also broadcast within the connection protocol as the rates supported by the Gateway.

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

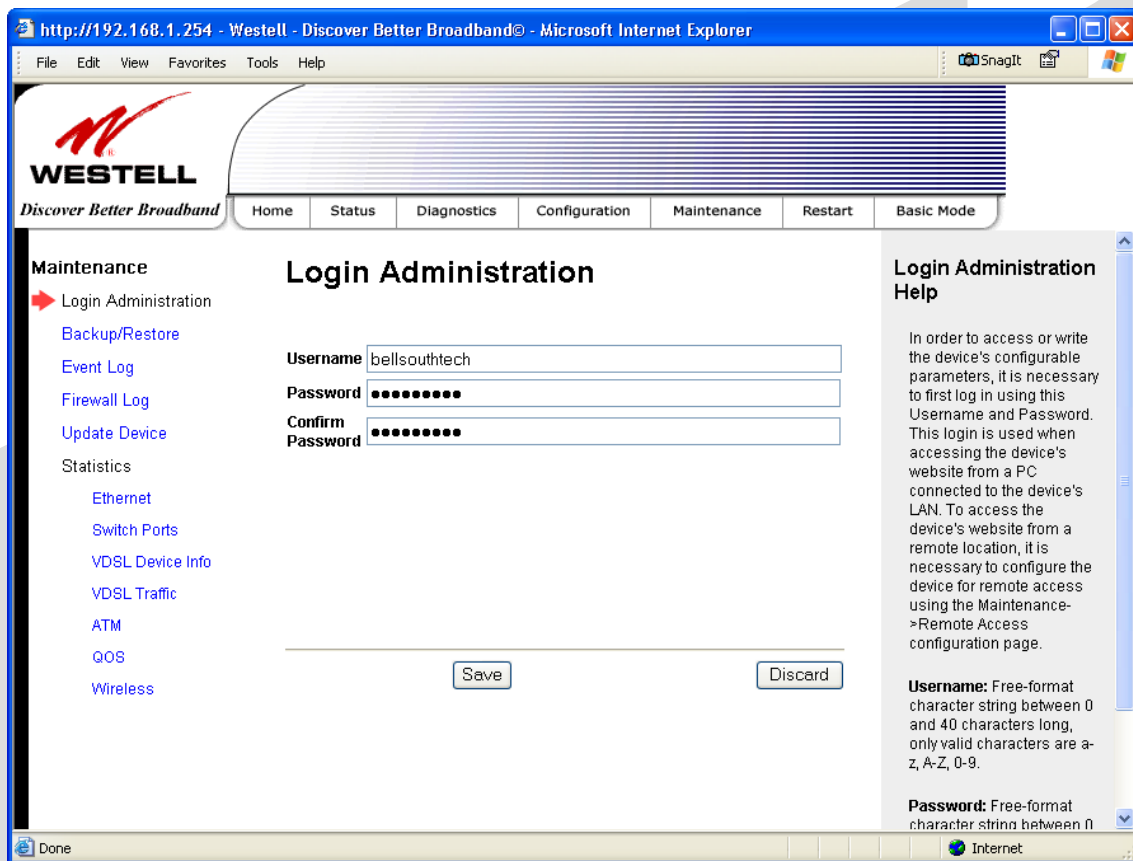


16. MAINTENANCE

16.1 Login Administration

The following screen will be displayed if you select **Maintenance > Login Administration** from the menu options. Enter the appropriate values, and then click **Save** to save the settings.

NOTE: Password must be at least 6 characters and must not exceed 12 characters long. Alphanumeric values are permitted. The **Password** and **Confirm Password** fields are masked with “*” for security measures.



Login Administration	
Username	The administrator's username. This is a free-format character string between 5 and 12 characters long, no spaces.
Password	The administrator's password. This is a free-format character string between 6 and 12 characters long, no spaces.
Confirm Password	The identical value that was entered in the password field.

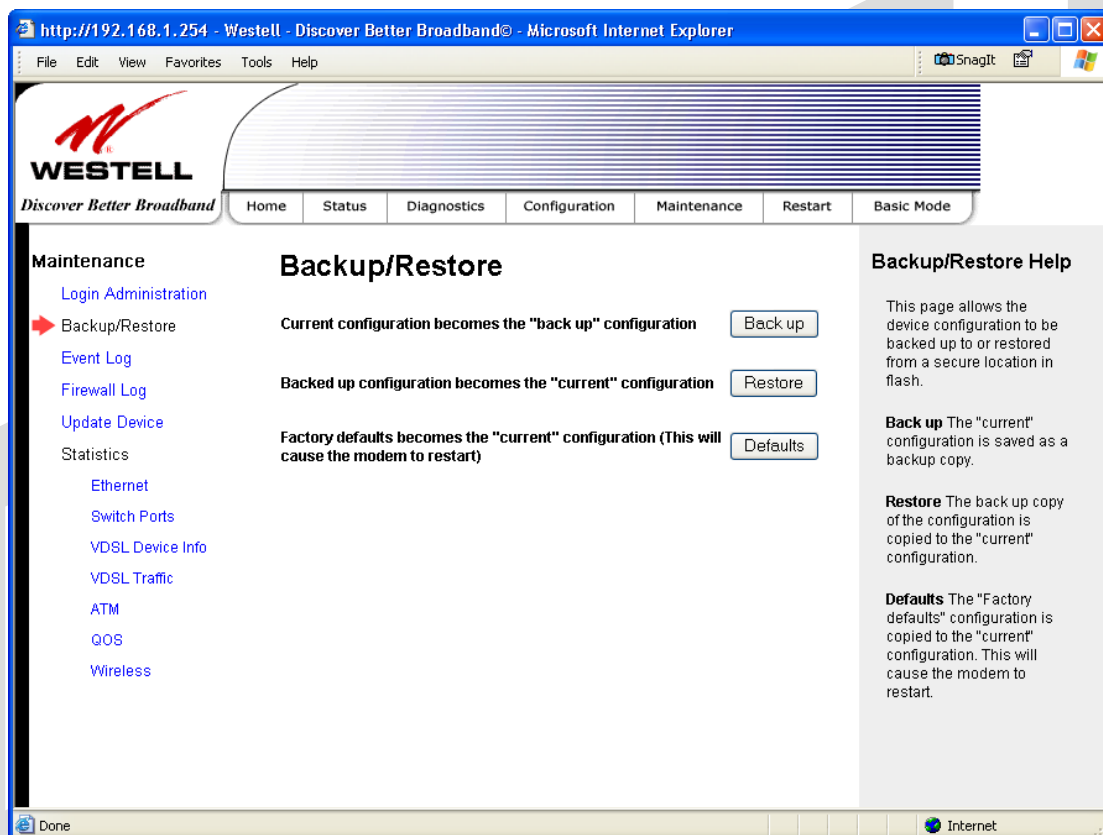
16.2 Backup/Restore

The following screen will be displayed if you select **Maintenance > Backup/Restore** from the menu options.

Select any of the following options:

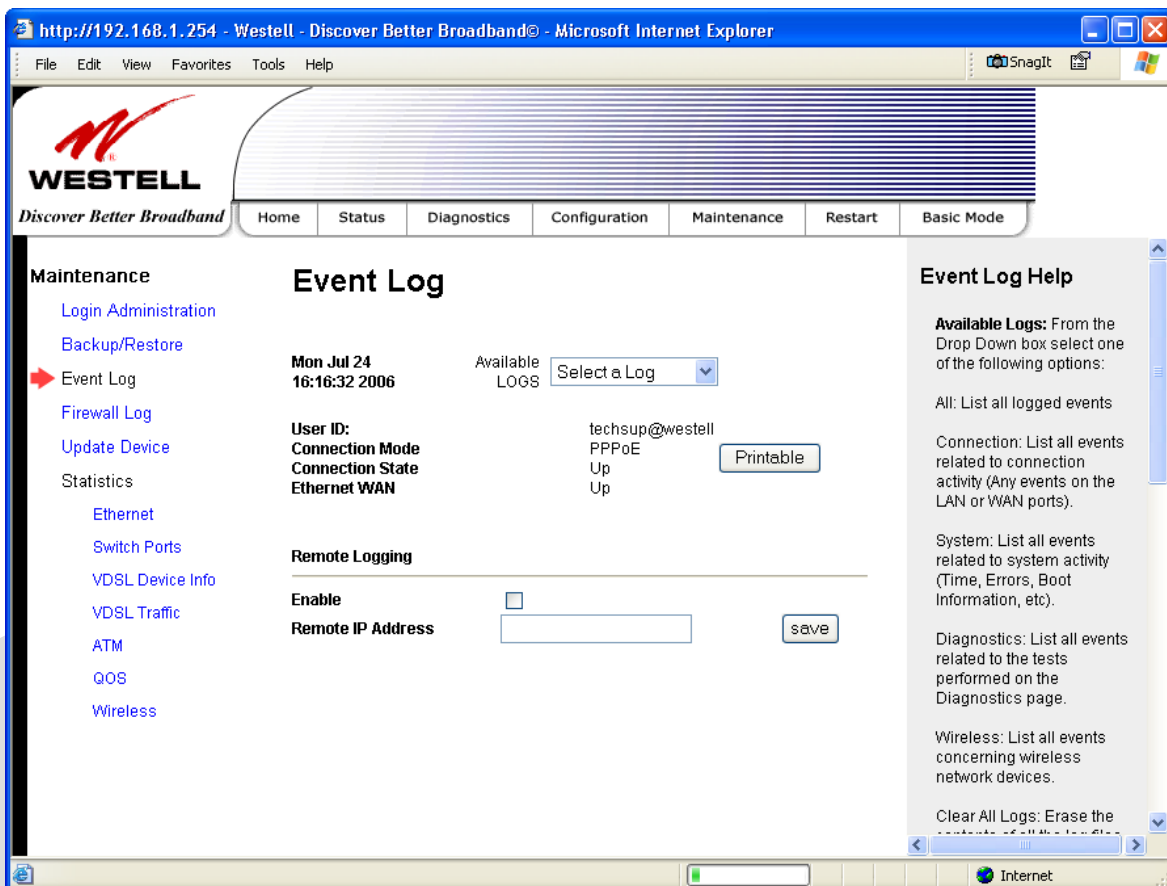
- Click **Backup** to back up the currently configured settings of your Gateway.
- Click **Restore** to allow the previously saved backup to override the Gateway's current settings.
- Click **Defaults** to erase the current configuration and to allow the factory default configuration to take effect. (If you restore the Gateway to factory default settings, all logged data in the Gateway will be lost.)

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



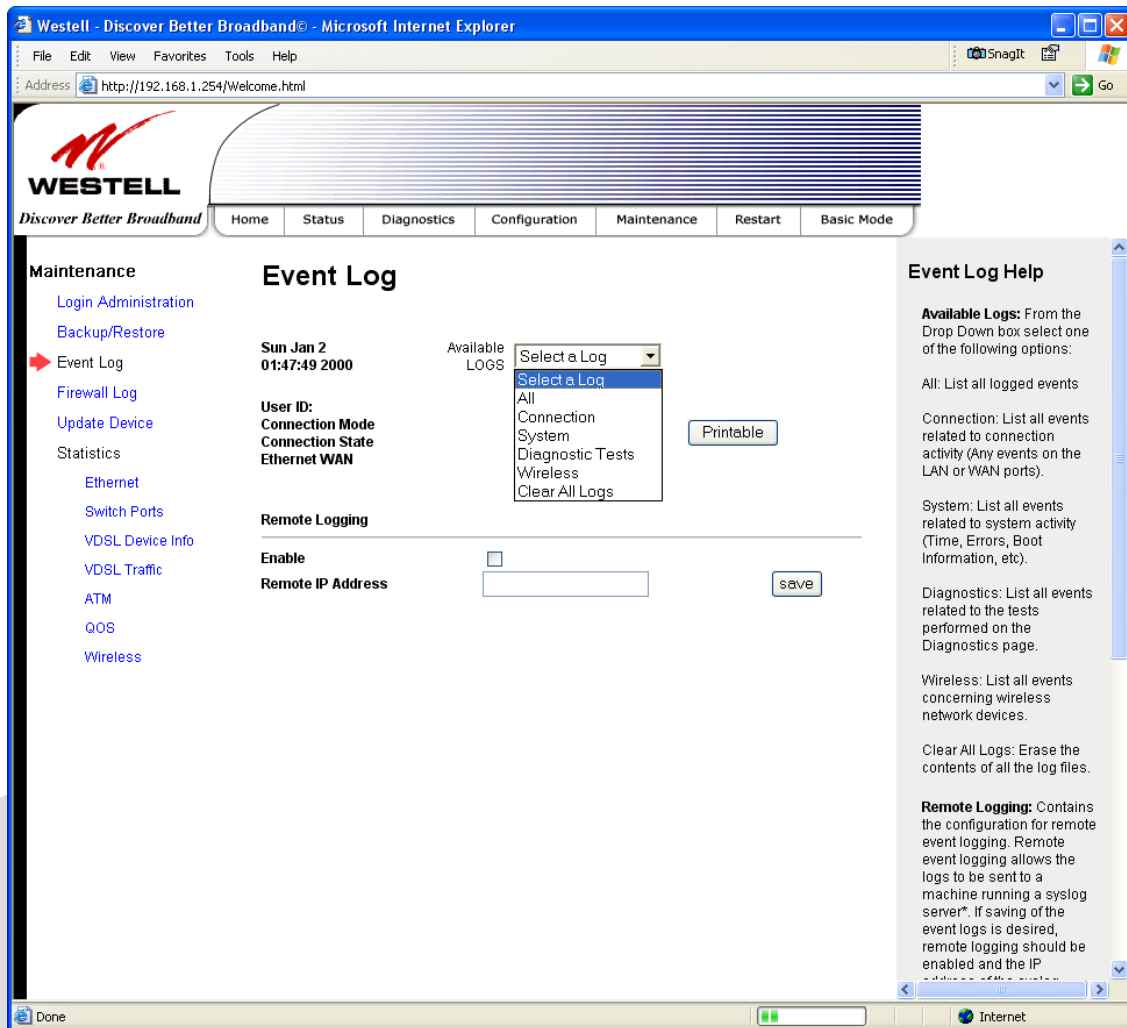
16.3 Event Log

The following screen will be displayed if you select **Maintenance > Event Log** from the menu options. The **Remote Logging** function enables event logs to be sent to a machine running a syslog server. To enable Remote Logging, click the box adjacent to **Enable** (a check mark will appear in the box). Then, enter an IP address in the **Remote IP Address** field, and click **Save** to save your settings.

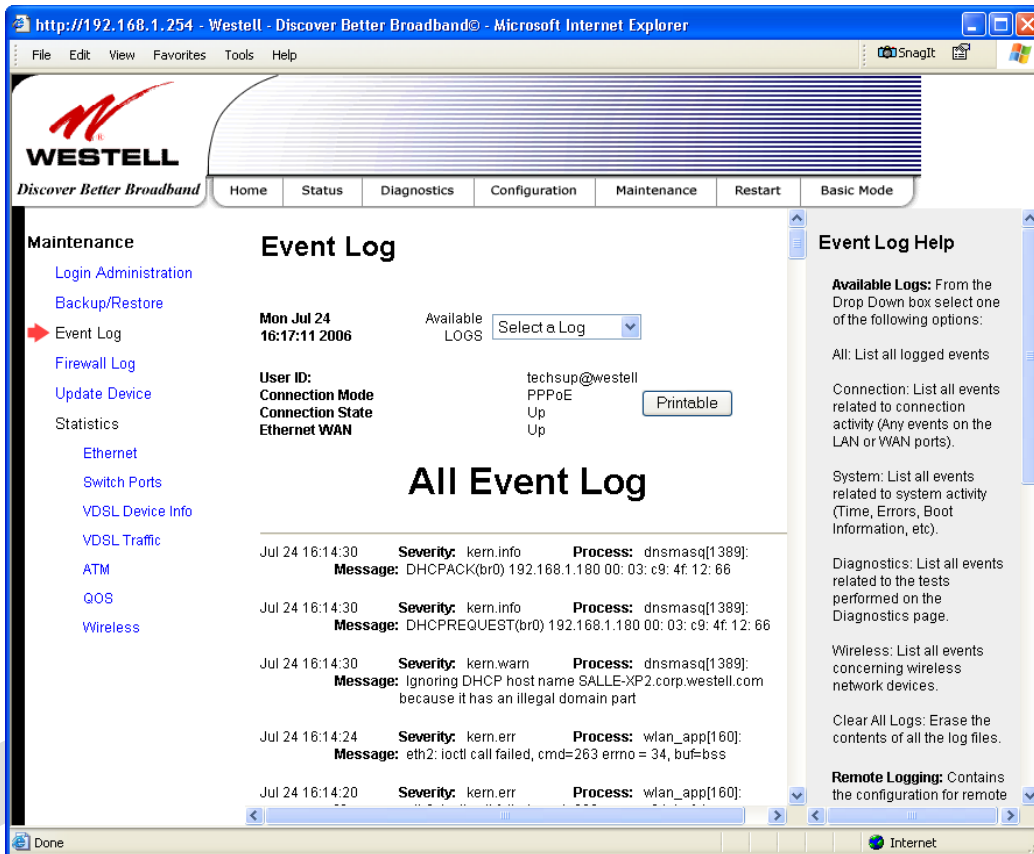


Event Log	
User ID	The name of your connection.
Connection Mode	The mode of connection used to connect to your ISP.
Connection State	The state of the PPP connection.
Ethernet WAN	The state of the Ethernet WAN connection.
Remote Logging	
Enable	Enables remote logging of Event Logs
Remote IP Address	The IP address of the syslog server machine on the local area network to which the Event Logs are sent.

To view logged events, select an option from the **Available LOGS** drop-down menu.



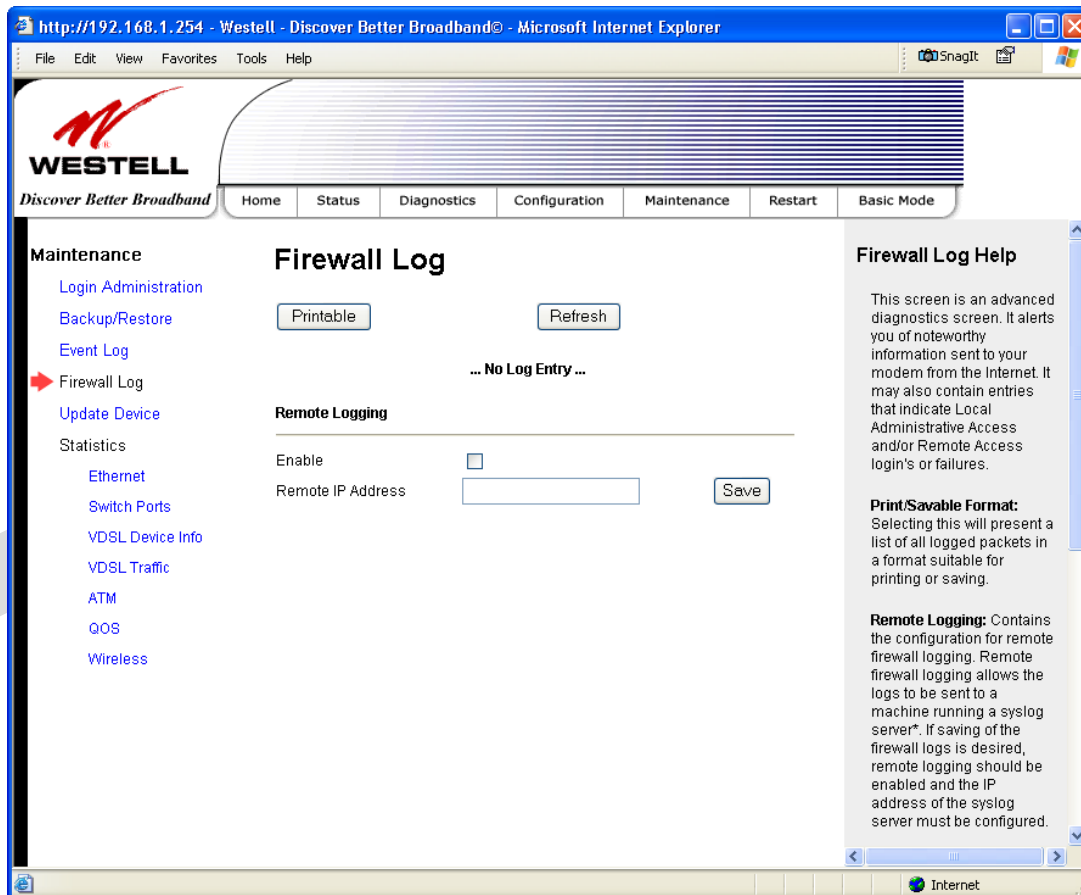
If you selected **All**, the following screen will be displayed. To obtain a printable version of the Event logs, click **Printable**.



16.4 Firewall Log

The following screen will be displayed if you select **Maintenance > Firewall Log** from the menu options.

- To enable Remote Logging, click the box adjacent to **Enable** (a check mark will appear in the box) and then enter an IP address in the **Remote IP Address** field. Click **Save** to save your settings.
- To obtain a printable version of the firewall logs, click **Printable**.
- Click **Refresh** to refresh the screen.



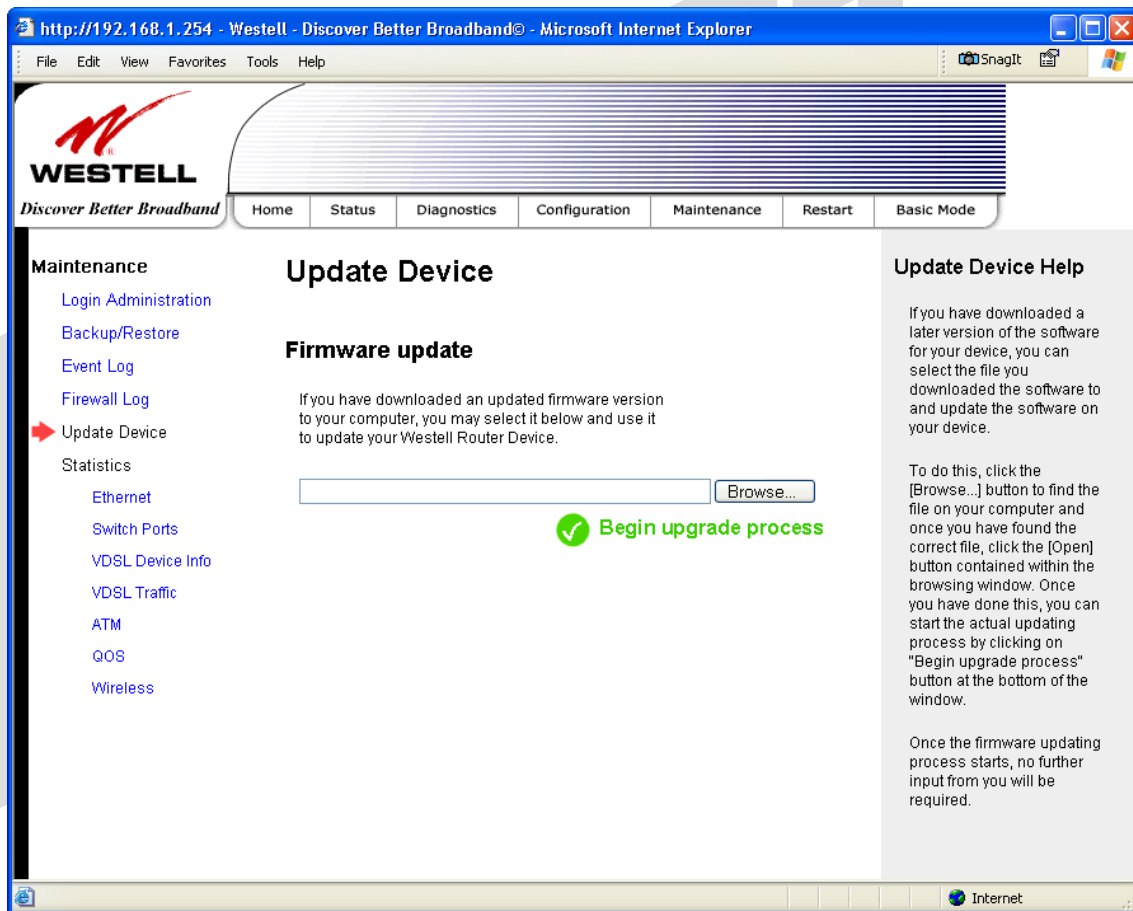
Remote Logging	
Enable	Factory Default = Disable If enabled (a check mark will appear in the box), the Gateway will send firewall logs to a syslog server.
Remote IP Address	The IP address of the syslog server machine to which the diagnostics logs to be sent.

16.5 Update Device

The following screen will be displayed if you select **Maintenance > Update Device** from the menu options. This screen enables you to update the software in your Gateway to the latest version supported.

To update your Gateway to the latest software version supported, do the following:

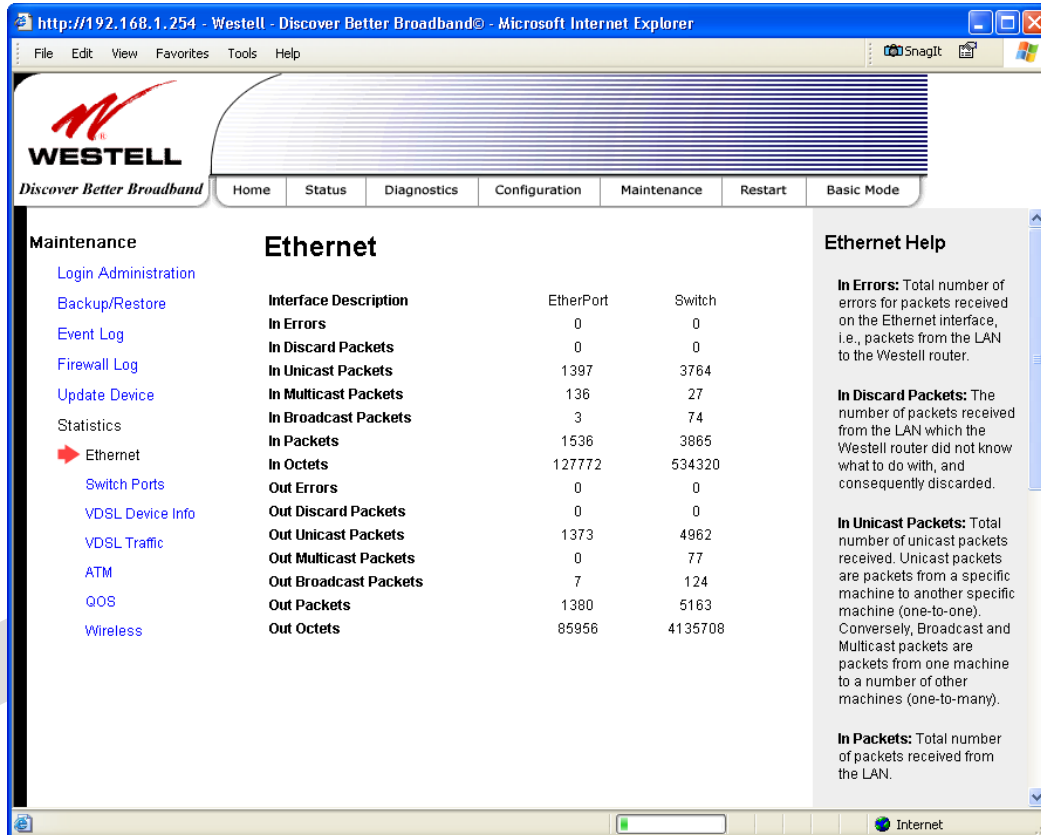
1. Download the update file and store it to a location on your PC.
2. Click the **Browse** button in the **Update Gateway** screen, and then navigate to the update file stored on your PC.
3. Click on the update file and then click **Open**. The path to the update file will appear in the **Browse** bar.
4. Click **Begin upgrade process** to begin the software update for your Gateway.
5. After your Gateway has been updated, wait a brief moment for the Gateway to reset and establish a WAN connection and a PPP session.
6. Confirm that the **WAN LED** on your Gateway is solid green before continuing your Gateway's configuration.



16.6 Statistics

16.6.1 Ethernet Statistics

The following screen will be displayed if you select **Maintenance > Statistics > Ethernet** from the menu options.



The screenshot shows the Westell web interface in Microsoft Internet Explorer. The browser address bar shows 'http://192.168.1.254 - Westell - Discover Better Broadband® - Microsoft Internet Explorer'. The page title is 'Discover Better Broadband'. The navigation menu includes Home, Status, Diagnostics, Configuration, Maintenance, Restart, and Basic Mode. The 'Maintenance' sidebar is expanded to show 'Ethernet' selected. The main content area displays 'Ethernet' statistics in a table format. The table has columns for 'Interface Description', 'EtherPort', and 'Switch'. The statistics are as follows:

Interface Description	EtherPort	Switch
In Errors	0	0
In Discard Packets	0	0
In Unicast Packets	1397	3764
In Multicast Packets	136	27
In Broadcast Packets	3	74
In Packets	1536	3865
In Octets	127772	534320
Out Errors	0	0
Out Discard Packets	0	0
Out Unicast Packets	1373	4962
Out Multicast Packets	0	77
Out Broadcast Packets	7	124
Out Packets	1380	5163
Out Octets	85956	4135708

On the right side of the interface, there is an 'Ethernet Help' section with the following text:

In Errors: Total number of errors for packets received on the Ethernet interface, i.e., packets from the LAN to the Westell router.

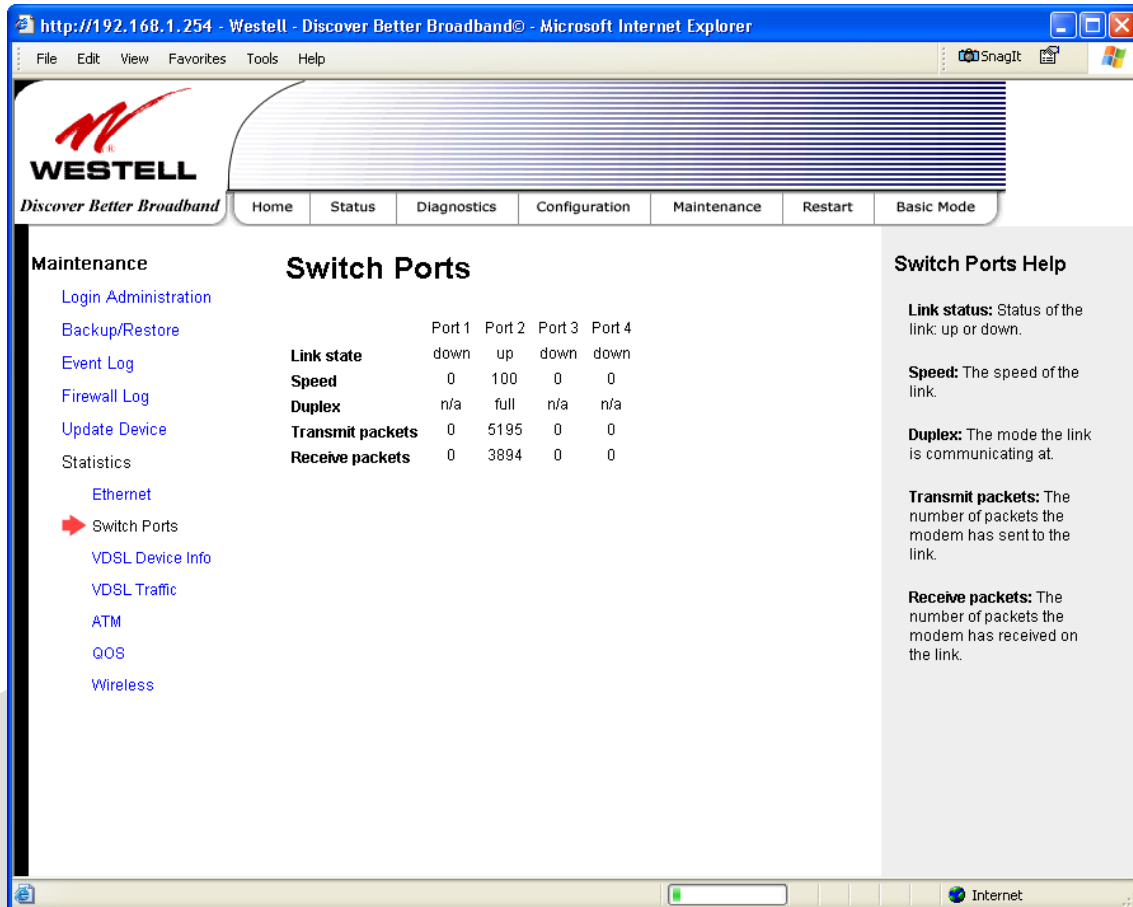
In Discard Packets: The number of packets received from the LAN which the Westell router did not know what to do with, and consequently discarded.

In Unicast Packets: Total number of unicast packets received. Unicast packets are packets from a specific machine (one-to-one). Conversely, Broadcast and Multicast packets are packets from one machine to a number of other machines (one-to-many).

In Packets: Total number of packets received from the LAN.

16.6.2 Switch Ports Statistics

The following screen will be displayed if you select **Maintenance > Statistics > Switch Ports** from the menu options.



The screenshot shows a web browser window displaying the Westell web interface. The browser address bar shows `http://192.168.1.254 - Westell - Discover Better Broadband© - Microsoft Internet Explorer`. The page title is "Discover Better Broadband". The navigation menu includes Home, Status, Diagnostics, Configuration, Maintenance, Restart, and Basic Mode. The "Maintenance" section is expanded, showing a list of options: Login Administration, Backup/Restore, Event Log, Firewall Log, Update Device, Statistics, Ethernet, Switch Ports (highlighted with a red arrow), VDSL Device Info, VDSL Traffic, ATM, QOS, and Wireless. The "Switch Ports" page displays a table of statistics for four ports:

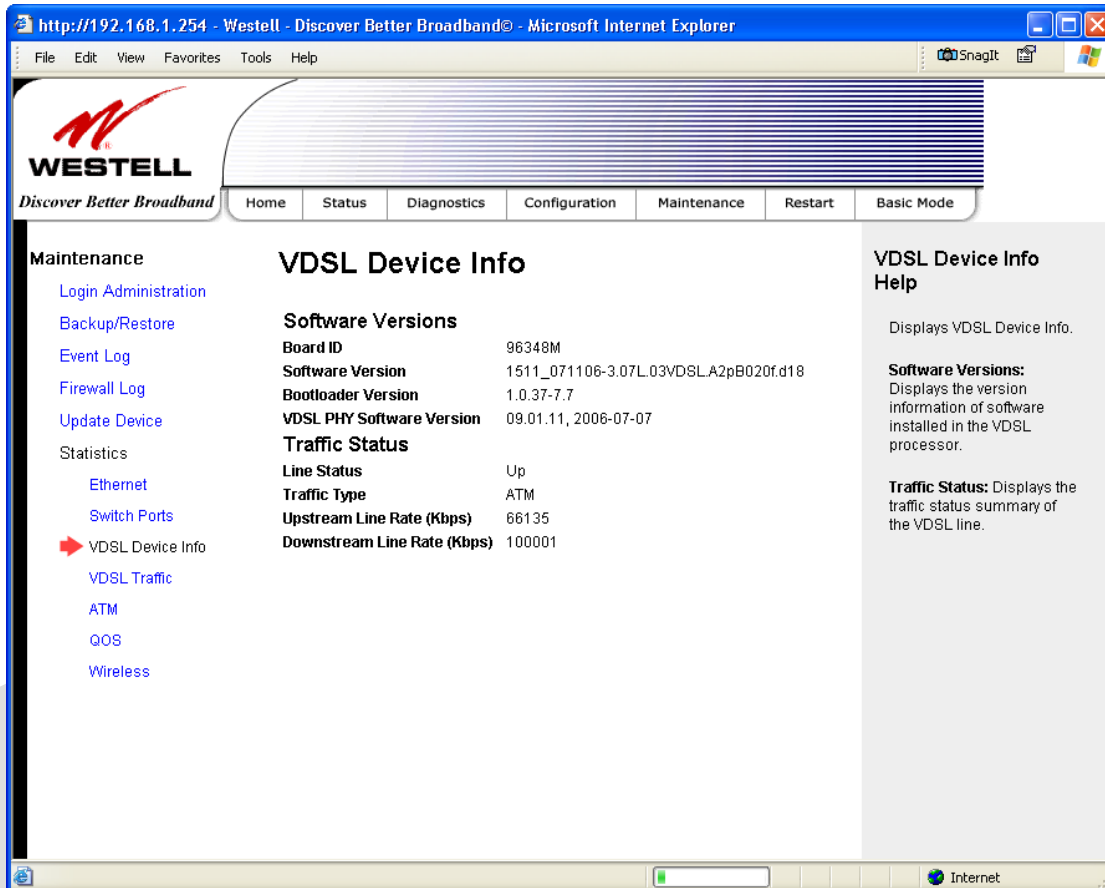
	Port 1	Port 2	Port 3	Port 4
Link state	down	up	down	down
Speed	0	100	0	0
Duplex	n/a	full	n/a	n/a
Transmit packets	0	5195	0	0
Receive packets	0	3894	0	0

To the right of the table is a "Switch Ports Help" section with the following definitions:

- Link status:** Status of the link: up or down.
- Speed:** The speed of the link.
- Duplex:** The mode the link is communicating at.
- Transmit packets:** The number of packets the modem has sent to the link.
- Receive packets:** The number of packets the modem has received on the link.

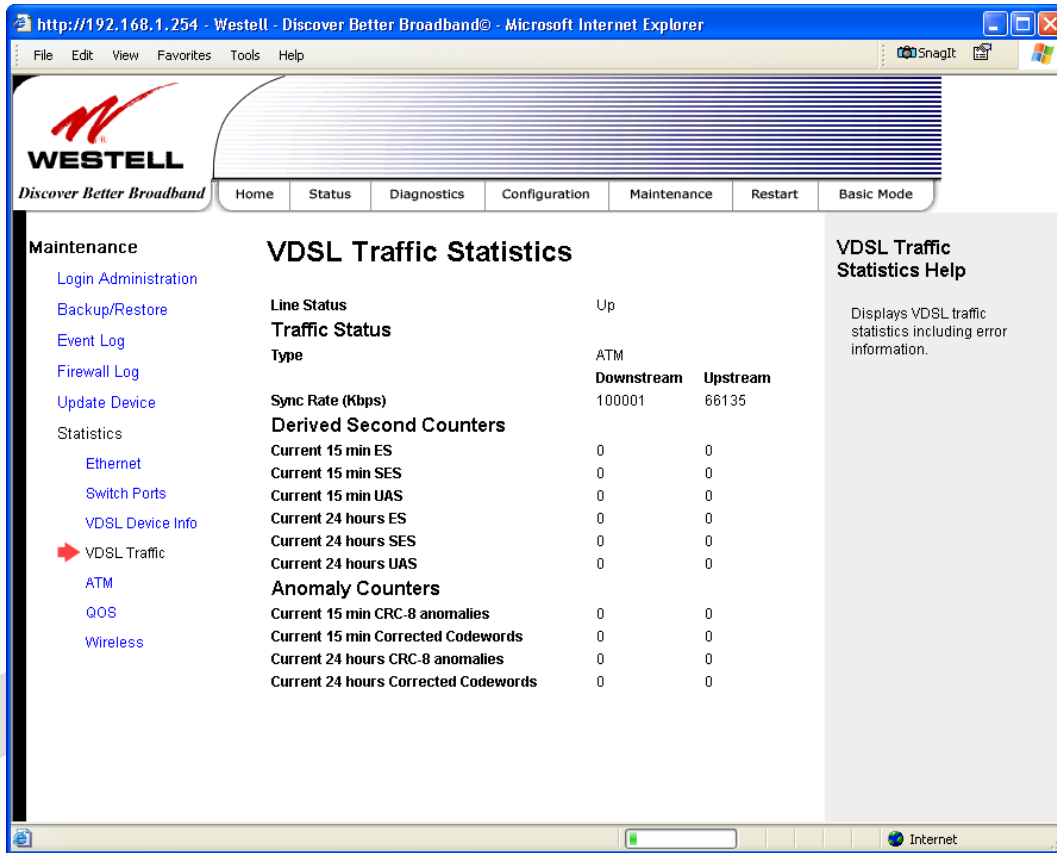
16.6.3 VDSL Device Info.

The following screen will be displayed if you select **Maintenance > Statistics > VDSL Device Info.** from the menu options.



16.6.4 VDSL Traffic Statistics

The following screen will be displayed if you select **Maintenance > Statistics > VDSL Traffic** from the menu options.



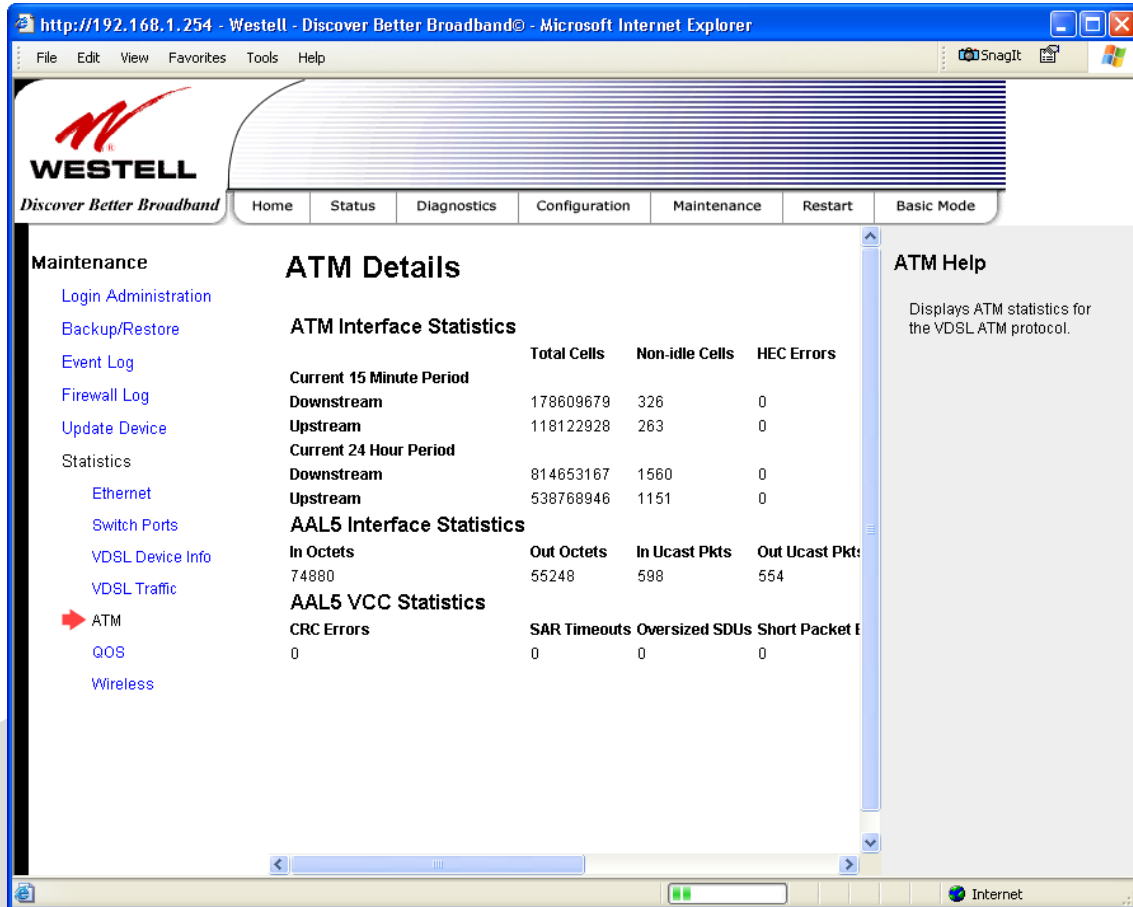
The screenshot shows a web browser window with the URL `http://192.168.1.254 - Westell - Discover Better Broadband® - Microsoft Internet Explorer`. The page title is "VDSL Traffic Statistics". The interface includes a navigation menu with options like Home, Status, Diagnostics, Configuration, Maintenance, Restart, and Basic Mode. The "Maintenance" menu is expanded, showing "VDSL Traffic" selected. The main content area displays the following statistics:

VDSL Traffic Statistics			
Line Status	Up		
Traffic Status	ATM		
Type	Downstream	Upstream	
Sync Rate (Kbps)	100001	66135	
Derived Second Counters			
Current 15 min ES	0	0	
Current 15 min SES	0	0	
Current 15 min UAS	0	0	
Current 24 hours ES	0	0	
Current 24 hours SES	0	0	
Current 24 hours UAS	0	0	
Anomaly Counters			
Current 15 min CRC-8 anomalies	0	0	
Current 15 min Corrected Codewords	0	0	
Current 24 hours CRC-8 anomalies	0	0	
Current 24 hours Corrected Codewords	0	0	

On the right side of the page, there is a "VDSL Traffic Statistics Help" section with the text: "Displays VDSL traffic statistics including error information."

16.6.5 ATM Statistics

The following screen will be displayed if you select **Maintenance > Statistics > ATM** from the menu options.



The screenshot shows a web browser window with the URL `http://192.168.1.254 - Westell - Discover Better Broadband® - Microsoft Internet Explorer`. The page features a navigation menu with options: Home, Status, Diagnostics, Configuration, Maintenance, Restart, and Basic Mode. The 'Maintenance' section is expanded, showing a list of options including Login Administration, Backup/Restore, Event Log, Firewall Log, Update Device, Statistics, Ethernet, Switch Ports, VDSL Device Info, VDSL Traffic, **ATM** (highlighted with a red arrow), QOS, and Wireless.

ATM Details

ATM Interface Statistics

	Total Cells	Non-idle Cells	HEC Errors
Current 15 Minute Period			
Downstream	178609679	326	0
Upstream	118122928	263	0
Current 24 Hour Period			
Downstream	814653167	1560	0
Upstream	538768946	1151	0

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts
74880	55248	598	554

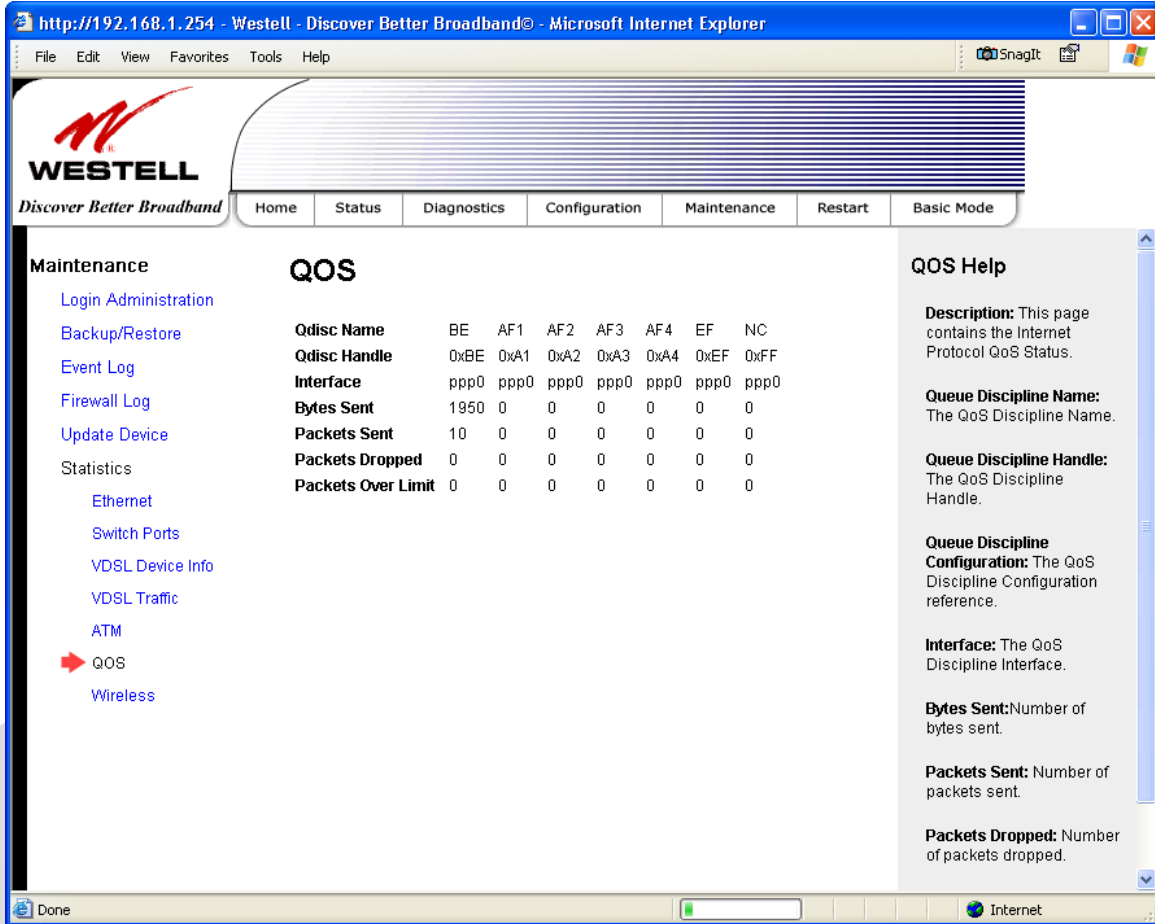
AAL5 VCC Statistics

CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet E
0	0	0	0

ATM Help
Displays ATM statistics for the VDSL ATM protocol.

16.6.6 QOS Statistics

The following screen will be displayed if you select **Maintenance > Statistics > QOS** from the menu options.



The screenshot shows a web browser window displaying the Westell management interface. The main content area is titled "QOS" and contains a table with the following data:

Qdisc Name	BE	AF1	AF2	AF3	AF4	EF	NC
Qdisc Handle	0xBE	0xA1	0xA2	0xA3	0xA4	0xEF	0xFF
Interface	ppp0	ppp0	ppp0	ppp0	ppp0	ppp0	ppp0
Bytes Sent	1950	0	0	0	0	0	0
Packets Sent	10	0	0	0	0	0	0
Packets Dropped	0	0	0	0	0	0	0
Packets Over Limit	0	0	0	0	0	0	0

To the right of the table is a "QOS Help" section with the following text:

Description: This page contains the Internet Protocol QoS Status.

Queue Discipline Name: The QoS Discipline Name.

Queue Discipline Handle: The QoS Discipline Handle.

Queue Discipline Configuration: The QoS Discipline Configuration reference.

Interface: The QoS Discipline Interface.

Bytes Sent: Number of bytes sent.

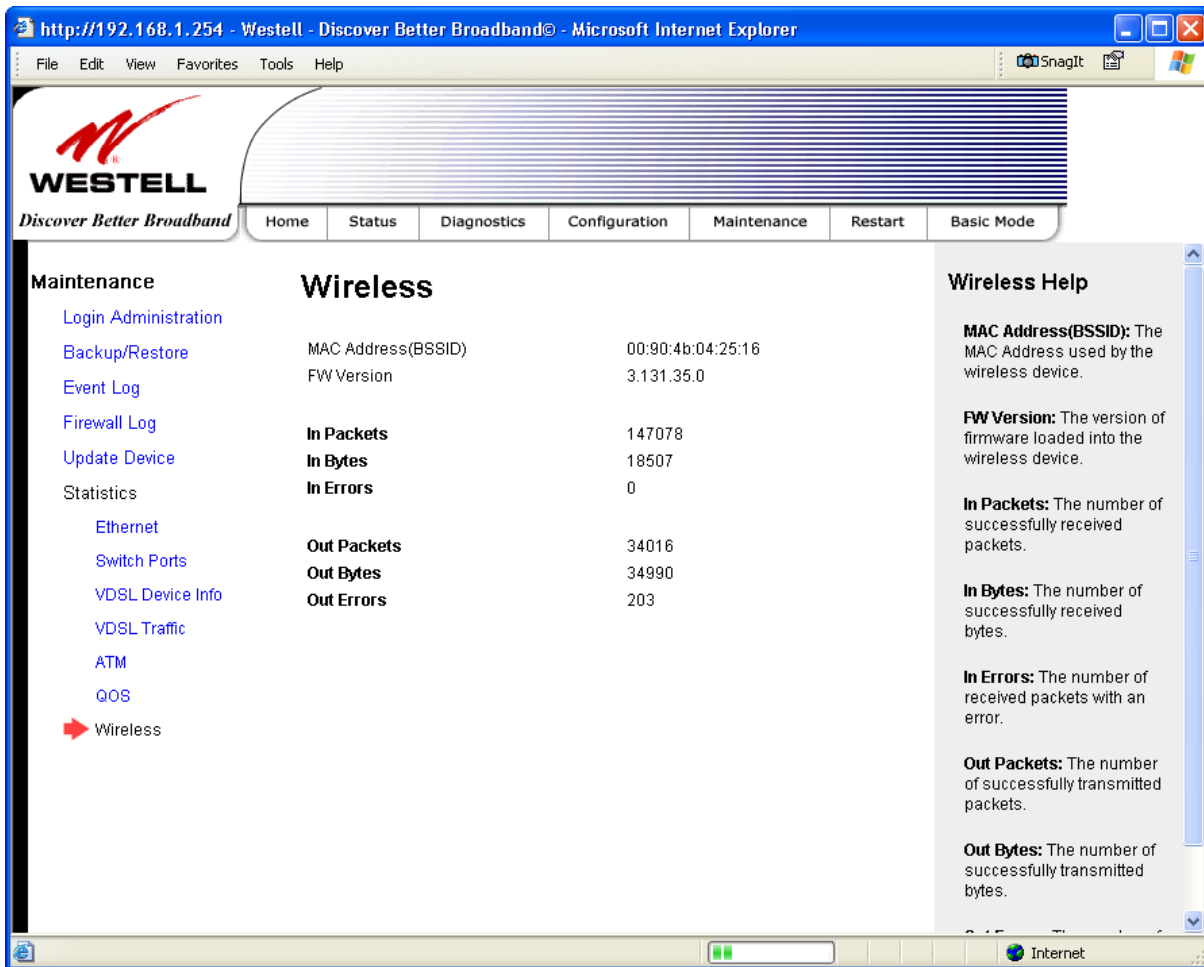
Packets Sent: Number of packets sent.

Packets Dropped: Number of packets dropped.

16.6.7 Wireless Statistics

The following screen will be displayed if you select **Maintenance > Statistics > Wireless** from the menu options.

NOTE: The fields in this screen will be blank if no stations are associated with the Gateway.



The screenshot shows a web browser window with the URL `http://192.168.1.254 - Westell - Discover Better Broadband® - Microsoft Internet Explorer`. The page features the Westell logo and a navigation menu with tabs: Home, Status, Diagnostics, Configuration, Maintenance, Restart, and Basic Mode. The 'Maintenance' tab is active, and the 'Wireless' sub-tab is selected. The main content area is titled 'Wireless' and displays the following statistics:

MAC Address(BSSID)	00:90:4b:04:25:16
FW Version	3.131.35.0
In Packets	147078
In Bytes	18507
In Errors	0
Out Packets	34016
Out Bytes	34990
Out Errors	203

The 'Wireless Help' sidebar on the right provides definitions for these terms:

- MAC Address(BSSID):** The MAC Address used by the wireless device.
- FW Version:** The version of firmware loaded into the wireless device.
- In Packets:** The number of successfully received packets.
- In Bytes:** The number of successfully received bytes.
- In Errors:** The number of received packets with an error.
- Out Packets:** The number of successfully transmitted packets.
- Out Bytes:** The number of successfully transmitted bytes.

17. NAT SERVICES

For your convenience, the Gateway supports protocols for Applications, Games, and VPN-specific programs. The following chart provides protocol information for the services supported by the Gateway.

NOTE: To configure the Gateway for a service or application, follow the steps in section 15.2, “Port Forwarding Configuration.”

Applications/Games/VPN Support	
Application/Game	Port/Protocol
Aliens vs. Predator	80 UDP, 2300 UDP, 8000-8999 UDP
Age of Empires II: The Conquerors	6073 UDP, 47624 TCP, 2300-2400 TCP/UDP This service will open up ports for both traffic directions.
Americas Army	TCP – 20045 UDP – 1716 to 1718, 8777, 27900
America Online	5190 TCP/UDP
Anarchy Online	TCP/UDP – 7012,7013, 7500 -7505
AOL Instant Messenger	4099 TCP, 5190 TCP
Asheron's Call	9000-9013 UDP, 28800-29000 TCP
Battlecom	2300-2400 TCP/UDP, 47624 TCP/UDP
Battlefield 1942	UDP - 14567, 22000, 23000 to 23009, 27900, 28900
Black and White	2611-2612 TCP, 6667 TCP, 6500 UDP, 27900 UDP
Blizzard Battle.net (Diablo II)	4000 TCP, 6112 TCP/UDP
Buddy Phone	700, 701 UDP
Bungie.net, Myth, Myth II Server	3453 TCP
Calista IP Phone	3000 UDP, 5190 TCP
Citrix Metaframe	1494 TCP
Client POP/IMAP	110 TCP
Client SMTP	25 TCP
Counter Strike	27015 TCP/UDP, 27016 TCP/UDP
Dark Reign 2	26214 TCP/UDP
Delta Force (Client and Server)	3568 UDP, 3100-3999 TCP/UDP
Delta Force 2	3568-3569 UDP
DeltaForce: Land Warrior	UDP 53 TCP 21 TCP 7430 TCP 80 UDP 1029 UDP 1144 UDP 65436 UDP 17478
DNS	53 UDP
Elite Force	2600 UDP, 27500 UDP, 27910 UDP, 27960 UDP
Everquest	1024-7000 TCP/UDP
F-16, Mig 29	3863 UDP
F-22 Lightning 3	4660-4670 TCP/UDP, 3875 UDP, 4533-4534 UDP, 4660-4670 UDP
F-22 Raptor	3874-3875 UDP
Fighter Ace II	50000-50100 TCP/UDP
Fighter Ace II for DX play	50000-50100 TCP/UDP, 47624 TCP, 2300-2400 TCP/UDP
FTP	20 TCP, 21 TCP
GameSpy Online	UDP 3783 UDP 6515

	TCP 6667 UDP 12203 TCP/UDP 13139 UDP 27900 UDP 28900 UDP 29900 UDP 29901
Ghost Recon	TCP 80 UDP 1038 UDP 1032 UDP 53 UDP 2347 UDP 2346
GNUTella	6346 TCP/UDP, 1214 TCP
Half Life Server	27005 UDP(client only) 27015 UDP
Heretic II Server	28910 TCP
Hexen II	26900 (+1) each player needs their own port. Increment by one for each person.
Hotline Server	5500, 5503 TCP 5499 UDP
HTTPS	443 TCP/UDP
ICMP Echo	4 ICMP
ICQ OLD	4000 UDP, 20000-20019 TCP
ICQ 2001b	4099 TCP, 5190 TCP
ICUII Client	2000-2038 TCP, 2050-2051 TCP, 2069 TCP, 2085 TCP, 3010-3030 TCP
ICUII Client Version 4.xx	1024-5000 TCP, 2050-2051 TCP, 2069 TCP, 2085 TCP, 3010-3030 TCP, 2000-2038 TCP, 6700-6702 TCP, 6880 TCP, 1200-16090 TCP
IMAP	119 TCP/UDP
IMAP v.3	220 TCP/UDP
Internet Phone	22555 UDP
IPSEC ALG	IPSEC ALG
IPSEC ESP	PROTOCOL 50
IPSEC IKE	500 UDP
Ivisit	9943 UDP, 56768 UDP
JKII:JO (Jedi Knight II: Jedi Outcast)	UDP - 28070 (default) UDP- 27000 to 29000
KALI, Doom & Doom II	2213 UDP, 6666 UDP (EACH PC USING KALI MUST USE A DIFFERENT PORT NUMBER STARTING WITH 2213 + 1)
KaZaA	1214 TCP/UDP
Limewire	6346 TCP/UDP, 1214 TCP
Medal Of Honor: Allied Assault	TCP 80 UDP 53 UDP 2093 UDP 12201 TCP 12300 UDP 2135 UDP 2139 TCP/UDP 28900
mIRC Chat	6660-6669 TCP
Motorhead Server	16000 TCP/UDP, 16010-16030 TCP/UDP
MSN Game Zone	6667 TCP, 28800-29000 TCP
MSN Game Zone (DX 7 & 8 play)	6667 TCP, 6073 TCP, 28800-29000 TCP, 47624 TCP, 2300-2400 TCP/UDP This service will open up ports for both traffic directions.

MSN Messenger	6891-6900 TCP, 1863 TCP/UDP, 5190 UDP, 6901 TCP/UDP
Napster	6699 TCP
Need for Speed 3, Hot Pursuit	1030 TCP
Need for Speed, Porsche	9442 UDP
Net2Phone	6801 UDP
NNTP	119 TCP/UDP
Operation FlashPoint	47624 UDP, 6073 UDP, 2300-2400 TCP/UDP, 2234 TCP
Outlaws	5310 TCP/UDP
Pal Talk	2090-2091 TCP/UDP, 2095 TCP, 5001 TCP, 8200-8700 TCP/UDP, 1025-2500 UDP
pcAnywhere host	5631 TCP, 5632 UDP, 22 UDP
Phone Free	1034-1035 TCP/UDP, 9900-9901 UDP, 2644 TCP, 8000 TCP
Quake 2	27910 UDP
Quake 3	27660 UDP Each computer playing QuakeIII must use a different port number, starting at 27660 and incrementing by 1. You'll also need to do the following: 1. Right click on the QIII icon 2. Choose "Properties" 3. In the Target field you'll see a line like "C:\Program Files\Quake III Arena\quake3.exe" 4. Add the Quake III net_port command to specify a unique communication port for each system. The complete field should look like this: "C:\Program Files\Quake III Arena\quake3.exe" +set net_port 27660 5. Click OK. 6. Repeat for each system behind the NAT, adding one to the net_port selected (27660,27661,27662)
Quicktime 4/Real Audio	6970-32000 UDP, 554 TCP/UDP
Rainbow Six & Rogue Spear	2346 TCP
RealOne Player	TCP - 554, 7070 to 7071 UDP - 6970 to 7170
Real Audio	6970-7170 UDP
Return To Castle Wolfenstein	Default -27960 TCP/UDP UDP - 27950 to 27980
Roger Wilco	TCP/UDP 3782 UDP 3783 (BaseStation)
SIP ALG	SIP ALG
ShoutCast Server	8000-8005 TCP
Spinner Radio/Netscape Music	TCP - 554
SSH Secure Shell	22 TCP/UDP
Starcraft	2346 TCP
Starfleet Command	2300-2400 TCP/UDP, 47624 TCP/UDP
SOF/SOFII (Soldier of Fortune / Soldier of Fortune II)	UDP - 28910 to 28915
Telnet	23 TCP
Tiberian Sun & Dune 2000	1140-1234, 4000 TCP/UDP
Tribes2	TCP - 15104, 15204, 15206, 6660 to 6699 UDP - 27999 to 28002
Ultima Online	5001-5010 TCP, 7775-7777 TCP, 8800-8900 TCP, 9999 UDP, 7875 UDP
Unreal Tournament server	7777 (default gameplay port) 7778 (server query port) 7779,7779+ are allocated dynamically for each helper UdpLink

	objects, including UdpServerUplink objects. Try starting with 7779-7781 and add ports if needed. 27900 server query, if master server uplink is enabled. Home master servers use other ports like 27500. Port 8080 is for UT Server Admin. In the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 and ServerName to the IP assigned to the router from your ISP.
USENET News Service	143 TCP
VNC, Virtual Network Computing	5500 TCP, 5800 TCP, 5900 TCP
Westwood Online, C&C	4000 TCP/UDP, 1140-1234 TCP/UDP
World Wide Web (HTTP)	80 TCP 443 TCP (SSL) 8008 or 8080 TCP (PROXY)
Yahoo Messenger Chat	5000-5001 TCP
Yahoo Messenger Phone	5055 UDP
Xbox Live	88 TCP/UDP, 3074 TCP/UDP
NAT/VPN Support	
IPSec Encryption	IPSec using AH can not be supported through NAT. IPSec using ESP and L2TP can be supported via an ALG
L2TP	IPSec using ESP and L2TP can be supported via an ALG.
PPTP	Works through NAT.

18. PRODUCT SPECIFICATIONS

Product Features

Data Features

- Network Address Port Translation
- DHCP client/server
- DNS server/relay
- Static Routes
- PPTP/L2TP/IPSEC VPN NAPT passthrough
- NAT ALG support for common applications
- Stateful Inspection Firewall with logging
- Diffserv IP QOS

WAN Protocol Features

PPPoE

- Bridge Encapsulation per RFC 1483
- PPP over Ethernet per RFC 2516
- PAP/CHAP PPP per RFC 1334,1994
- PPPoE Tunneling

Routed IP

- IP over Ethernet framing and RAS discovery per RFC894
- Static WAN IP assignment or WAN DHCP

Public LAN Features

- DHCP server
- Bridge mode mapped to a separate PVC

VDSL WAN

- RJ-11 connector

Ethernet LAN

- Four port 10/100 Base-T Ethernet switch
- Auto-sense ports MDI/MDI-X detection

Wireless LAN

- IEEE 802.11b/g with frame bursting
- WEP and WPA-PSK security
- MAC address filtering
- Upgradeable to 802.11i, 802.11e, WME
- High gain removable external antenna

Management

- Web-based GUI

System Requirements

Ethernet

- Pentium® or equivalent and above machines
- Operating System:

- Microsoft Windows 98 SE or
- Microsoft Windows ME or
- Microsoft Windows 2000 (all versions and service packet levels) or
- Microsoft Windows XP (all versions and service packet levels) or
- Microsoft Server 2003 (all versions and service packet levels) or
- Macintosh OS X 10.1 or later or
- Linux installed
- Internet Explorer 5.x or later, Netscape 7.x or later. Browsers must use HTTP 1.1 or later
- Operating System CD on hand
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Ethernet 10/100 Base-T Network Interface Card (NIC)

Wireless

- Pentium® or equivalent and above class machines
- Operating System:
 - Microsoft Windows 98 SE or
 - Microsoft Windows ME or
 - Microsoft Windows 2000 (all versions and service packet levels) or
 - Microsoft Windows XP (all versions and service packet levels) or
 - Microsoft Server 2003 (all versions and service packet levels) or
 - Macintosh OS X 10.1 or later or
 - Linux installed
- Internet Explorer 5.x or later, Netscape 7.x or later. Browsers must use HTTP 1.1 or later
- Operating System CD on hand
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- IEEE 802.11b/g PC adapter

Physical/Environmental Specifications

Dimensions/Weight

- Height: 1.5 in (3.81 cm)
- Width: 10.0 in (25.4 cm)
- Depth: 6.50 in (16.5 cm)
- Weight: Approx. 1.26 lbs. (0.57 kg)

Environmental

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

Network Interface

- WAN: VDSL RJ-11 port
- LAN: 10/100 Base-T RJ-45 port (to PC or Hub)
- Wireless: SMA Antenna

Power

- Power Adapter:
 - Input: AC 120V/
 - Output: DC +12V
- Power Consumption: Less than 14W typical from 120 VAC

LED Indicators

- Power
- Ethernet
- Wireless
- VDSL
- Internet

Connectors

- VDSL: RJ-11
- Four Ethernet: RJ-45
- Power: Barrel connector
- Two Wireless IEEE 802.11b/g SMA connectors with antennas

Compliance

EMC

- FCC Part 15 Class B

Safety

- ANSI/UL 60950-1
- CAN/CSA C22.2 No. 60950-1 First Edition dated April 1, 2003 with revisions through November 26, 2003

Regulatory Approval

- UL, CSA, FCC Part 68, ACTA 968-A-3 Industry Canada CS03

DRAFT

19. TECHNICAL SUPPORT INFORMATION

Westell Technical Support

If technical assistance is required, contact your Internet service provider for support. By using one of the following options:

North America
Phone: 1-630-375-4500

U.K./Europe
Phone: (44) 01256 843311

Visit Westell at www.Westell.com to view frequently asked questions and enter on-line service requests, or send email to global_support@westell.com to obtain additional information.

20. WARRANTY AND REPAIRS

Warranty

Westell warrants this product free from defects at the time of shipment. Westell also warrants this product fully functional for the period specified by the terms of the warranty. Any attempt to repair or modify the equipment by anyone other than an authorized representative will void the warranty.

Repairs

Westell will repair any defective Westell equipment without cost during the warranty period if the unit is defective for any reason other than abuse, improper use, or improper installation, or acts of nature. Before returning the defective equipment, request a **Return Material Authorization (RMA)** number from Westell. An RMA number must be quoted on all returns. When requesting an RMA, please provide the following information:

- Product model number (on product base)
- Product serial number (on product base)
- Customer ship-to address
- Contact name
- Problem description
- Purchase date

After an RMA number is obtained, return the defective unit, freight prepaid, along with a brief description of the problem to one of the following options:

North America
Westell, Inc.
ATTN: R.G.M Department
750 N. Commons Drive
Aurora, IL 60504-7940 USA

U.K./Europe
Westell, Ltd.
Ringway House
Bell Road
Daneshill
Basingstoke
RG24 8FB
United Kingdom

Westell will continue to repair faulty equipment beyond the warranty period for a nominal charge. Contact a Westell Technical Support Representative for details.



21. PUBLICATION INFORMATION

Westell® UltraLine II VDSL (Model 826010)
User Guide Part Number 030-300237 Rev. A

Copyright © 2006 Westell, Inc.
All rights reserved.

Westell, Inc.
750 North Commons Drive
Aurora, Illinois 60504 USA
www.westell.com

All trademarks and registered trademarks are the property of their respective owners.

DRAFT 1