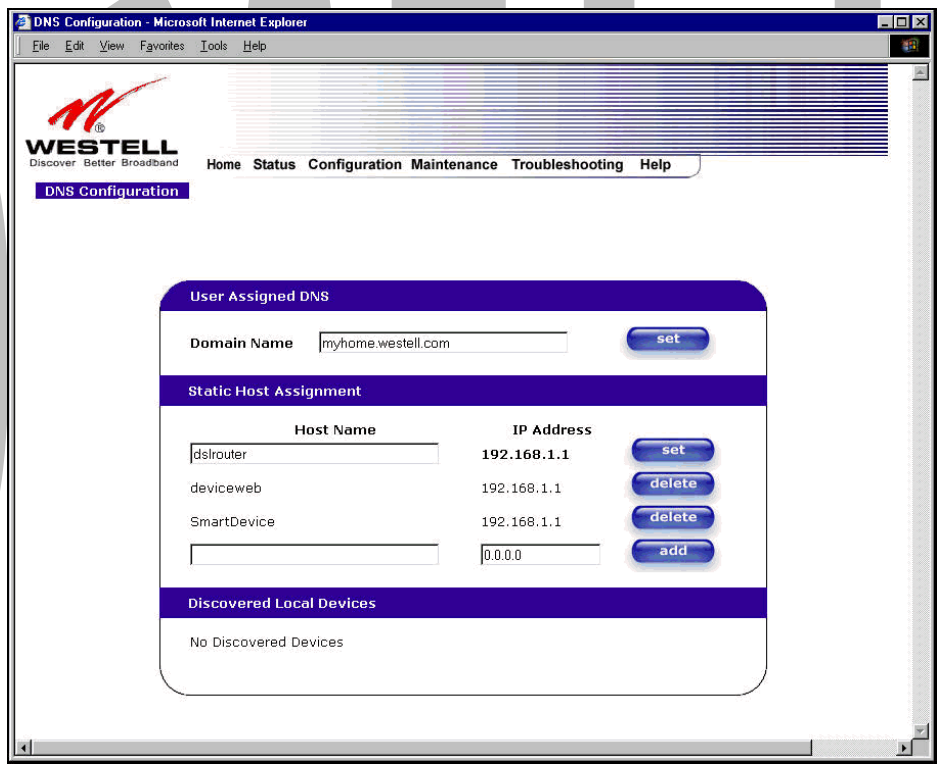
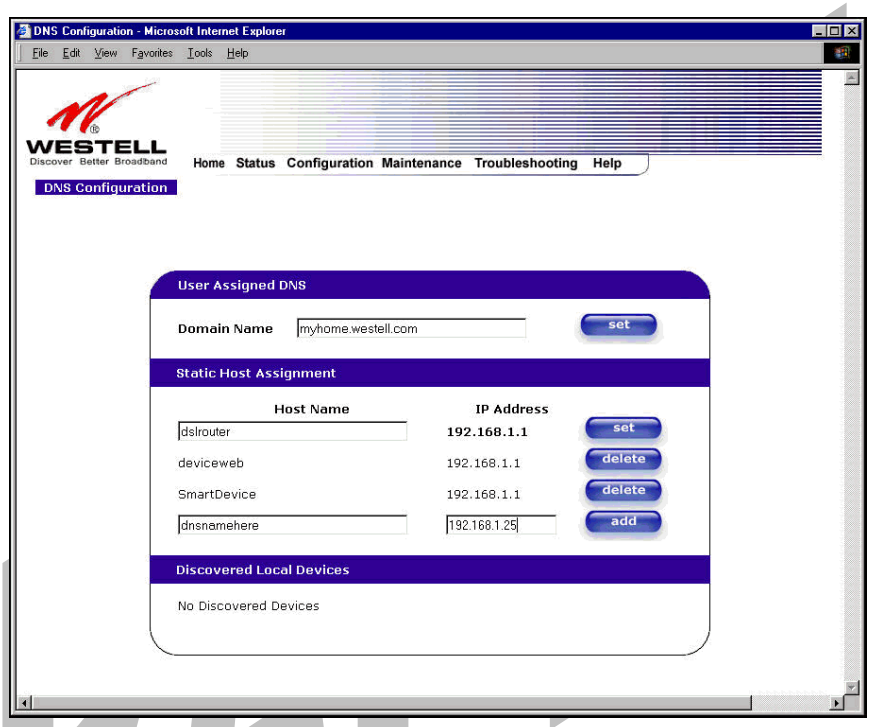
require the name for identification purposes.	new domain name and click **Set.**
Static Host Assignment	
Host Name	This field allows you to enter a HOST name for the Media Gateway. To add a new Host name, in the field under Static Host Assignment, type in the Host Name and the IP address and click **Set.**
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 Gateway's **Host Name** and **IP Address** in the fields provided in the **Static Host Assignment** section.



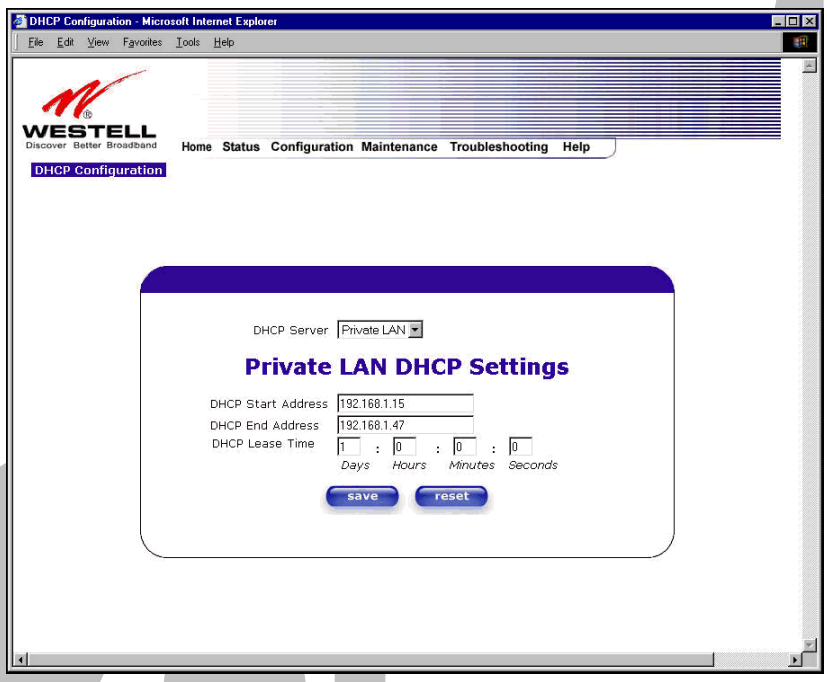
The following screen displays a **Host Name** and an **IP Address** in the fields. Now click on **add.**



If you clicked on **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 **DHCP** from the **Advanced LAN** menu.



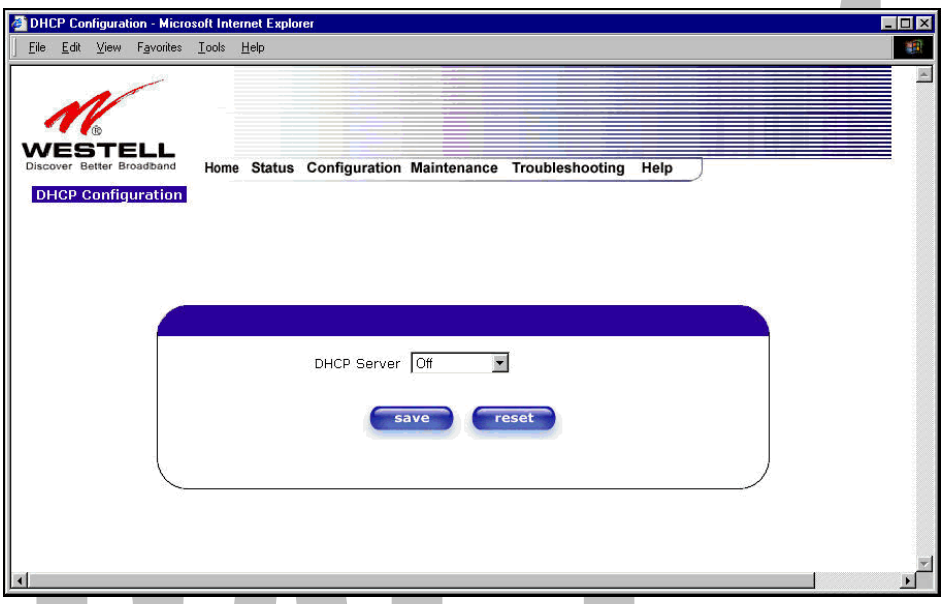
DHCP Server	This setting allows Media Gateway to automatically assign IP addresses to local devices connected on the LAN. Westell advises setting this to enabled for the private LAN. Off = DHCP Server is disabled Private LAN = DHCP addresses will be saved into the Private LAN configuration. Public LAN = 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 your ISP 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)

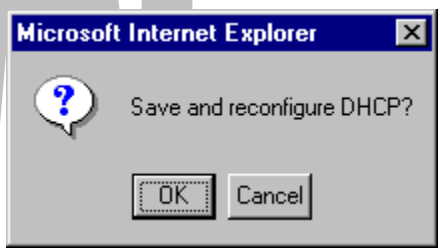
13.5.3 Disabling the DHCP Server

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 on **OK.**

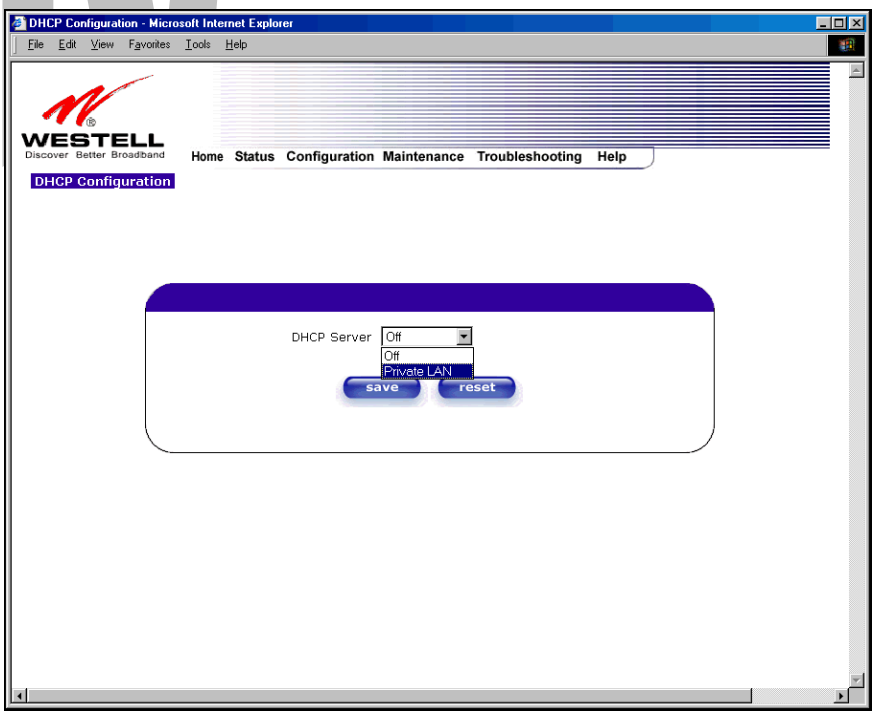


STOP: After you disable the DHCP server, you must reboot your PC

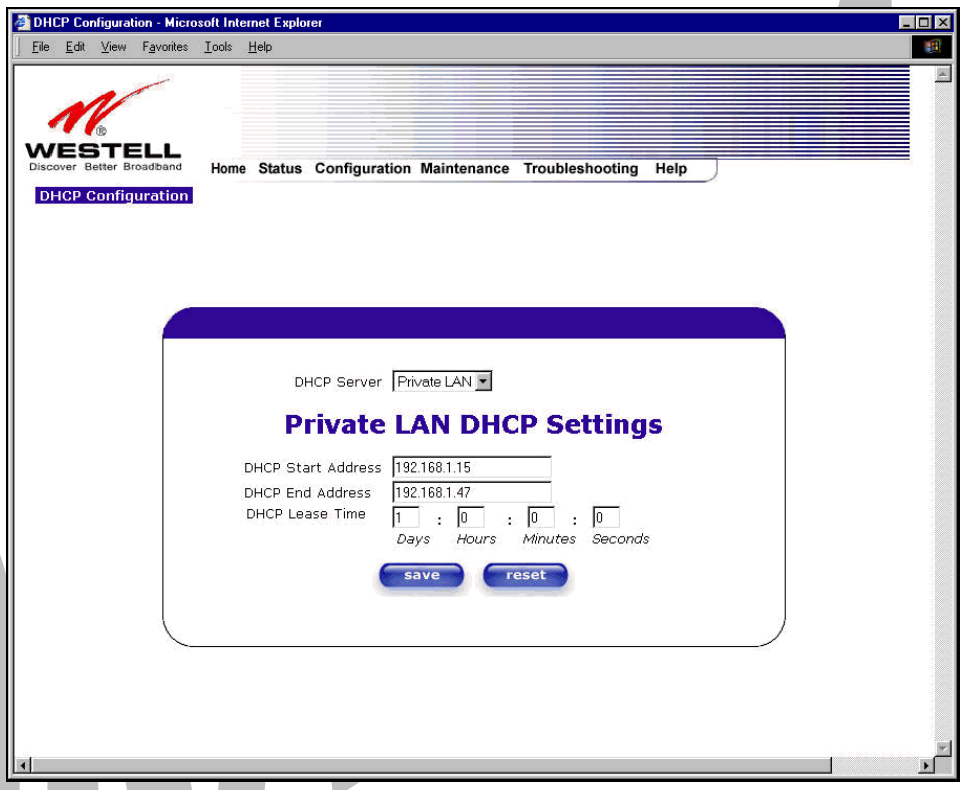
13.5.4 Enabling the DHCP Server

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

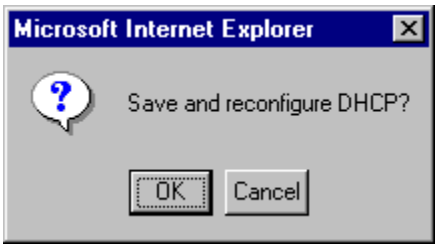
If you have recently disabled the DHCP Server for Private LAN, select **Private LAN** while in the following screen.



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.**



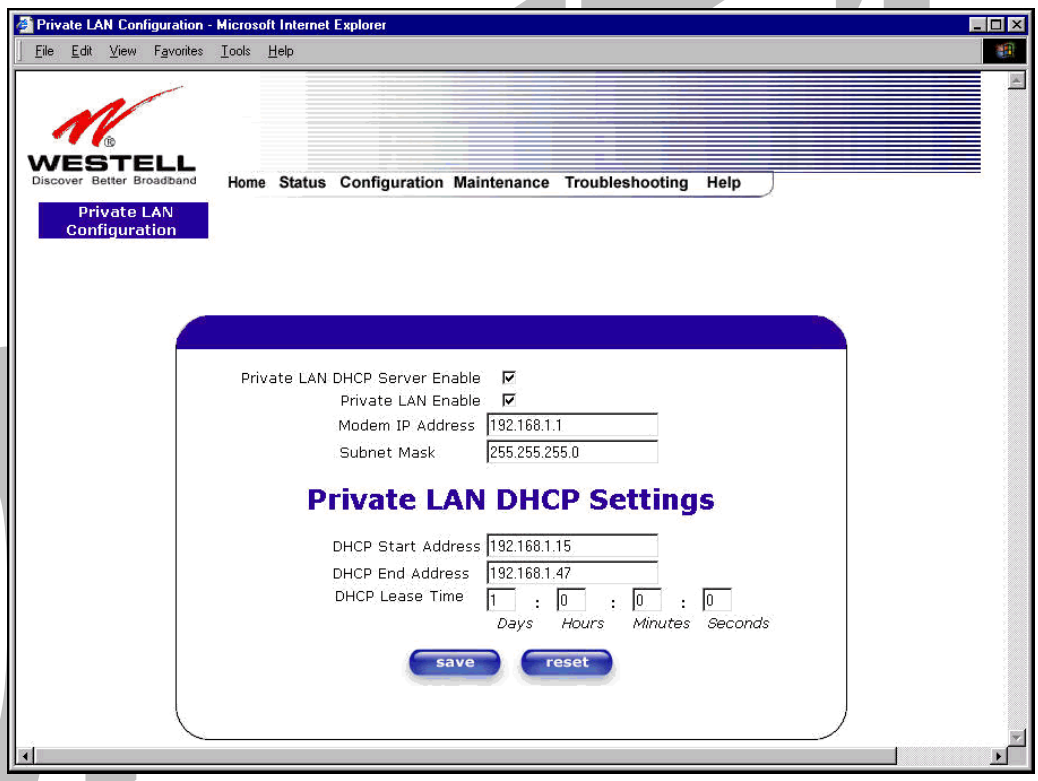
STOP: After you enable the DHCP server, you must reboot your PC

13.5.5 Private LAN Configuration – Configuring NAT

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

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

If you change the settings in this screen, click on **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 Media Gateway'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).

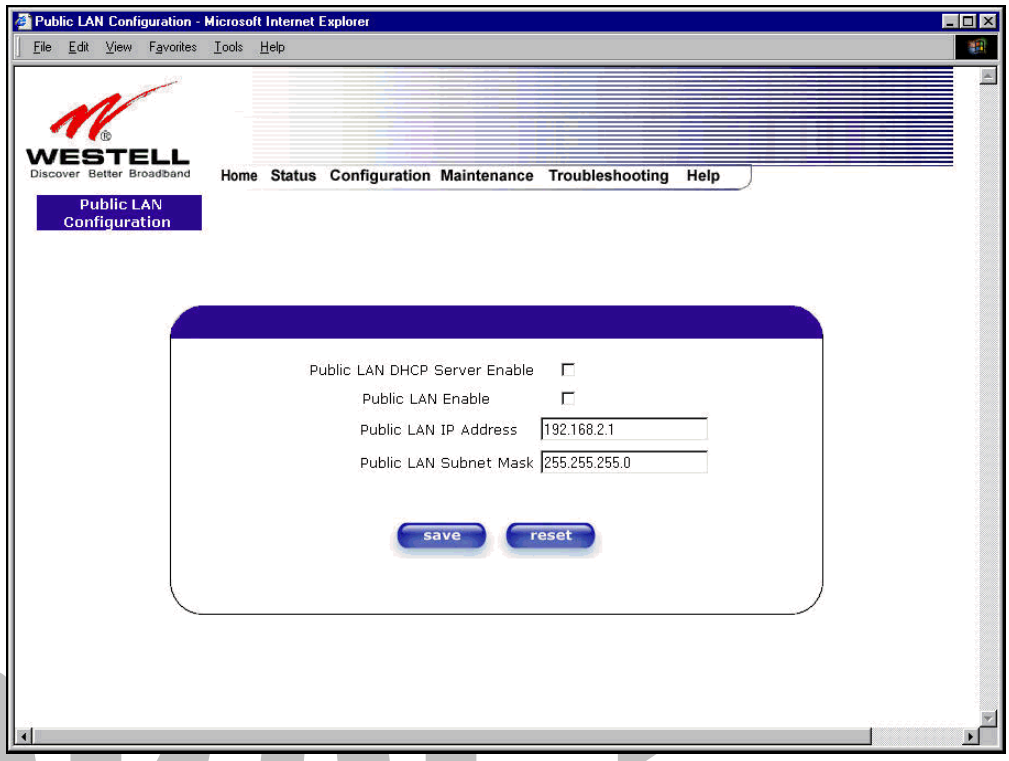
If the settings you have entered in the **Private LAN Configuration** screen are incorrect, the following warnings messages may be displayed via pop-up screens. If this occurs, check the settings in the **Private LAN Configuration** screen.

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

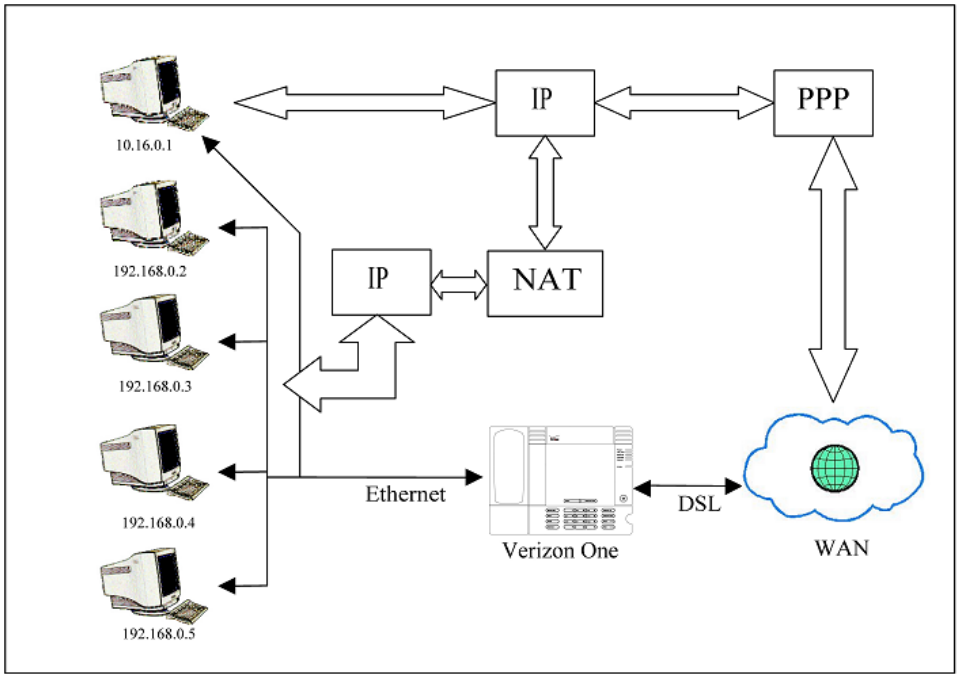
13.5.6 Public LAN Configuration – Multiple IP Address PassThrough

The following screen will be displayed if you select **Public LAN** from the **Advanced LAN** 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 ISP, allows Media Gateway 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 Media Gateway, your ISP must support Public LAN and Static IP. Contact your ISP for details.



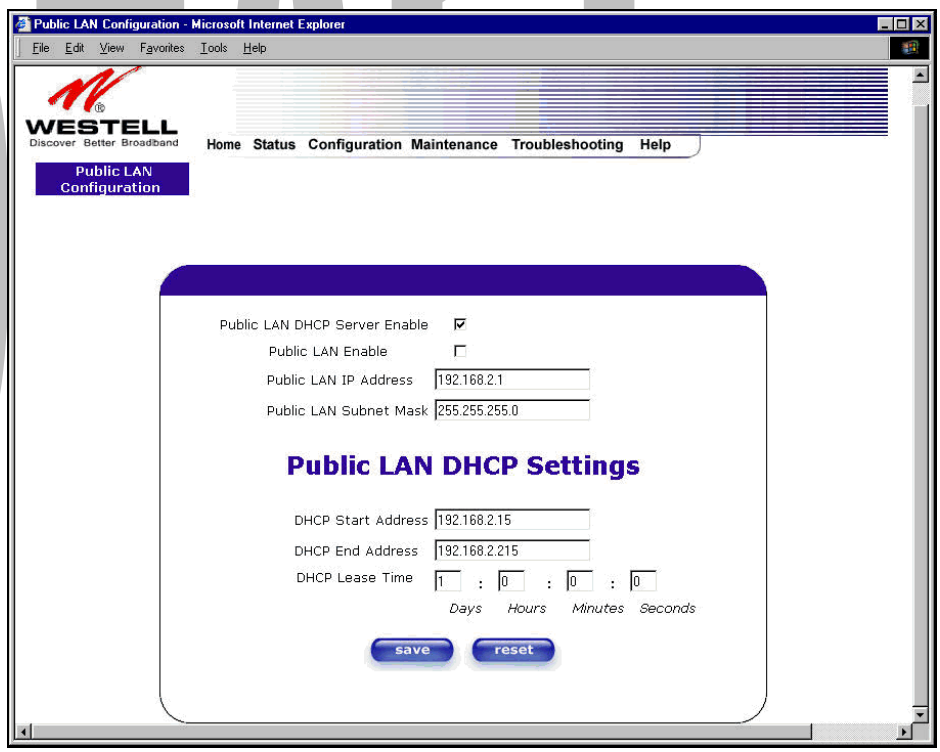
The public devices are visible on the Internet unlike a local NAT'ed PC. The example below shows four NAT'ed PCs and one global PC. The arrows show the data path for each flow.



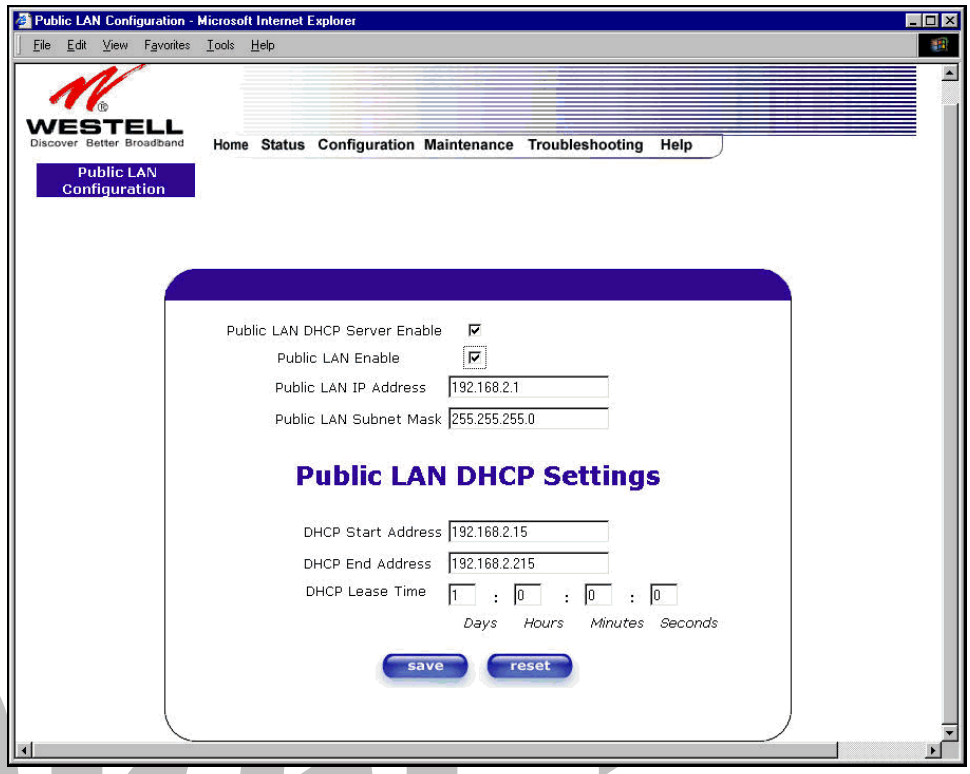
Public LAN DHCP Server Enable	Default = NOT CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Public LAN pool.
Public LAN Enable	Default = NOT CHECKED If this box is CHECKED, it enables the addresses from the Public LAN to bypass the NAT interface.
Public LAN IP Address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

If you clicked on 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 Media Gateway.



If you clicked on 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 on **save**, the following pop-up screen will be displayed. Click on **OK** to save the new settings. If you click on **Cancel**, your new settings will not take effect.

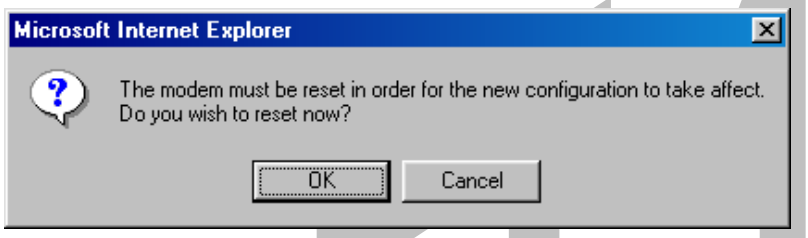
NOTE: DHCP Lease Time values must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.

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.

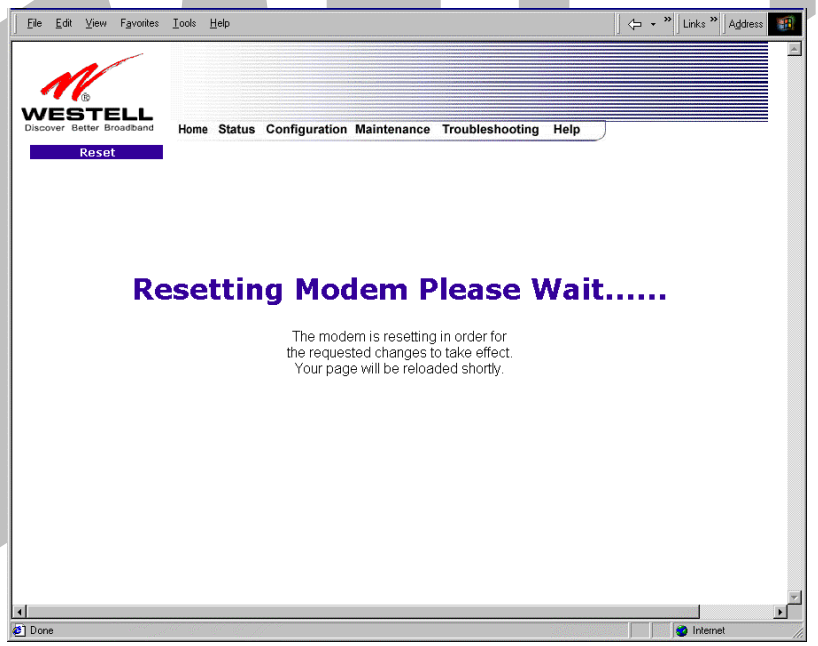
Warning Message	Check Public LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field
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. Media Gateway will be reset and the new configuration will take effect.

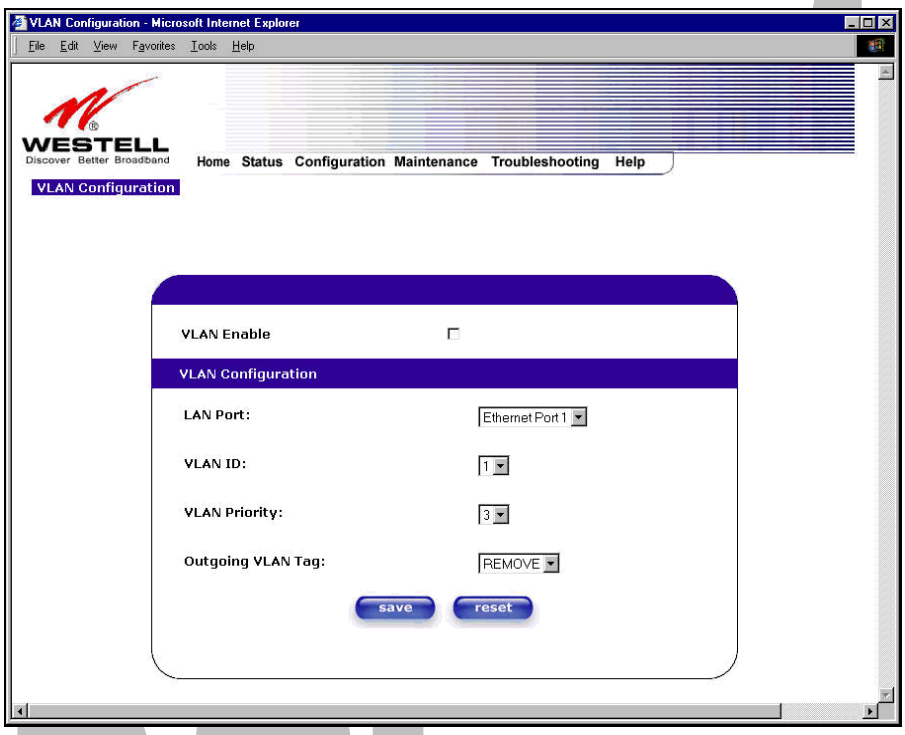


After a brief delay, the home page will be displayed. Confirm that your PPP session displays **UP.** (Click on the **connect** button to establish a PPP session).

NOTE: Whenever the PPP Status displays **DOWN,** you do not have a PPP session established. If the Media Gateway's connection setting is set to "Always On," after a brief delay the PPP session will be established automatically and the PPP Status will display **UP.** If the connection setting is set to "Manual," you must click on the **Connect** button to establish a PPP session. Once the PPP session has been established (PPP Status displays **UP**), you may proceed with the Media Gateway's configuration.

13.5.7 VLAN

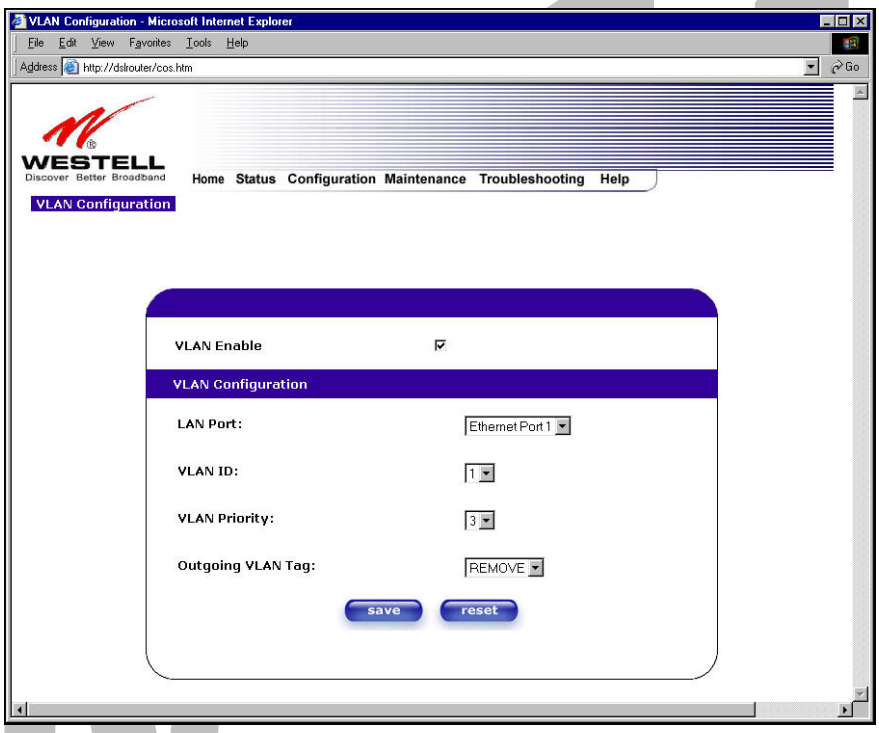
The following settings will be displayed if you select **VLAN** from the **Advanced LAN** menu.



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 responses are: Ethernet Port 1 Ethernet Port 2 Ethernet Port 3 Ethernet Port 4 WLAN Port
VLAN ID	This allows you to assign a VLAN ID to the port. Possible responses are: 1 through 8
VLAN Priority	This allows you to set the VLAN priority for the port. Possible responses are: 0 through 7
Outgoing VLAN Tag	This allows you to keep or remove the VLAN tag on the port when data is outgoing.

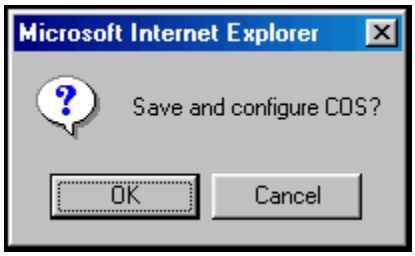
To enable VLAN click on the box adjacent to the **VLAN Enable** field. A check mark will appear in the box. Click on **save.**

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 13.6.3).



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

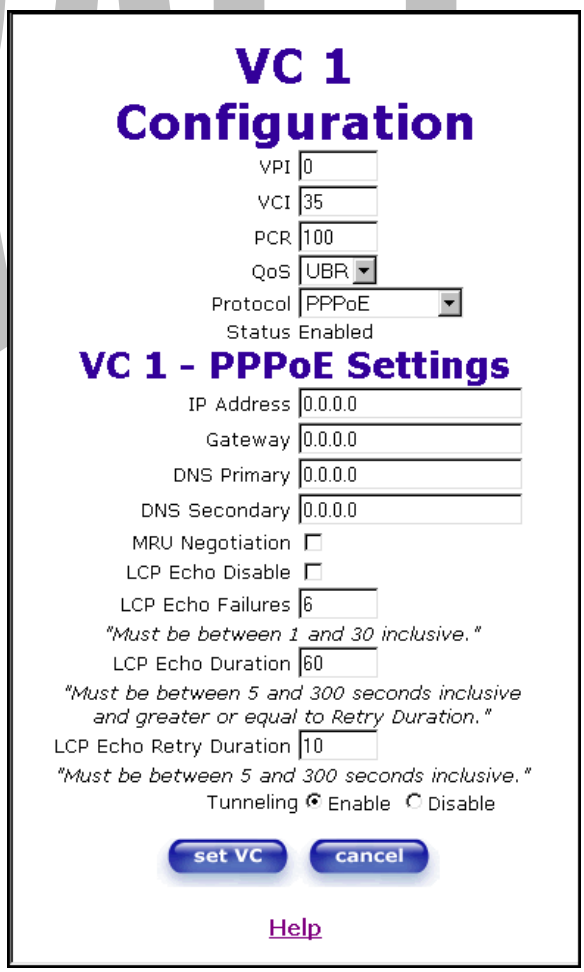
This section explains the configurable features of Media Gateway that are available if you select **Advanced WAN** from the **Configuration** menu.

13.6.1 Editing the WAN Configuration

The following **VC 1 Configuration** screen will be displayed if you click on the **edit** button adjacent to any of the 'Enabled' protocols displayed in the **WAN Configuration** screen. (Note: The Protocol must be enabled before you can edit its VC configuration.) The **VC 1 Configuration** screen allows you to edit your virtual connection (VC). A virtual connection identifies a connection through the ATM network to your ISP. Unlike physical hardware connections, virtual connections are defined by data.

If you change any of the VC settings in the following screen, click on the **Set VC** button.

NOTE: If you experience any problems, please reset Media Gateway via the external hardware reset button or via the procedure defined under the **Maintenance** menu in section 15.1. The actual information displayed in this screen may vary, depending on network connection established.



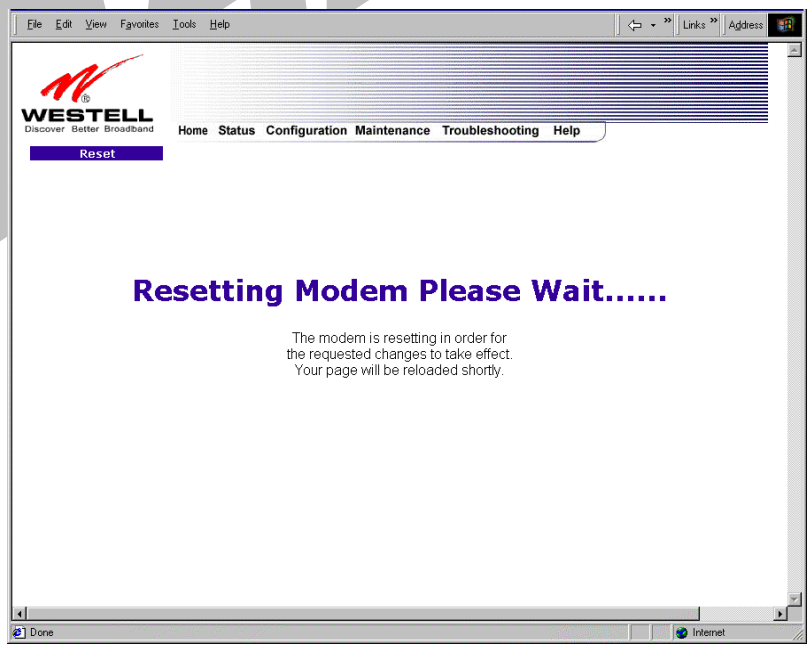
VC 1 Configuration	
VPI	This setting allows you to change your VPI (Virtual Path Indicator) value for a particular VC, which is defined by your ISP.
VCI	This setting allows you to change your VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your ISP.
PCR	Factory Default = 100% Peak Cell Rate (PCR)-The maximum rate at which cells can be transmitted across a virtual circuit, specified in cells per second and defined by the interval between the transmission of the last bit of one cell and the first bit of the next. This value is a percentage of the current data rate. 100 allows this VC to use 100% of the available bandwidth. 80 allows this VC to use 80% of the available bandwidth.
QoS	Quality of Service, which is determined by your ISP. Possible Responses: CBR = Constant Bit Rate UBR = Unspecified Bit Rate VBR = Variable Bit Rate
Protocol	The Protocol for each VC, which is specified by your ISP. Possible Responses: 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.
Status	The protocol status.
VC x PPPoE Settings	
IP Address	Displays the IP network address that your modem is on.
Gateway	Displays the Media Gateway's IP address
DNS Primary	Provided by your ISP.
DNS Secondary	Provided by your ISP.
MRU Negotiation	Factory Default = DISABLED If ENABLED, the Maximum Received Unit (MRU) would enforce MRU negotiations. (NOTE: enable this option only if your ISP instructs you to do so.)
LCP Echo Disable	Factory Default = Enable If checked, this option will disable the modem LCP Echo transmissions.
LCP Echo Failures	Indicates number of continuous LCP echo non-responses received before the PPP session is terminated.
LCP Echo Retry Duration	The interval between LCP Echo transmissions with responses.
LCP Echo Retry Duration	The interval between LCP. Echo after no response.
Tunneling	Factory Default = ENABLE If ENABLED, this option allows PPP traffic to be bridged to the WAN. This feature allows you to use a PPPoE shim on the host computer to connect to your ISP, by bypassing the Media Gateway's capability to do this. NOTE: Tunneling is available in PPPoE mode only.

NOTE: The values for IP Address, Gateway, DNS Primary, and DNS Secondary 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.

If you have made any changes to your VC settings, you need to save them. To save the new VC settings, click on **OK** when asked **Set this PPPoE VC configuration?** If you click on **cancel**, the new VC settings will not be saved.

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

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



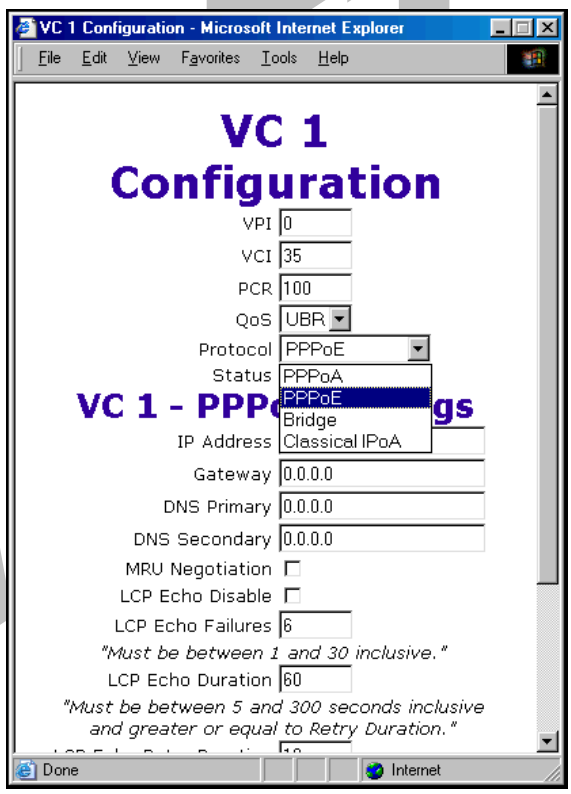
After a brief delay, the home page will be displayed. Confirm that your PPP session displays **UP.** (Click on the **connect** button to establish a PPP session).

13.6.2 Configuring the Media Gateway's Protocol Settings for PPPoE Mode

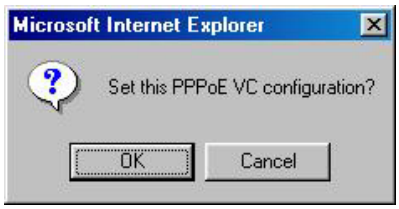
To configure the Media Gateway's protocol settings for PPPoE mode, select **WAN** from the **Advanced WAN** menu. The **WAN Configuration** screen will be displayed. Next, click on the **edit** button adjacent to any of the existing 'Enabled' VC (Virtual Connection) protocols.

NOTE: The protocol status must display "Enable" to allow edits to its VC configuration.

If you clicked on **edit** in the **WAN Configuration** screen, the following **VC 1 Configuration** screen will be displayed. Select **PPPoE** from the options listed in **Protocol** drop-down arrow. After you have made the configuration for this protocol, select the **set VC** button.



If you click the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset your Gateway, as previously discussed in section 13.6.1.



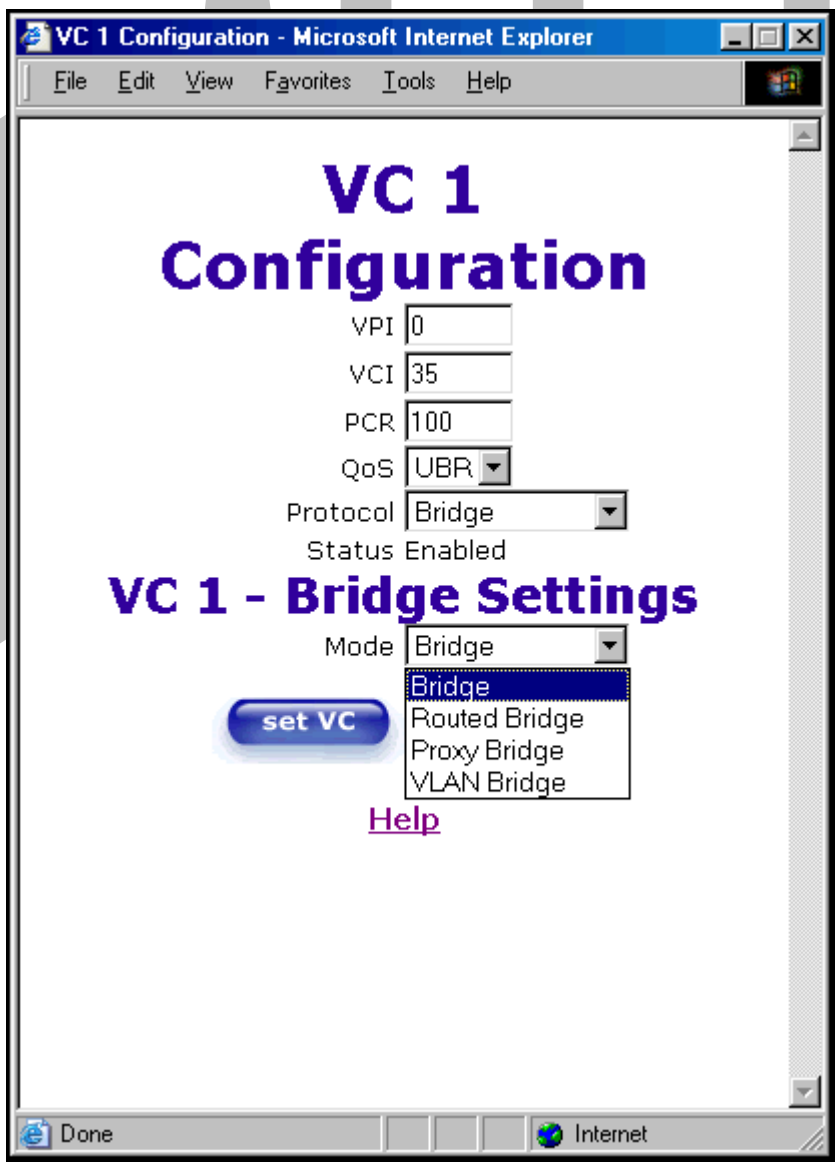
13.6.3 Configuring the Media Gateway's Protocol Settings for Bridge Mode

To configure the Media Gateway's protocol settings for **Bridge** mode, select **WAN** from the **Advanced WAN** menu. The **WAN Configuration** screen will be displayed. Next, click on the **edit** button adjacent to any of the existing 'Enabled' VC (Virtual Connection) protocols. The **VC1 Configuration** screen will be displayed.

NOTE: The protocol status must display "Enable" to allow edits to its VC configuration.

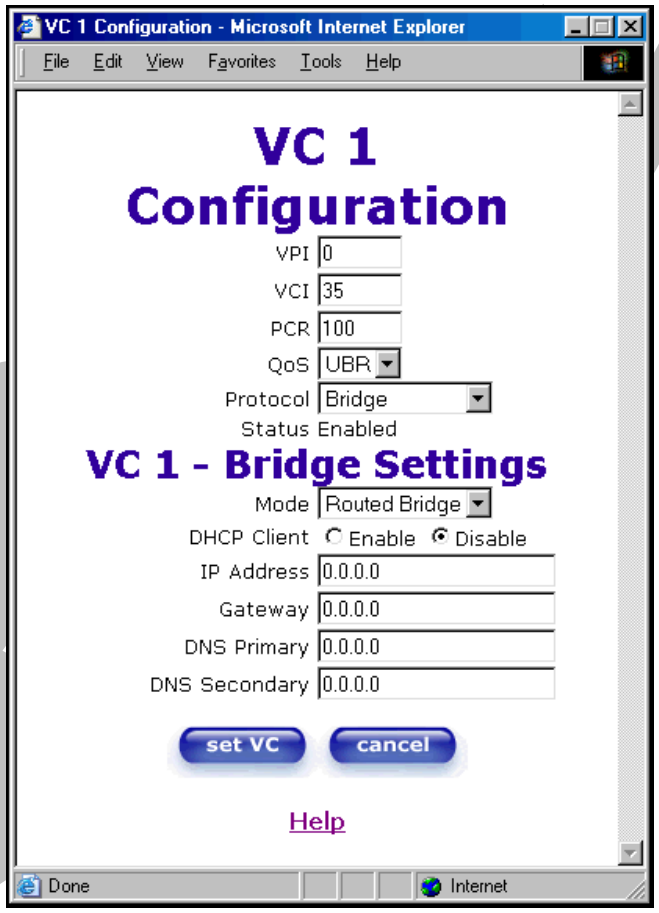
If you select **Bridge** protocol from the **Protocol** drop-down arrow, the following screen will be displayed. Select a mode from the options listed in the **Mode** drop-down arrow, under **VC 1 – Bridge Settings**.

NOTE: In certain network configurations, the user must configure the Media Gateway's VC protocol settings for "Routed Bridge" and "DHCP enable." Please refer to your Internet service provider for instructions on protocol settings.



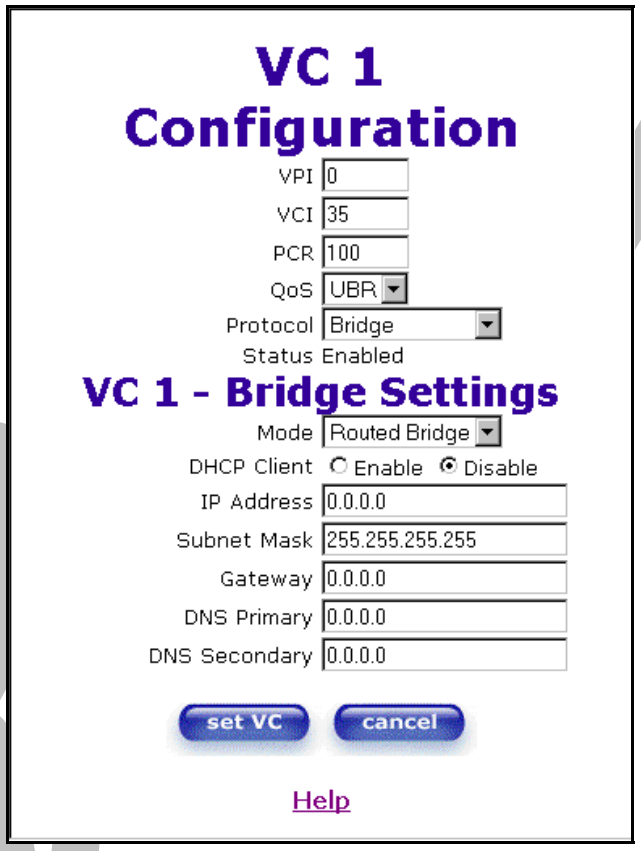
VC 1 Configuration	
VPI	This setting allows you to change your VPI (Virtual Path Indicator) value for a particular VC, which is defined by your ISP.
VCI	This setting allows you to change your VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your ISP.
PCR	Factory Default = 100% Peak Cell Rate (PCR)-The maximum rate at which cells can be transmitted across a virtual circuit, specified in cells per second and defined by the interval between the transmission of the last bit of one cell and the first bit of the next. This value is a percentage of the current data rate. 100 allows this VC to use 100% of the available bandwidth. 80 allows this VC to use 80% of the available bandwidth.
QoS	Quality of Service, which is determined by your ISP. CBR = Constant Bit Rate UBR = Unspecified Bit Rate VBR = Variable Bit Rate
Protocol	The Protocol for each VC, which is specified by your ISP. PPPoA = Point to Point Protocol over ATM (Asynchronous Transfer Mode) PPPoE = Point to Point Protocol over Ethernet Bridge = Bridge Protocol Classical IPoA = Internet Protocol over ATM (Asynchronous Transfer Mode). This is an ATM encapsulation of the IP protocol.
Status	The protocol status.
VC 1 Bridge Settings	
Mode	Bridge = A bridge is a layer 2 device that connects two segments of the same LAN that use the same protocol such as Ethernet. The modem does not have a WAN IP address in this mode. The client PC will typically get an IP address from a DHCP server in the network or the IP address can be assigned to the client PC statically.
	Routed Bridge = Routed Bridged Encapsulation (RBE) is the process by which a bridged segment is terminated on a routed interface. Specifically, your ISP is routing on an IEEE 802.3 or Ethernet header carried over RFC 1483 bridged ATM. RBE was developed to address the known RFC1483 bridging issues, including broadcast storms and security. The modem will get a WAN IP address through DHCP or can be assigned statically. NAT will use the global address assigned to the modem.
	Proxy Bridge = Proxy Bridge is the process in which the modem acts as a proxy ARP agent for a local public subnet. The modem will be assigned an IP address from within that public subnet. The modem will direct all traffic to your ISP's Gateway, which is configured statically. Media Gateway address must not reside within your ISP's Gateway assigned public subnet. All traffic will be sent via the Media Gateway's MAC address. The LAN may also have a private NAT'ed network. NAT will use the global address assigned to the modem.
	VLAN = Assigns VLAN tags to individual data ports on the modem.

If you selected the **Routed Bridge** mode under **VC 1- Bridge Settings,** the following screen will be displayed. Enter the appropriate values in the fields and click on **set VC.**

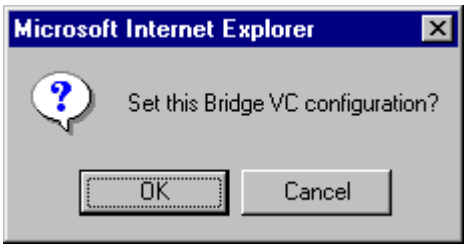


VC 1 - Bridge Settings (Routed Bridge)	
Mode	The Mode you have selected to use with Bridge protocol.
DHCP Client	Selecting a radio button allows you to either Enable or Disable the DHCP Client.
IP Address	Displays the IP network address that your modem is on.
Gateway	Displays the modem's IP gateway address.
DNS Primary	Provided by your ISP.
DNS Secondary	Provided by your ISP.

After you have configured the VC 1 Configuration screen, you must click the **set VC** button to save your VC settings.



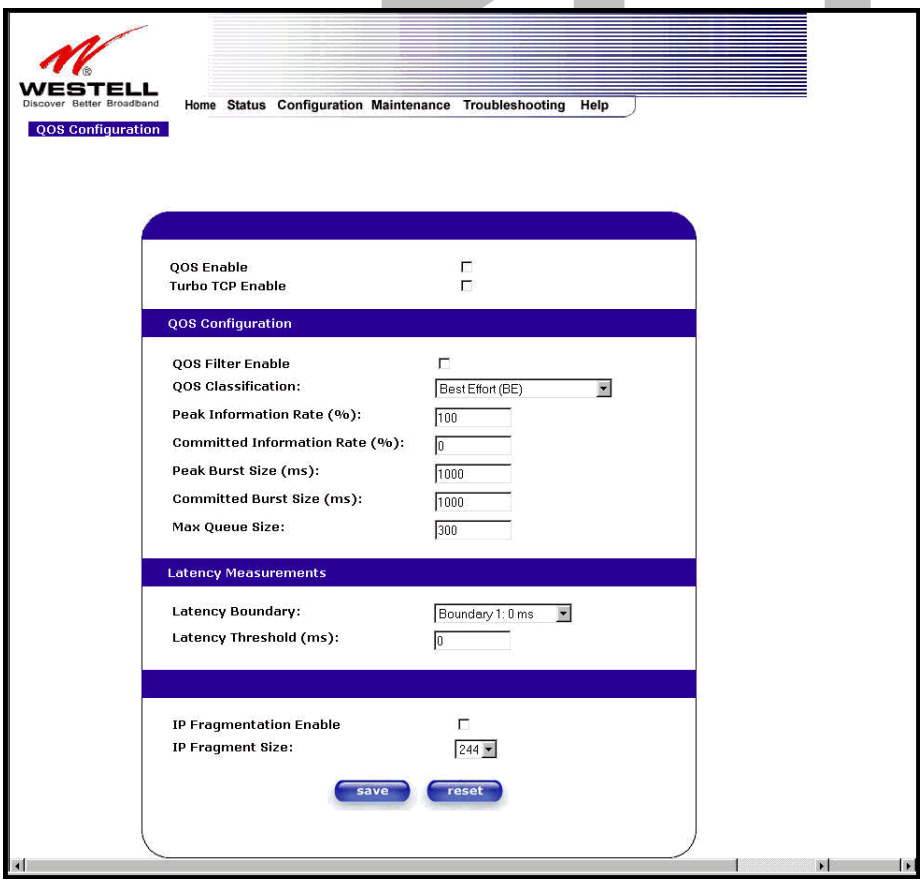
If you click the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset your Gateway, as previously discussed in section 13.6.1.



13.6.4 QOS

The following settings will be displayed if you select **QOS** from the **Advanced WAN** menu. If you change any settings in this screen, click on **save.** If you click on **reset,** this screen will refresh and display your last saved QoS configuration.

NOTE: The QOS feature helps ensure data integrity in high-speed transmissions. QOS provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QOS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay bounds for each traffic class.



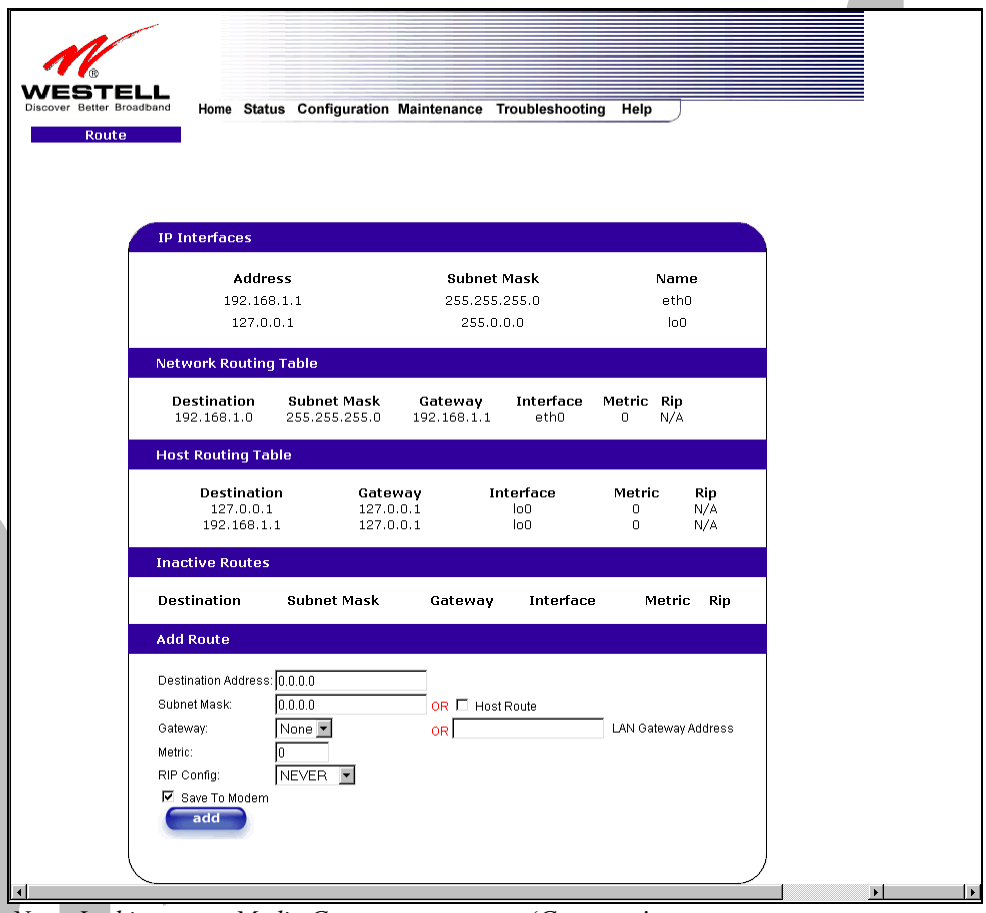
QOS Enable	Factory Default = DISABLED If this box is checked, Quality of Service (QOS) will be Enabled.
Turbo TCP Enable	Factory Default = DISABLED If this box is checked, Turbo TCP will be Enabled.
QOS Configuration	
QOS Filter Enable	Factory Default = DISABLED If this box is checked, this will Enable the QOS filter.
QOS Classification	This feature provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QoS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay

	bounds for each traffic class. Possible responses are: Best Effort (BE) Assured Forwarding (AF1) Assured Forwarding (AF2) Assured Forwarding (AF3) Assured Forwarding (AF4) Expedited Forwarding (EF) Network Control (NC)
Peak Information Rte (%)	The maximum allowed rate for this priority.
Committed Information Rate (%)	The committed rate for this priority.
Peak Burst Size	The interval in milliseconds for averaging the peak offered rate.
Committed Burst Size	The interval in milliseconds for averaging the committed offered rate.
Max Queue Size	The number of packets that can be queued for this priority.
Latency Measurements	
Latency Boundary	This configures the maximum latency boundary in milliseconds that a specific packet may be delayed by.
Latency Threshold (ms)	This setting configures the maximum latency boundary in milliseconds that a specific packet may be delayed by. Possible responses are: Boundary 1:0 ms Boundary 2:10 ms Boundary 3:30 ms Boundary 4:40 ms Boundary 5:100 ms Boundary 6:1000 ms Boundary 7:3000 ms
IP Fragmentation Enable	Factory Default = DISABLED If this box is checked, IP Fragmentation will be Enabled. If Enabled and packets larger than 1500 bytes total are received, they will be fragmented.
IP Fragment Size	This is the IP Packet Size. Possible responses are: 100, 148, 244, 292, 340, 388, or 436

If you made changes to the **QOS Configuration** and clicked on **save,** the following screen will be displayed. Click on **OK.** This will save your new QOS settings.

13.6.5 Route

The following settings will be displayed if you select **Route** from the **Advanced WAN** menu. The Route table maintains the routes or paths of where specific types of data shall be routed across a network.



Note: In this screen, Media Gateway represents 'Gateway.'

To add a Route, enter a **Subnet Mask** address, or check the **Host Route** box. Click on the **add** button to establish a static route.

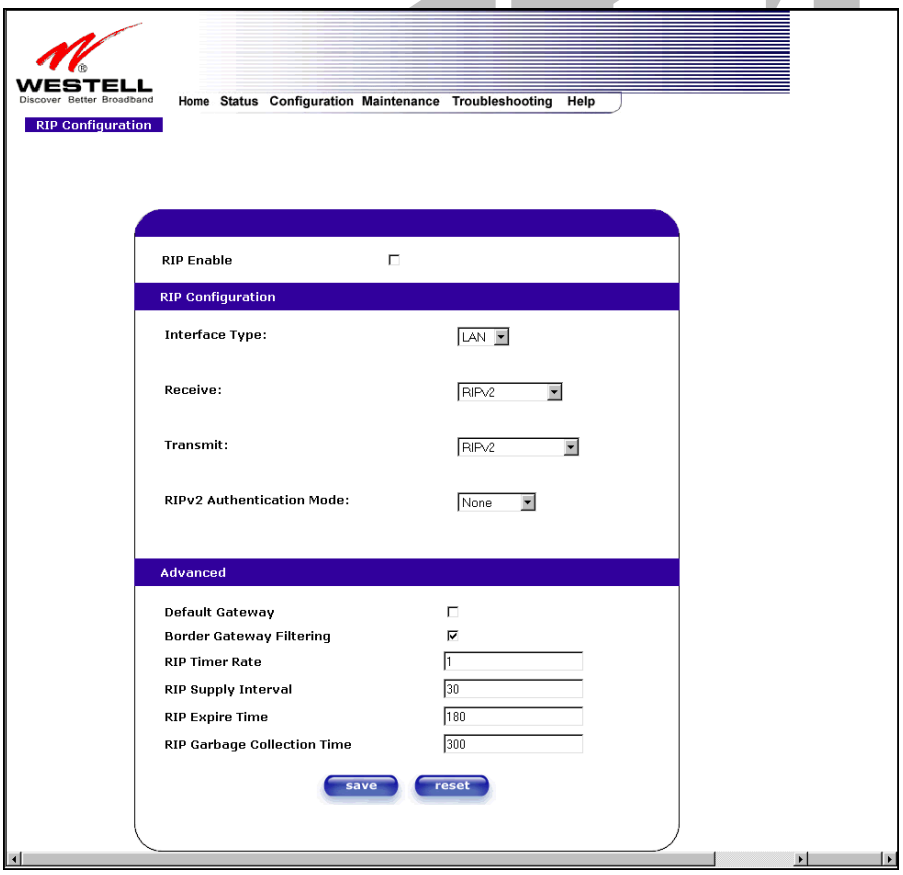
IP Interfaces	
IP Interfaces	The list of active interfaces on the modem and their IP and Subnet mask address. Eth0 is the local LAN interface. Lo0 is the loopback interface.
Address	The IP interface address.
Subnet Mask	The IP interface subnet address.
Name	The IP interface device name.
Network Routing Table	
Network Routing Table	The list of network routes. These can be either routes for directly connected interfaces or static routes.
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
Gateway	Indicates were to send the packet if it matches this route.
Interface	Indicates were to send the packet if it matches this route.

Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
Host Routing Table	
Host Routing Table	The list of host routes. A host route is an IP route with a 32-bit mask, indicating a single destination (as opposed to a subnet, which could match several destinations.)
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
Gateway	Indicates were to send the packet if it matches this route.
Interface	Indicates were to send the packet if it matches this route.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
Inactive Routes	
Inactive Routes	Static routes whose interface is currently not in service.
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
Gateway	Indicates were to send the packet if it matches this route.
Interface	Indicates were to send the packet if it matches this route.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
Add Route	
Add Route	This is used to add a new static route in the modem.
Destination Address	The IP address or subnet of the Route.
Subnet Mask/ Host Route	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
Gateway/IP Address	The interface to use for sending the packet, if it matches this route. (Only active Gateways can be used to create a static route.)
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP Conf	Determines whether or not to advertise the static route, using RIP. (RIP must also be enabled before the route will be advertised.)
Save to Modem	If checked, then the route will be made permanent by saving it to flash memory. If not checked, the route will disappear the next time the modem restarts.

13.6.6 RIP

The following details will be displayed if you select **RIP** from the **Advanced WAN** menu. If you change any settings in this screen, click on **save.** If you click on **reset,** this screen will refresh and display your last saved RIP configuration.

RIP (Routing Interface Protocol) is a dynamic inter-network routing protocol primarily used in interior routing environments. A dynamic routing protocol, as opposed to a static routing protocol, automatically discovers routes and builds routing tables.



Note: In this screen, Media Gateway represents 'Gateway.'

RIP Enable	Factory Default = DISABLED If this box is checked, RIP will be Enabled (turned ON).
RIP Configuration	
Interface Type	LAN: Select this if you are configuring RIP for the LAN side. WAN: Select this if you are configuring RIP for the WAN side. (WAN side is receive only.)
Receive	The version of RIP to be accepted. Possible responses are: None RIPv1 RIPv2 RIPv1 or RIPv2

Transmit	The version of RIP to be transmitted. (WAN side RIP never transmits) Possible responses are: None RIPv1 RIPv1 Compatible RIPv2
RIPv2 Authentication Mode	If using RIP V2, you must select the type of authentication to use. Possible responses are: None Clear Text MD5 (If MD5 authentication, the password)
Advanced	
Default Gateway	Factory Default = DISABLED If this box is check (Enabled), this feature will determine whether the modem advertises itself as a Gateway (i.e., the default route)
Border Gateway Filtering	Factory Default = ENABLED If this box is unchecked (Disabled), the modem will not summarize subnets into a single route before advertising.
RIP Timer Rate	Indicates how often to update the local routing table.
RIP Supply Interval	Indicates how often to advertise routes to neighbors.
RIP Expire Time	Indicates how long routes received from neighbors become invalid, if no refresh of the route is received.
RIP Garbage Collection Time	Indicates how long to advertise invalid routes after they have expired.

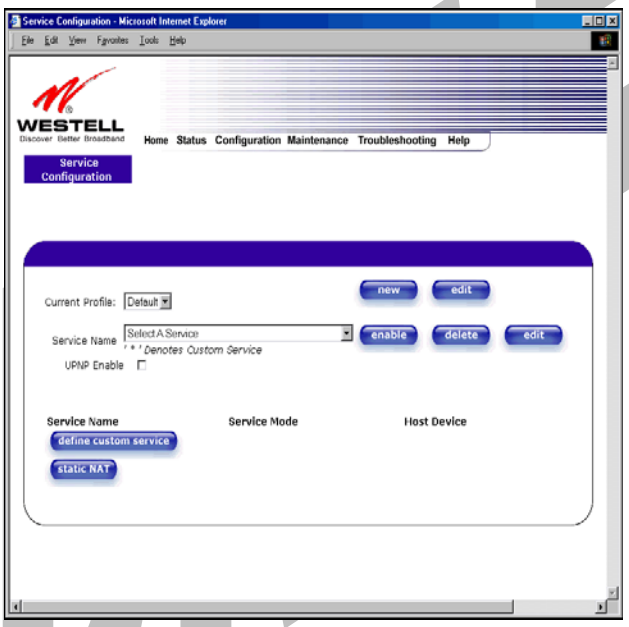
If you change any settings in the **RIP Configuration** screen and clicke on **save,** the following screen will be displayed. Click on **OK** to save your new RIP settings.

14. SETTING UP ADVANCED SERVICE CONFIGURATION

You can set up additional Service Configuration options for Media Gateway that allow you to enter the port forwarding and trigger ports ranges of your choice. Go to **Configuration** at the homepage menu and select **Services.**

When you click on **define custom service** in the **Service Configuration** screen, the **Custom Service** screen will guide you through the steps of creating an advanced NAT service entry via the **define custom service** button.

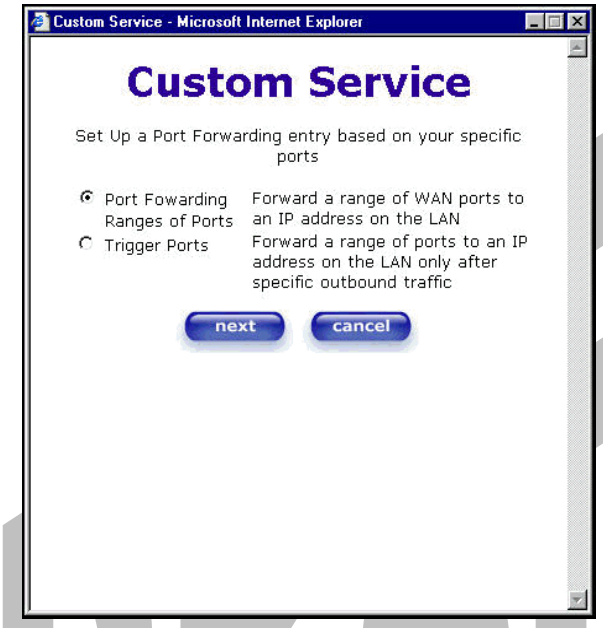
NOTE: Westell strongly recommends that you do not change any values in this section. If you experience any problems, please reset Media Gateway via the external hardware reset button or the procedure defined under the **Maintenance** menu.

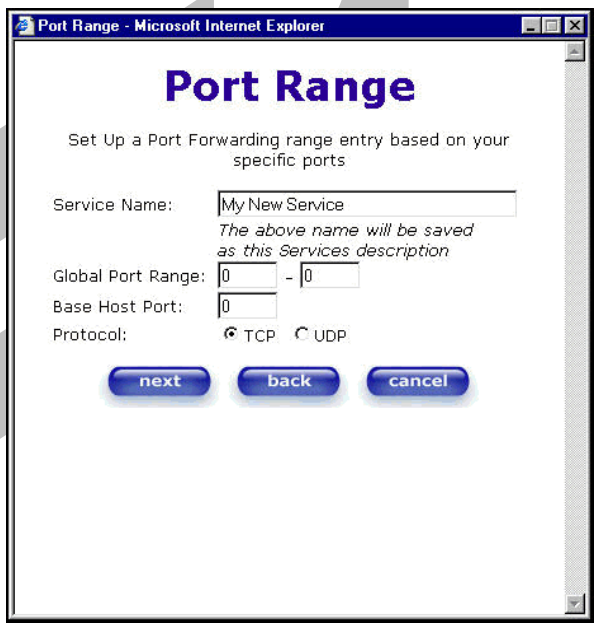


Port Forwarding Ranges of Ports	This option allows you to forward a range of WAN ports to an IP address on the LAN.
Trigger Ports	This option allows you to forward a range of ports to an IP address on the LAN only after specific outbound traffic.

14.1 Port Forwarding Ranges of Ports

To select **Port Forwarding Ranges of Ports**, click on **define custom service** from the **Service Configuration** screen, and then select **Port Forwarding Ranges of Ports** from the **Custom Service** screen. Click on **Next**. The **Port Range** screen will be displayed. Enter your values in the **Global Port Range** fields and click **next** to continue.





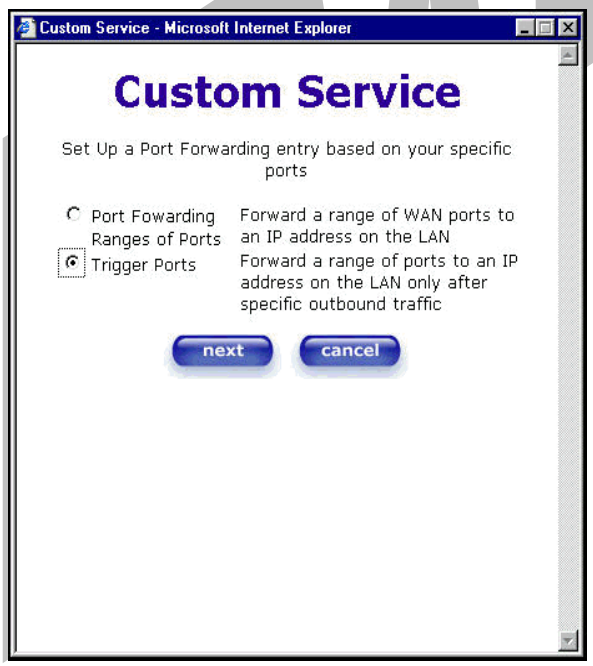
14.2 Adding Port Forwarding Ports

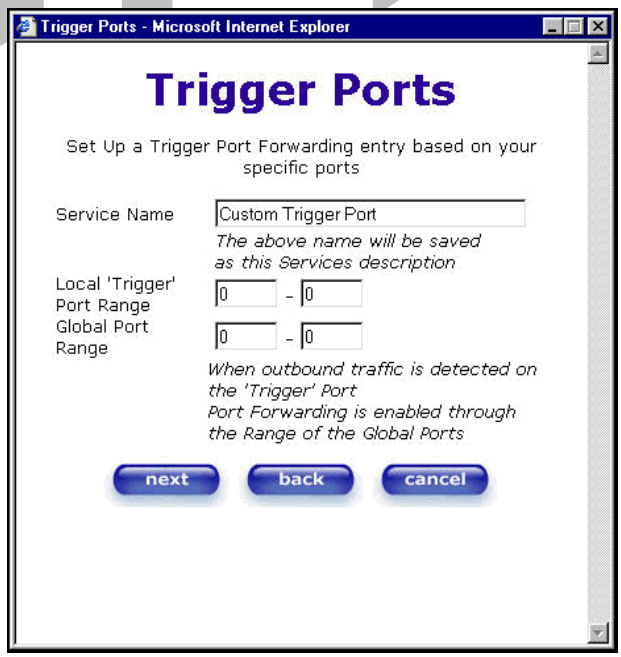
If you made changes in the **Port Range** screen and clicked on **next**, the following screen will be displayed. Click on **close** to accept the changes, or click on **add** to go back to **Port Range** screen and enter additional port range values. You can repeat this step for each range of ports that you want to add (up to 62 port forwarding ranges). When you are finished adding ports to the Global Port Range, you must click on **close** to accept the information you have entered and return to the **Service Configuration** screen.

Service Name	The NAT service for which you are configuring Port Forwarding.
Type	The type of NAT service configuration you selected.
Protocol	The type of Protocol that is used to run this NAT service. TCP- Transmission Control Protocol. UDP-User Datagram Protocol (UDP).
Local IP Address	If a static IP address has been assigned, it will be displayed here.
Base Host Port	The port on the WAN that will host the NAT service selected. Base Host Port is the first port that will be used for a specific service when configured for a range of ports.

14.3 Port Forwarding Trigger Ports

To select **Port Forwarding Trigger Ports**, click on **define custom service** from the **Service Configuration** screen, and then select **Trigger Ports** from the **Custom Service** screen. Click on **next**. The follow settings will be displayed in the **Trigger Ports** screen. Enter your values in the **Local 'Trigger' Port Range** fields and click on **next** to continue.





Service Name	The NAT service you selected.
Local Trigger Port Range	The local LAN side TCP/UDP port.
Global Port Range	The WAN side TCP/UDP port range.

14.4 Adding Local Trigger Ports

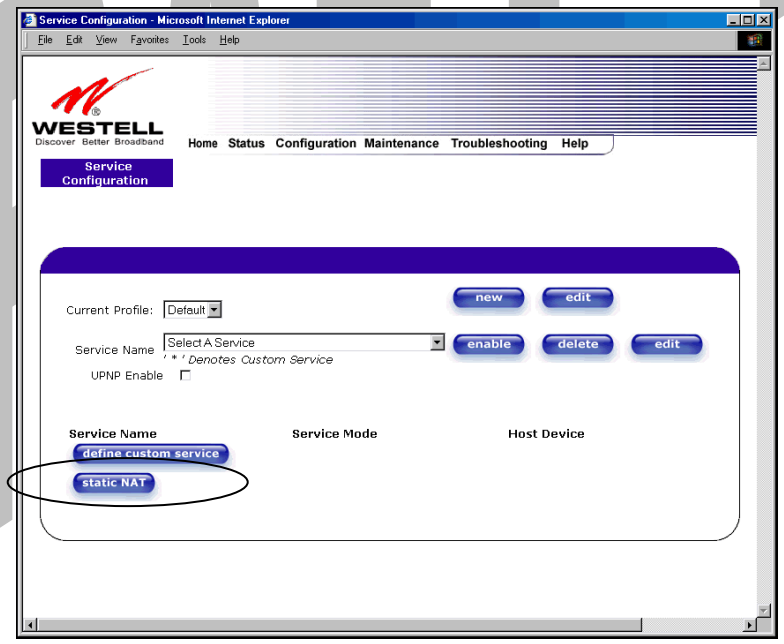
If you made changes in the **Local 'Trigger' Port Range** screen and clicked **next**, the following screen will be displayed. Click on **close** to accept the changes, or click on **add** to go back to the **Trigger Ports** screen and enter additional port range values. You can repeat this step for each port range that you want to add (up to 10 trigger ports). When you are finished adding ports to the Local 'Trigger" Port Range, you must click on **close** to accept the information you have entered and to return to the **Service Configuration** screen.

14.5 Static NAT

If you select **Services** from the **Configuration** menu, the following screen will be displayed, showing the static NAT button. Static NAT allows you to configure Media Gateway to work with the special NAT services.

NOTE: When Media 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.

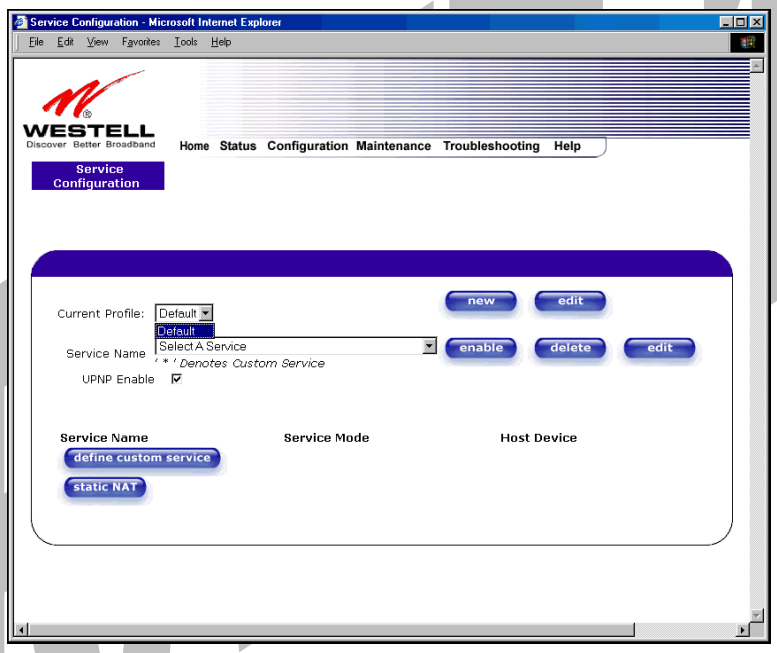
STOP: Single Static IP must be disabled (if it has been enabled previously) before you enable **static NAT**. To disable Single Static IP, select **Single Static IP** from the **Configuration** menu. Next, click on the **disable** button, and then click on **OK** in the pop-up screens to allow Media Gateway to be reset. As explained in section 13.1 (Single Static IP), you must reboot your computer after you enable or disable Single Static IP. After you have rebooted your computer, return to static NAT configuration screen by selecting **Services** from the **Configuration** menu and clicking on the **static NAT** button.



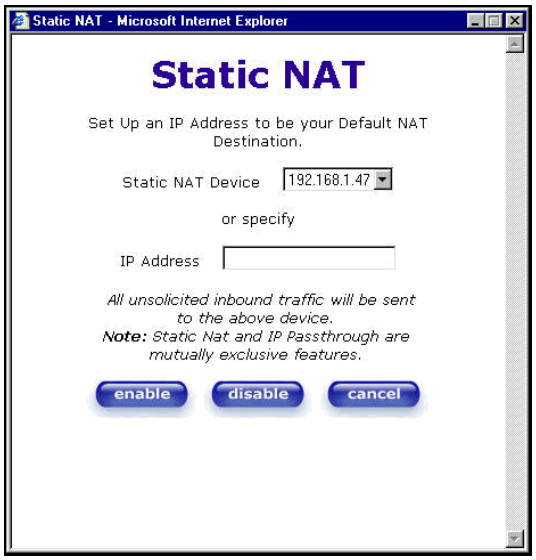
14.6 Enabling Static NAT

Before you enable static NAT, you must select **Default** from the **Current Profile** drop-down box. Static NAT must be configured for the Media Gateway's default account profile. After you select the default profile, click the **static NAT** button.

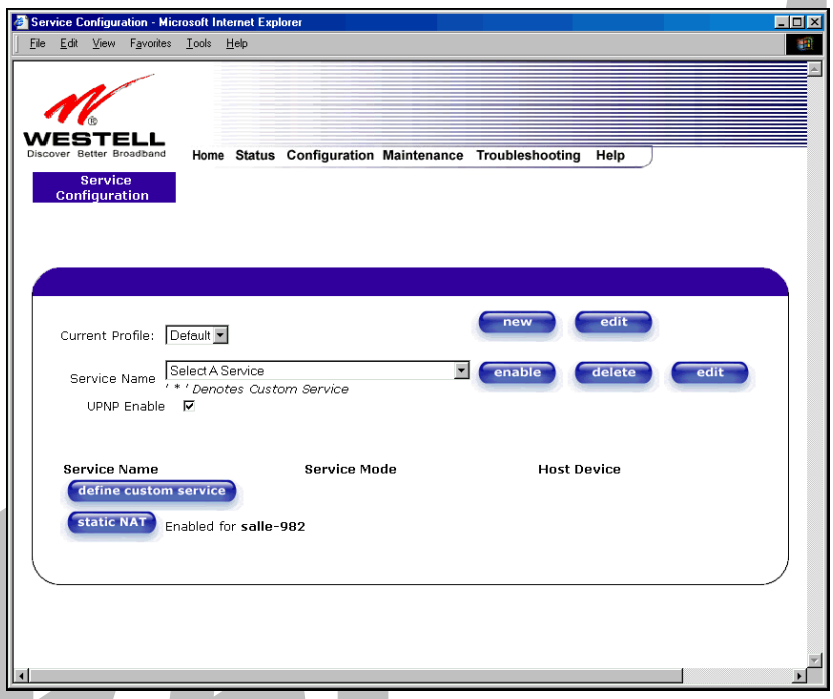
NOTE: In the following screen, the default account profile is labeled **Default**. However, if you have renamed the default account profile, you must select the profile name you created as the default profile.



If you click on the **static NAT** button in the **Service Configuration** screen, the following screen will be displayed. Select your device from the **Static NAT Device** drop-down arrow, or type the IP address of the device in the field labeled **IP Address**. Click on **enable**. This will automatically enable the Static NAT feature for that device.

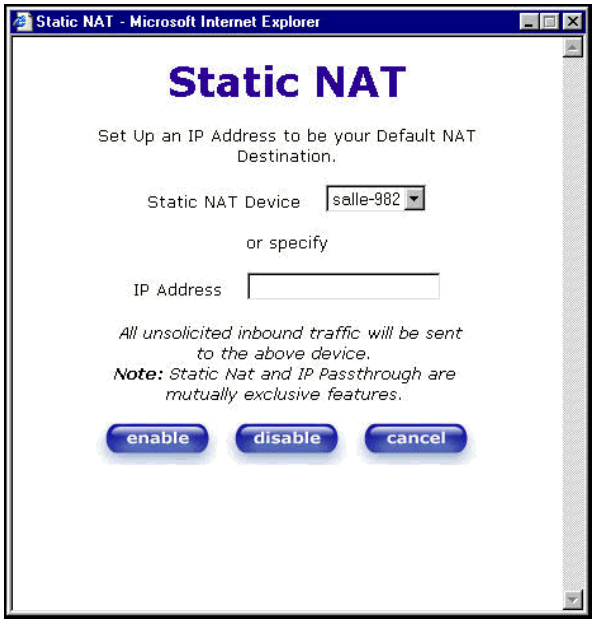


If you click **enable,** the following Service Configuration screen will display. Static NAT is now enabled for the device you selected.

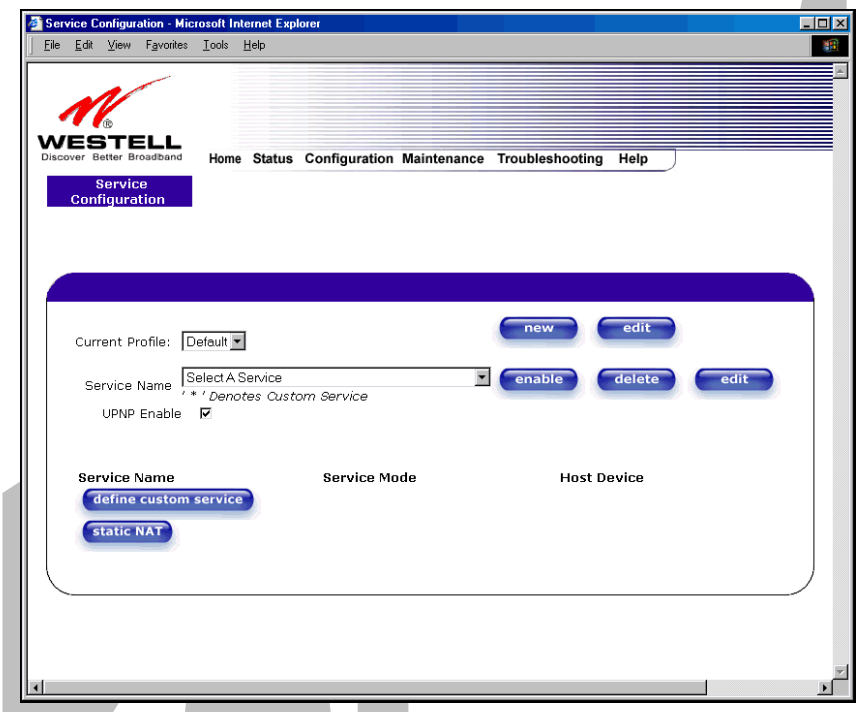


14.7 Disabling Static NAT

If you click on **static NAT** in the **Service Configuration** screen, the following screen will be displayed, select a device name from the **Static NAT Device** drop-down arrow, or type the IP address of the device in the field labeled **IP Address.** Click on **disable.** This will automatically disable the Static NAT feature for that device.



If you click **disable,** the following Service Configuration screen will be displayed. Static NAT is now disabled for the device you selected. (No device is displayed in the field adjacent to the **static Nat** button.)

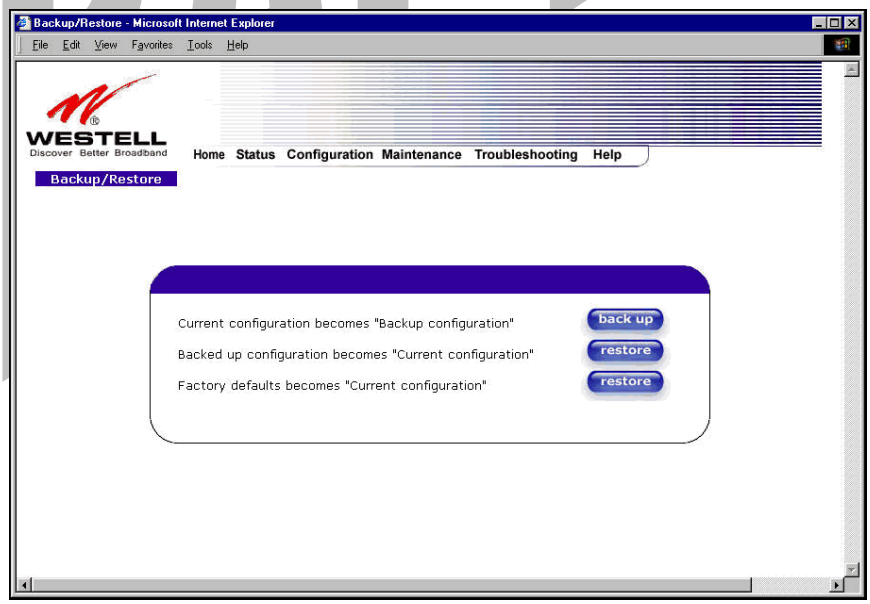


15. MAINTENANCE

15.1 Backup/Restore

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

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

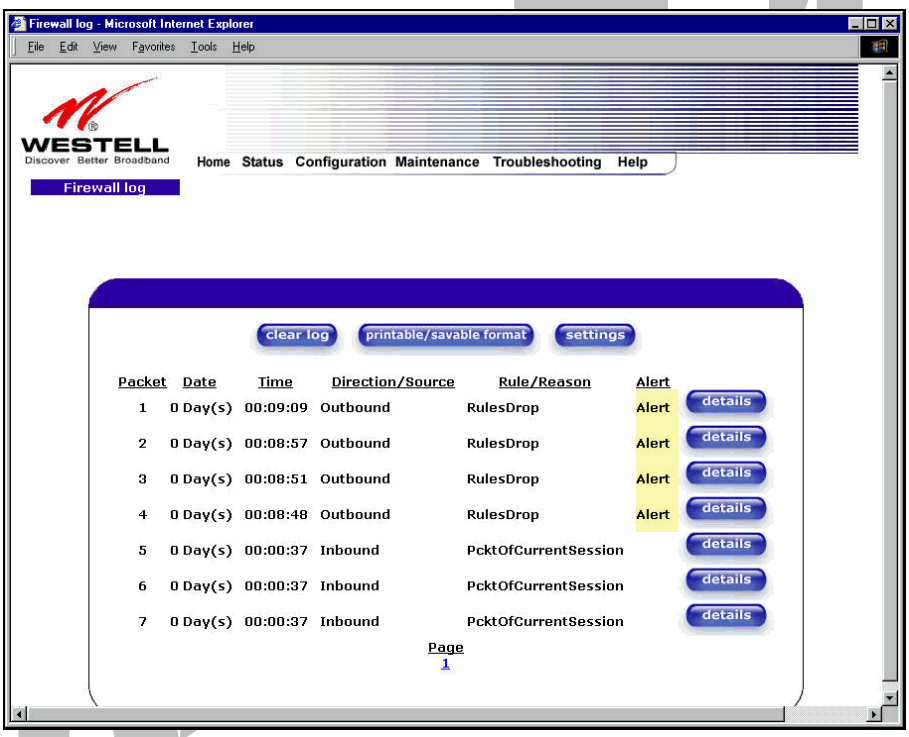


Current configuration becomes Backup Configuration	Select this button if you want to store all of the current configuration data such that it can be recalled later.
Backed up configuration becomes Current configuration	Select this button if you want to retrieve the last back up copy of all configuration parameters and make these values current.
Factory default becomes Current configuration	Select this button if you want set all user configurable parameters back to the factory default.

15.2 Firewall Log

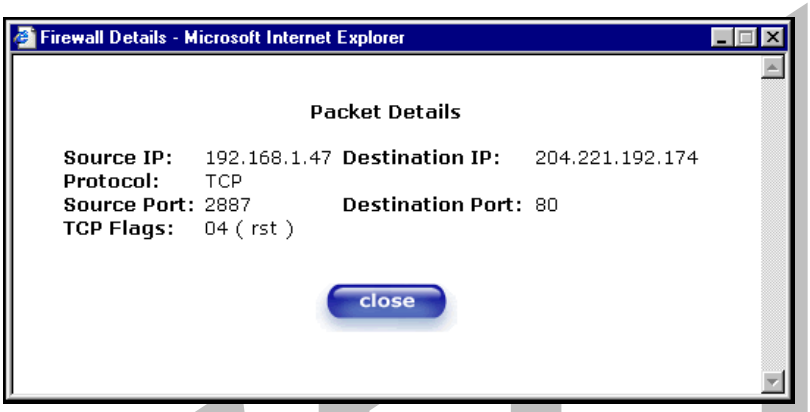
The following settings will be displayed if you select **Firewall Log** from the **Maintenance** menu.

This screen is an advanced diagnostics screen. It alerts you of noteworthy information sent to Media Gateway from the Internet. The screen can contain 1000 entries, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for the new entries as they occur. The following settings are displayed.



Clear log	Selecting this button removes all entries from the log.
Printable/savable format	Selecting this button opens a new window that contains a list of all the logged packets that can be saved or printed.
Settings	Selecting this button opens a new window that contains configuration settings for selecting the information that you want logged.
Packet	The packet number.
Date	The number of days passed since that the packet was sent.
Time	The time that the packet was sent.
Direction/Source	The direction of transmission.
Rule/Reason	The internal rule that caused the logged event. The internal rule is set up under Firewall rules.
Alert	Displays a description of the logged event.

If you clicked on **details** in the **Firewall Log** screen, the **Packet Details** screen will be displayed. Click on **close.**



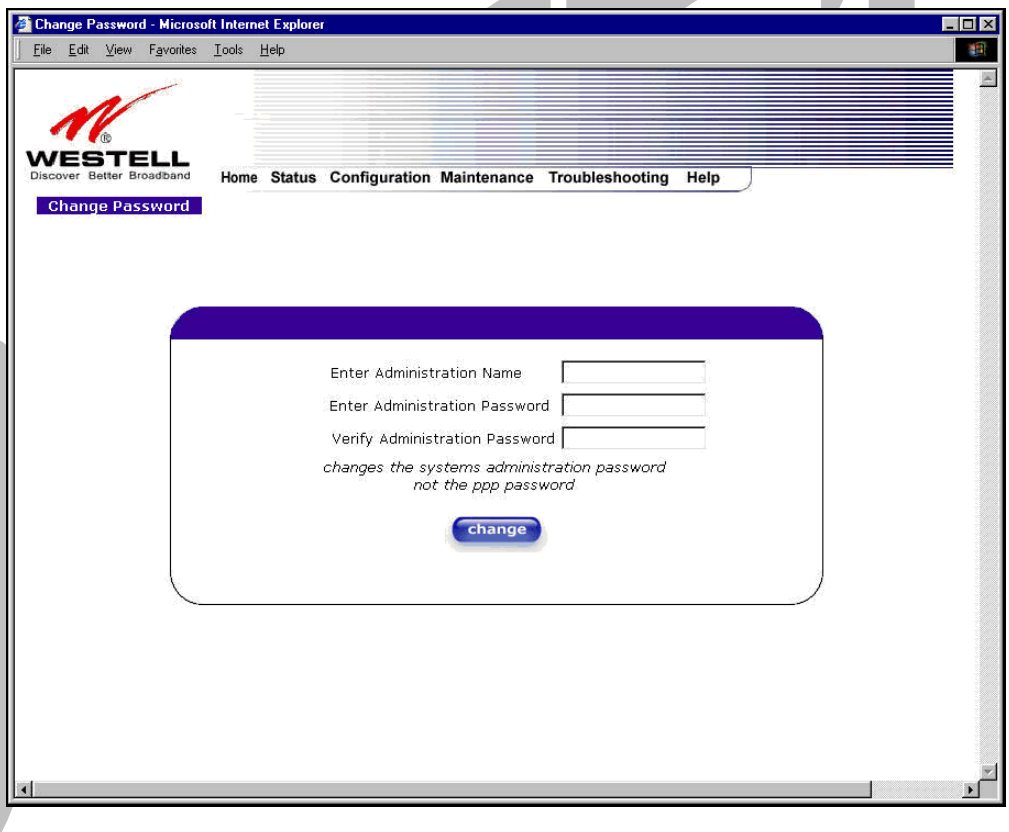
To clear the Firewall log, click **clear log** in the **Firewall Log** screen. The following pop-up screen will be displayed. Click **OK** when asked "**Do you wish to clear the Firewall log file?"** If you click **Cancel**, the firewall log will not be cleared.

To obtain a printable format of the Firewall Log, at the **Firewall Log** screen, click **Printable/Savable Format**. This will allow you to send a copy of the Firewall log to your designated printer.

15.3 Administrative Password

The following settings will be displayed if you select **Administrative Password** from the **Maintenance** menu. After you enter your data into the appropriate settings, click on **change**.

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

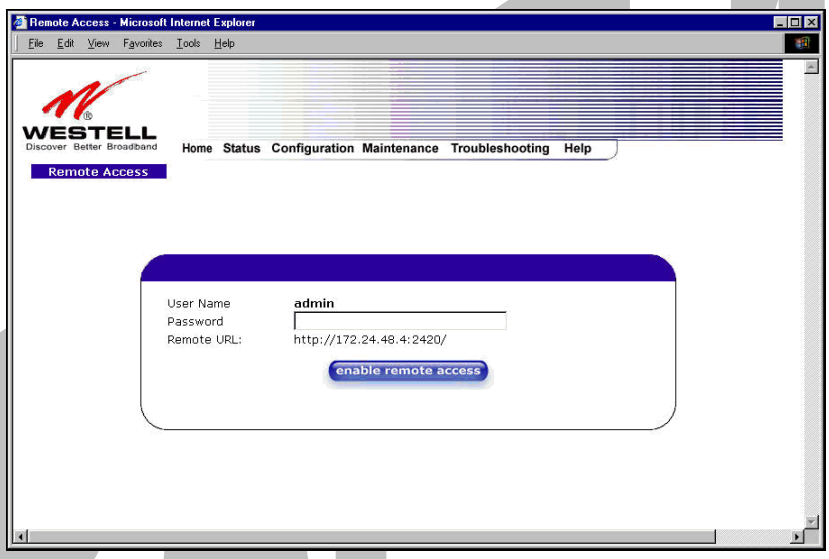


Enter Administrative Name NOTE: This changes the Systems Administrator password not the PPP password.	Type the name of your network administrative.
Enter Administrative Password	Type your network administrator's password.
Verify Administrative Password	Re-type your network administrator's password.

15.4 Remote Access

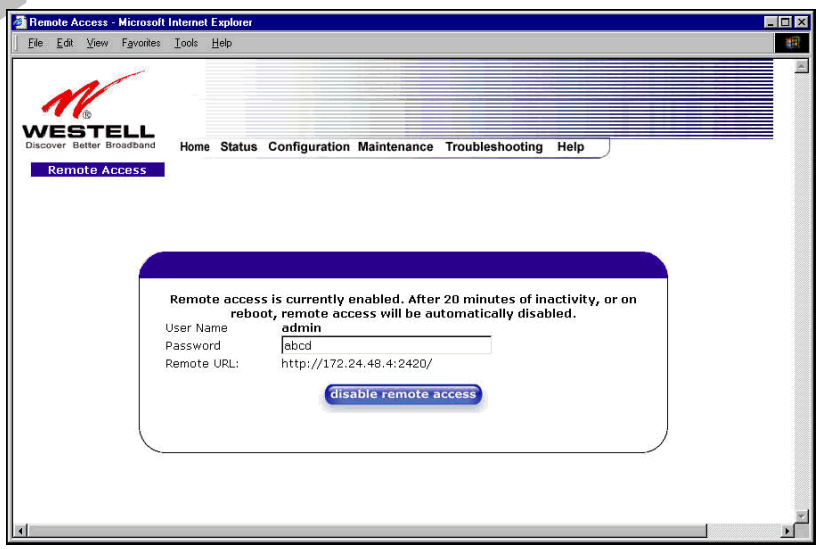
The following screen will appear if you select **Remote Access** from the **Maintenance** menu. To enable Remote Access, type in a password and click the **enable remote access** button.

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



User Name	Displays your current User Name (Static field)
Password	Field for entering your password
URL	Displays the IP address of the remote management of your Gateway.

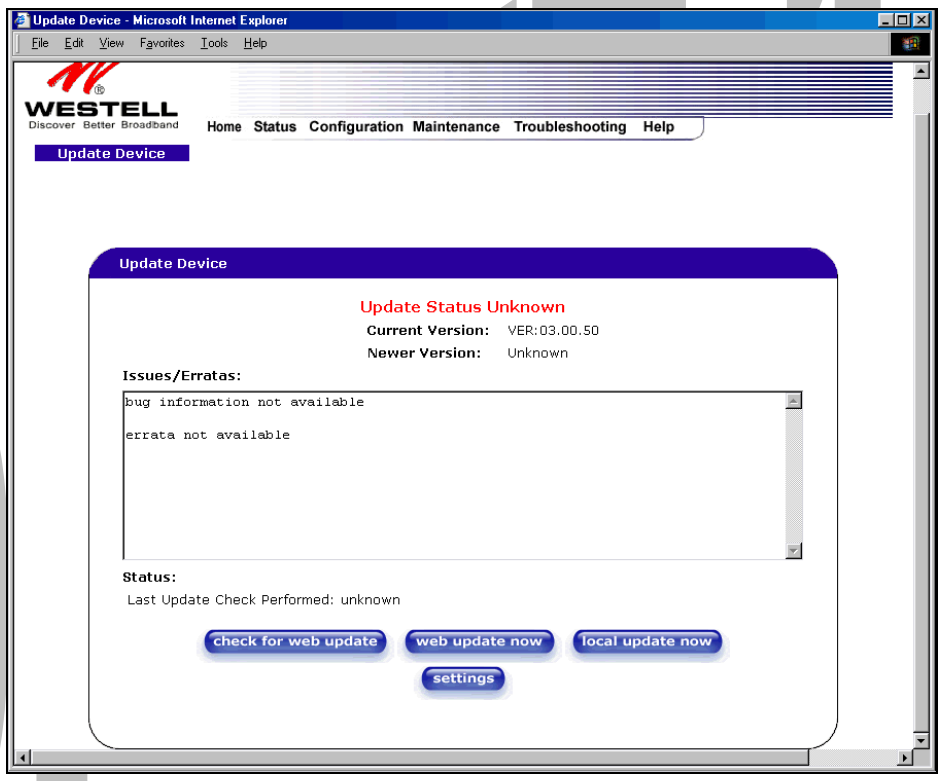
The following screen displays a message that the remote access is currently enabled. After 20 minutes of inactivity, or on reboot, remote access will be automatically disabled. To disable remote access, click on the **disable remote access** button.



15.5 Update Device

The following screen will be displayed if you click on **Update Device** from the **Maintenance** menu. This screen is used to update the firmware that controls the operation of your Gateway. The updated firmware may be loaded from either a file that is located on your PCs hard drive or from update files stored on an Internet server.

NOTE: The configurable settings of Media Gateway may be erased during the update process.

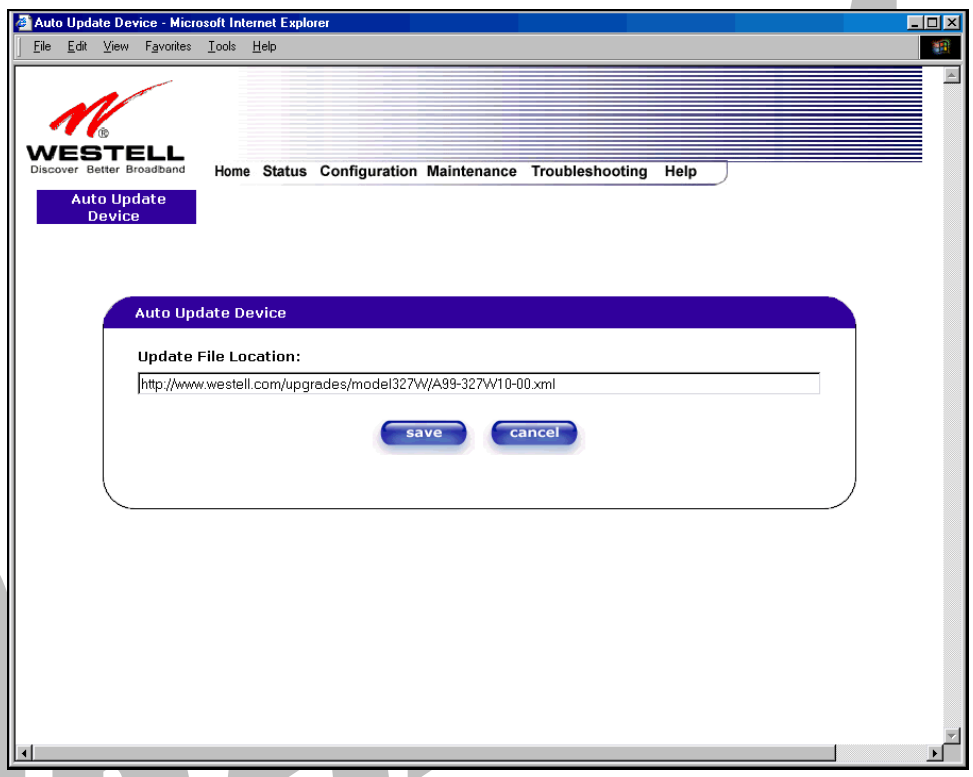


Click on the **check for web update** button in the **Update Device** screen to check the web for possible software updates. This screen will retrieve the software update file and display any available update information. You must be connected to the Internet to use this option.

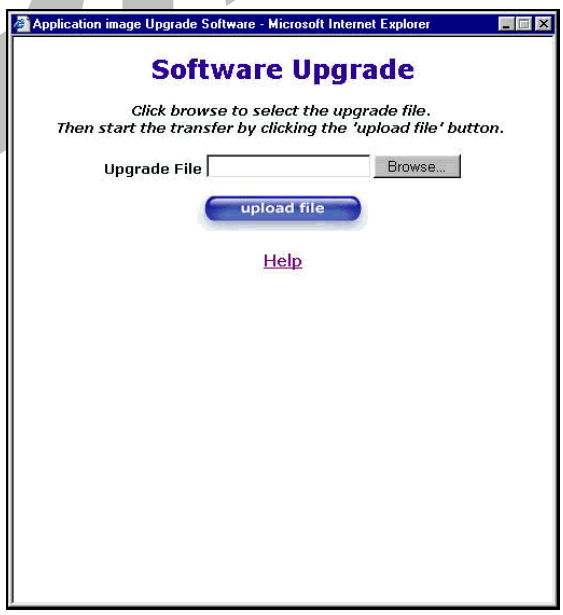
NOTE: If you click on check for web update and the page returns a “page not found” message, this indicates that the software update file is not available. Go back to the previous screen to continue.

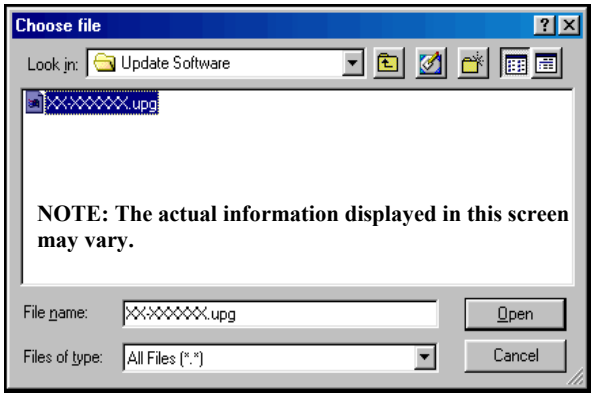
Click on the **web update now** button in the **Update Device** screen to download the software update file and automatically update the modem firmware if an update is available and applicable. You must be connected to the Internet to use this option.

If you click on the **settings** button in the **Update Device** screen, the following screen will appear. This screen displays the location of the software update file.

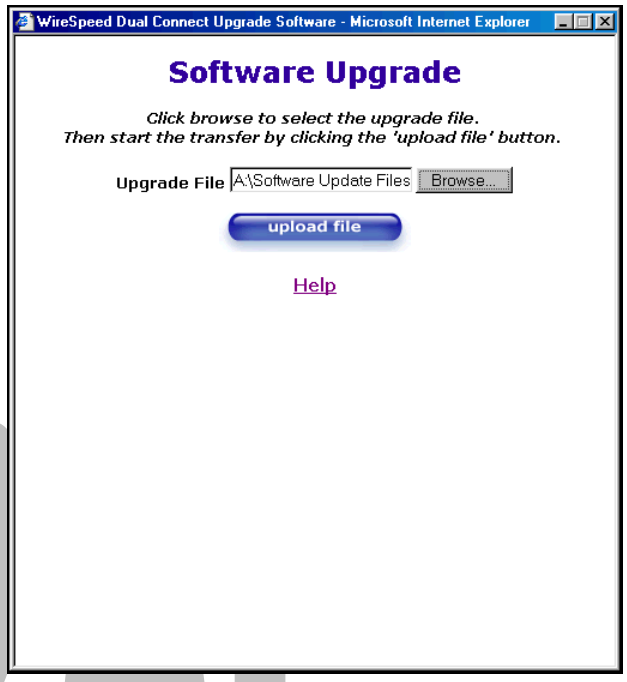


Click on the **local update now** button in the **Update Device** screen to select the upgrade file from your PC's hard drive. This screen allows you to upgrade the software on your Media Gateway. Click **Browse…** and go to the location where the upgrade file is stored.

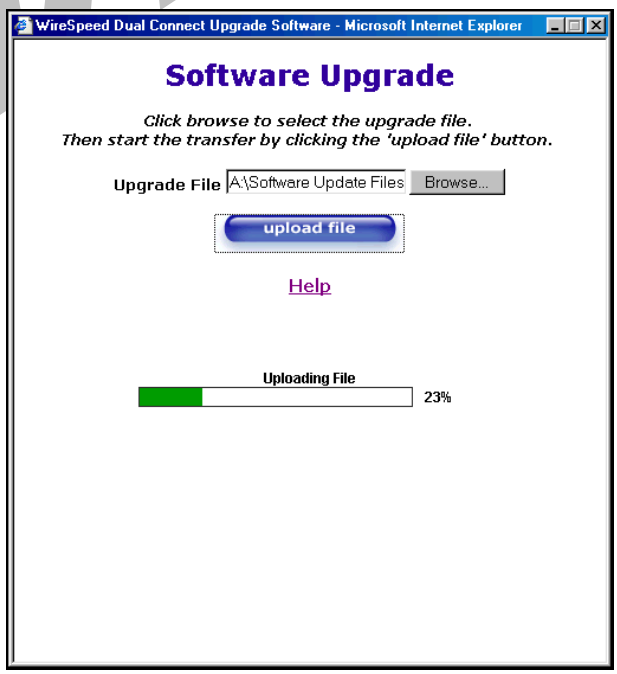




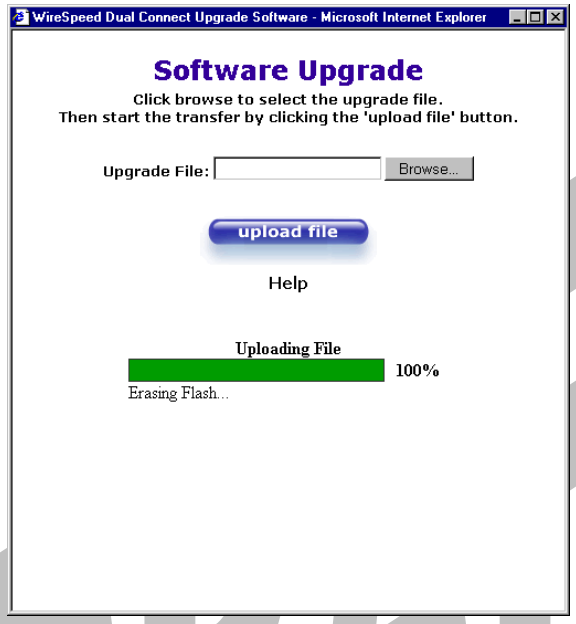
Select the appropriate upgrade file from your browser. The file name will appear in the field labeled **Upgrade File**. Click on **upload file.**

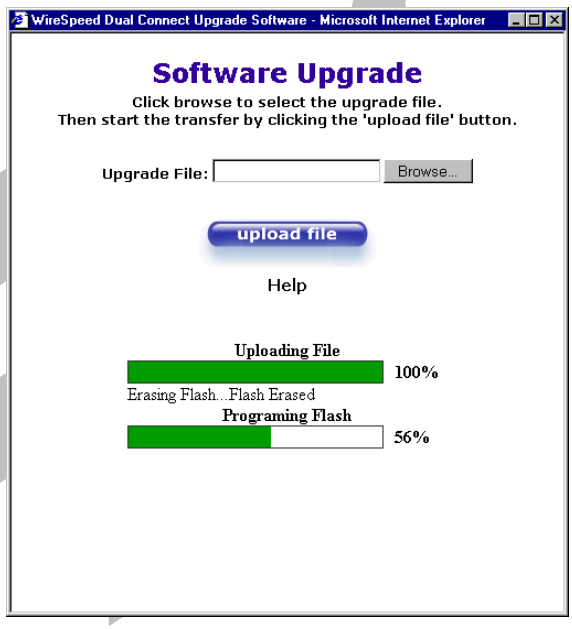


This screen shows that the file is being uploaded to your Gateway.

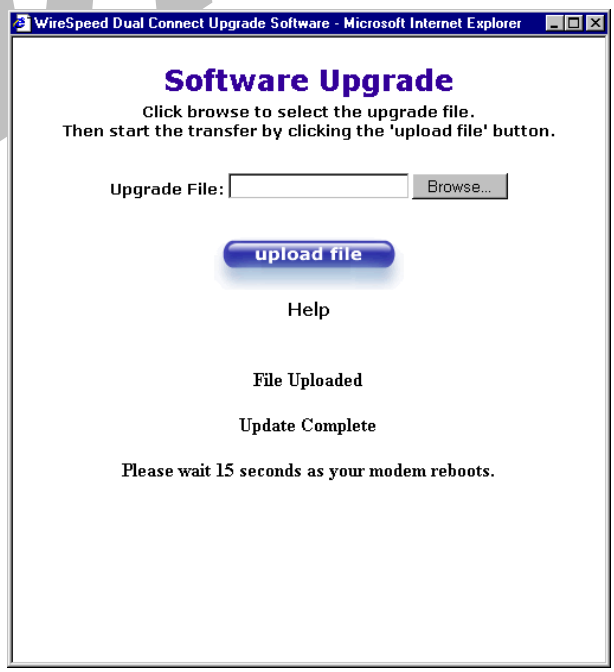


The screens below show that the file upload has completed and that the Programming Flash is being erased to prepare the Flash storage area for upload of the new file. (Programming Flash is a temporary storage area for uploaded files.)

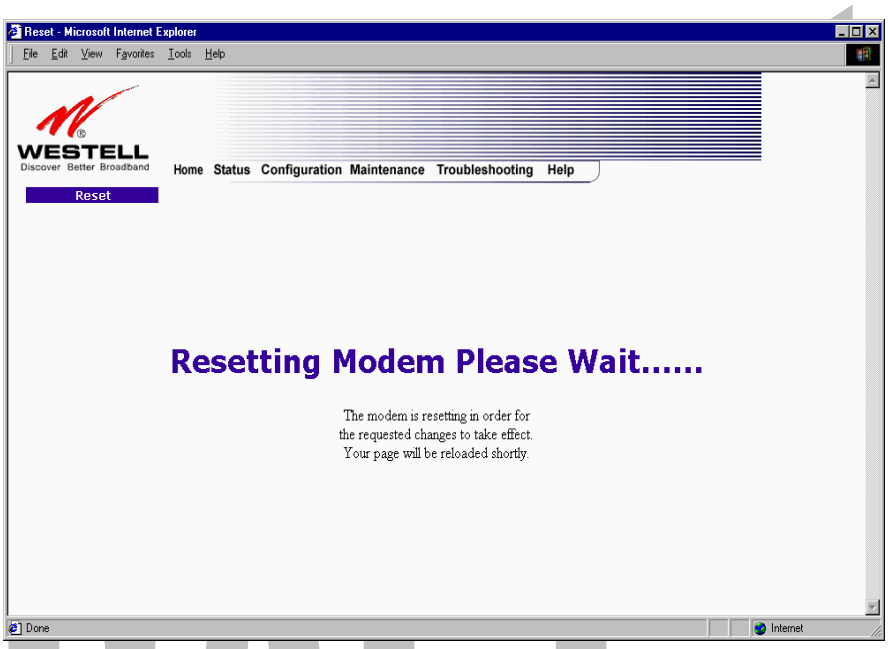




The screen below shows that the upload was successful. The Media Gateway Communications Subsystem will now reboot.

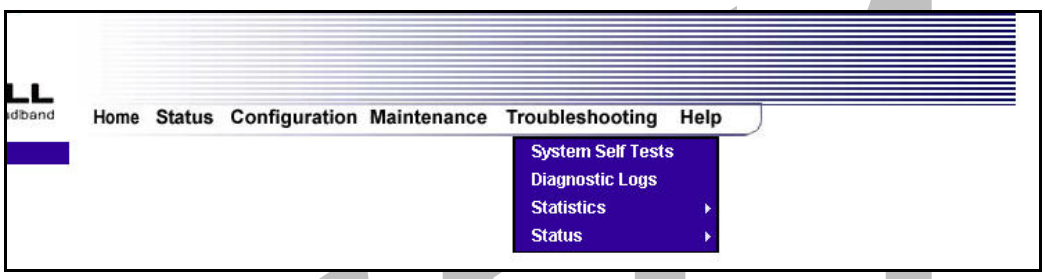


The following screen will be displayed as Media Gateway is being reset.



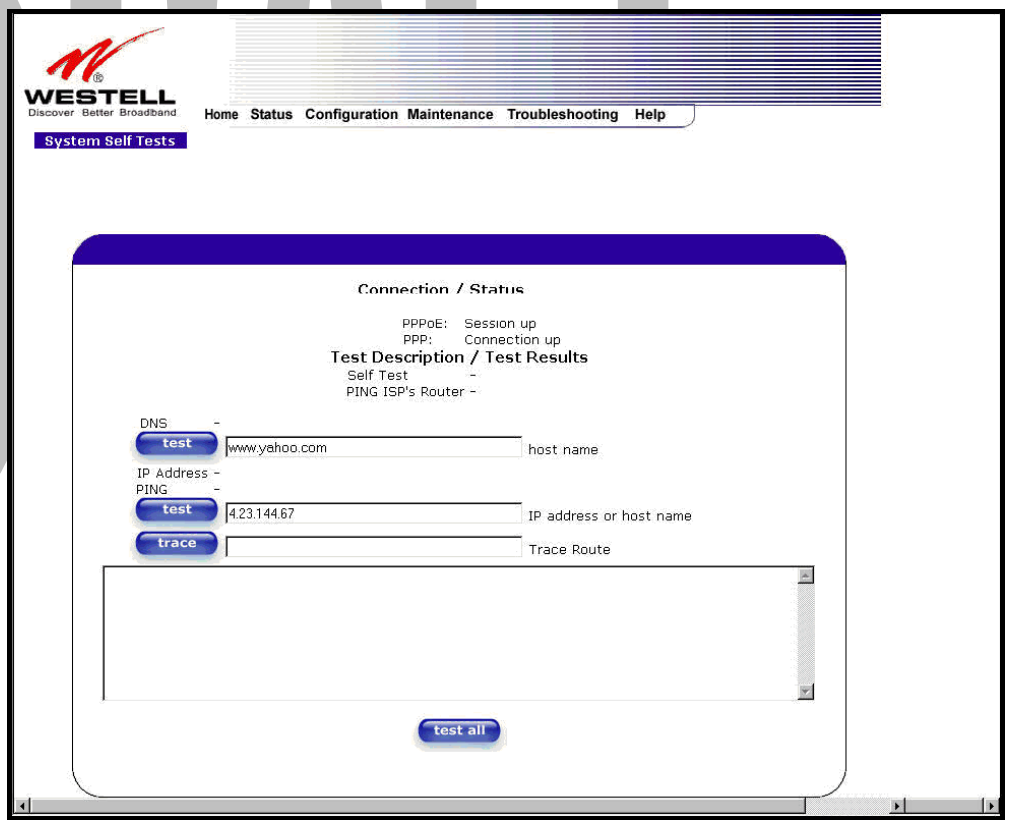
After a brief delay, the home page will be displayed. Confirm that the PPP Status displays **UP.** (Click on the **reset** button to re-establish your PPP session.)

16. TROUBLESHOOTING



16.1 System Self Tests

The following settings will be displayed if you select **System Self Tests** from the **Troubleshooting** menu. Click on **test all** to run a diagnostic test on the Media Gateway's connection.



If you want to PING using the System Self Test screen (diagnostics page) shown above, enter your **DNS** or **IP** address in the fields provided and click on the **test** button. The System Self Test will run a diagnostic test that executes independent of firewall security settings. See the following table for test descriptions and possible responses.

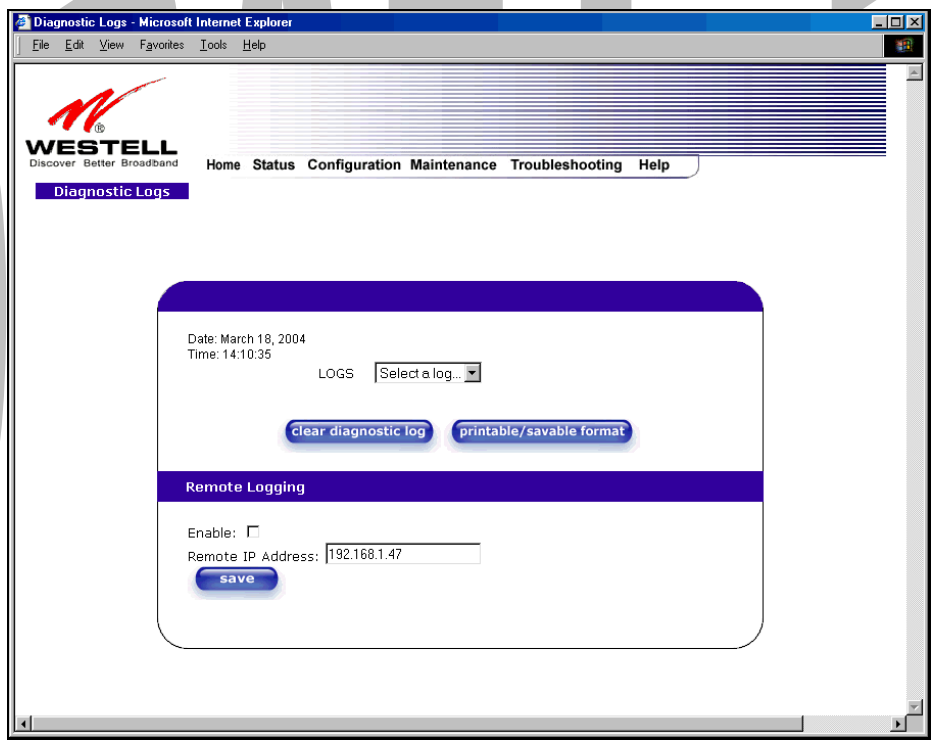
If you want to PING using the MS-DOS (shell) window, first you will need to check your firewall security setting. (If you PING via DOS shell you are susceptible to firewall rules, as this PING is dependent on the Media Gateway's firewall settings.) If your firewall is set to **Medium** or **High**, you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

Connection/Status	
PPPoE	Indicates that a PPPoE session is or is not established. Possible responses are: Session UP: A valid PPPoE session has been detected. No Session: Currently there is no active PPPoE session established. Initiating Session: A PPP session must be connected from the homepage screen.
PPP	Indicates that a PPPoE or PPPoA session must already be established. Possible responses are: Connection UP: Media Gateway has established a connection No Connection: There is no PPP connection Initiating Connection: The PPP connection process has been initiated Connection Halted: A successful PPP connection was halted Cannot Connect: A PPP connection could not be made because of a PPPoE session failure. Authorization Failure: The user name or password is incorrect. Link Control Protocol Failed: Re-establish the session (from the home page).
Test Description / Test Results	
Self Test	Performs an integrity check of certain internal components of your Gateway.
PING your ISP's system	Performs an IP network check (i.e., an IP Ping) of your ISP's system. This test verifies that Media Gateway can exchange IP traffic with an entity on the other side of the Internet connection. Possible responses are: Success: Media Gateway has detected an IP Remote connection. No Response: The IP Remote system does not answer the IP Ping. Could not test: The test could not be executed due to Media Gateway settings. Check your PPP session. You must have a PPP connection established to execute a PING.
DNS	Performs a test to try to resolve the name of a particular host. The host name is entered in the input box. Possible responses are: Success: Media Gateway has successfully obtained the resolved address. The IP address is shown below the host name input box. No Response: Media Gateway has failed to obtain the resolved address. Host not found: The DNS Server was unable to find an address for the given host name. No data, enter host name: No host name is specified. Could not test: The test could not be executed due to Media Gateway settings. Check your PPP session. You must have a PPP connection established to execute a PING.
IP Address	IP Address of the Host Name.
PING (via IP Address or Host Name)	Performs an IP connectivity check to a remote computer either within or beyond the Media Gateway's network. You can PING a remote computer via the IP address or the DNS address. If your PING fails, try a different IP or DNS address.

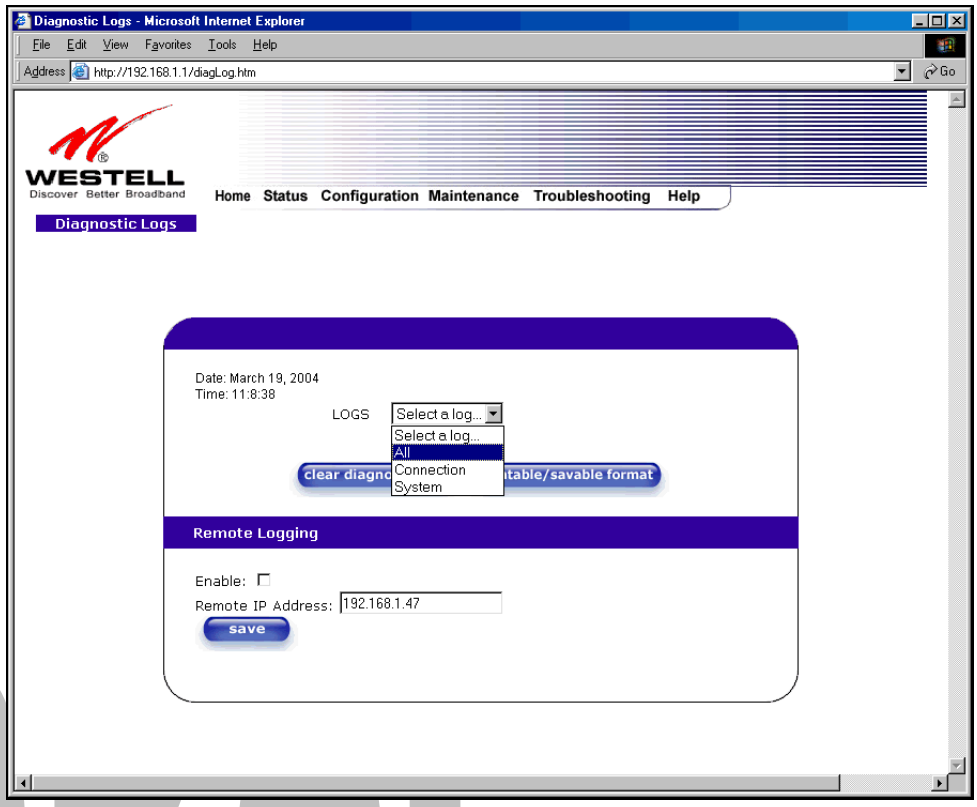
	Possible responses are: Success: The Remote Host computer was detected. No Response: There was no response to the Ping from the remote computer. No name or address to PING: No host name or IP address was specified. Could not test: The test could not be executed due to Media Gateway settings. Check your PPP session. You must have a PPP connection established to execute a PING.
Trace	Determines the route taken to destination by sending Internet Control Message Protocol (ICMP) echo packets with varying IP Time-To-Live (TTL) values to the destination. Trace Route is used to determine where the packet is stopped on the network.

16.2 Diagnostic Logs

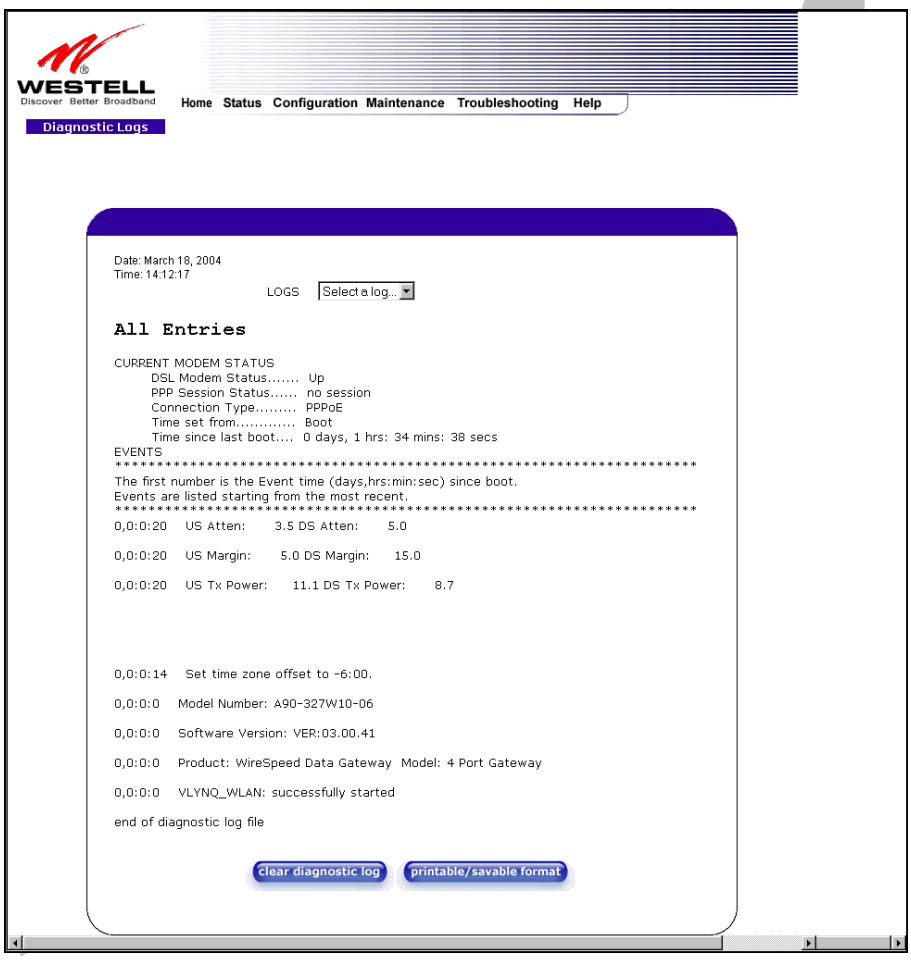
If you select **Diagnostic Log**, from the **System Self Test** menu, the following screen will be displayed.



To see a list of the log options, click on the arrow at the **LOGS** drop-down menu. Select an option from the list provided at the **Diagnostics Logs** screen.

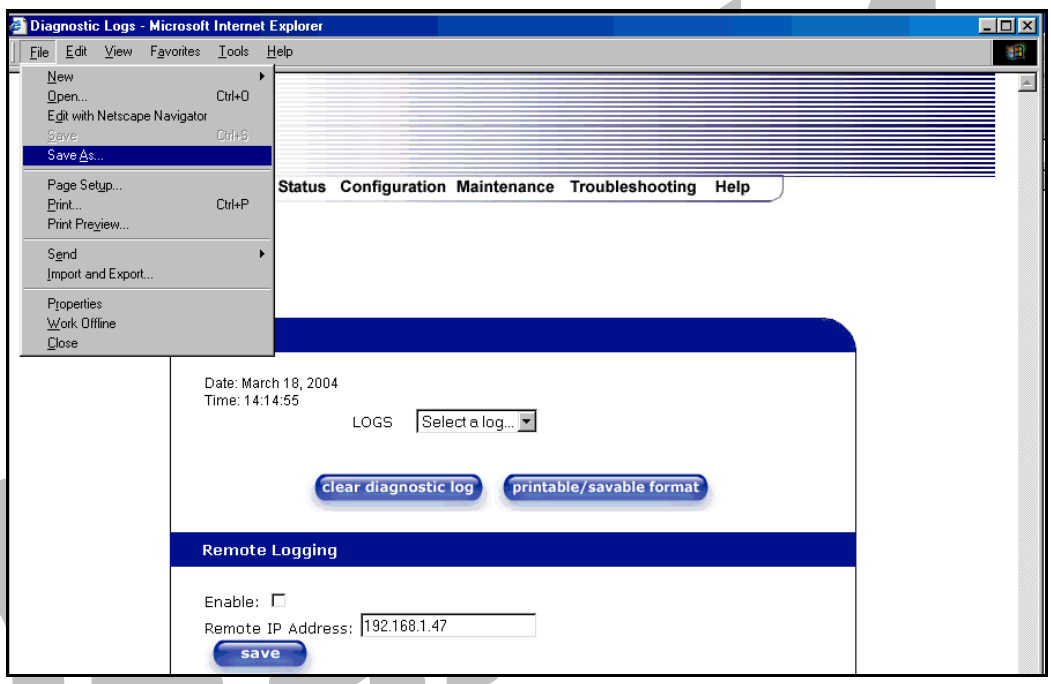

Diagnostic Logs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.1.1/diagLog.htm
Go
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Diagnostic Logs
Date: March 19, 2004
Time: 11:8:38
LOGS
Select a log...
Select a log...
All
Connection
System
clear diagno
table/savable format
Remote Logging
Enable:
Remote IP Address:
192.168.1.47
save

If you clicked on **All,** the following screen will be displayed. This screen provides a detailed list of the Media Gateway's connection status and system information. Click on **clear diagnostic log** to clear the diagnostic log information.

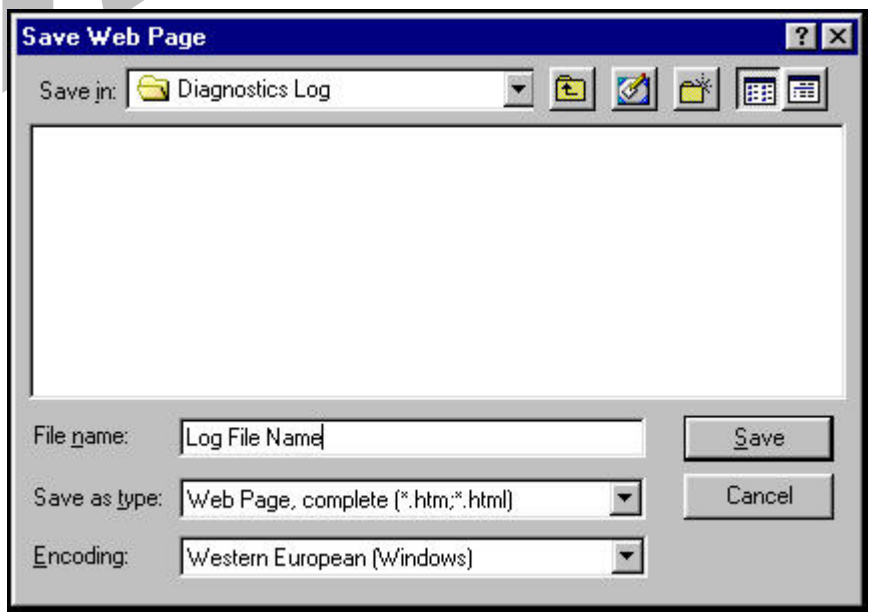


16.2.1 Saving the Diagnostic Log File

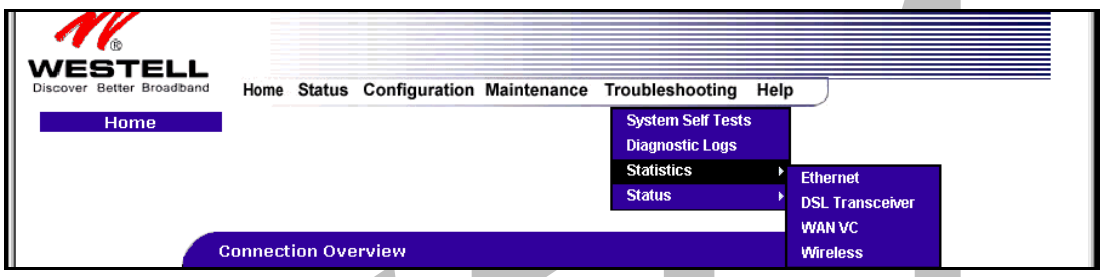
If you want to save the diagnostic log file, go to your Browser's menu and select **File,** then select **Save As** from the drop-down menu.



At the **Save Web Page** dialog box, select a destination for your log file from the **Save in** drop-down arrow. Next, enter a name for your log file in the field labeled **File name** and click on **Save**.

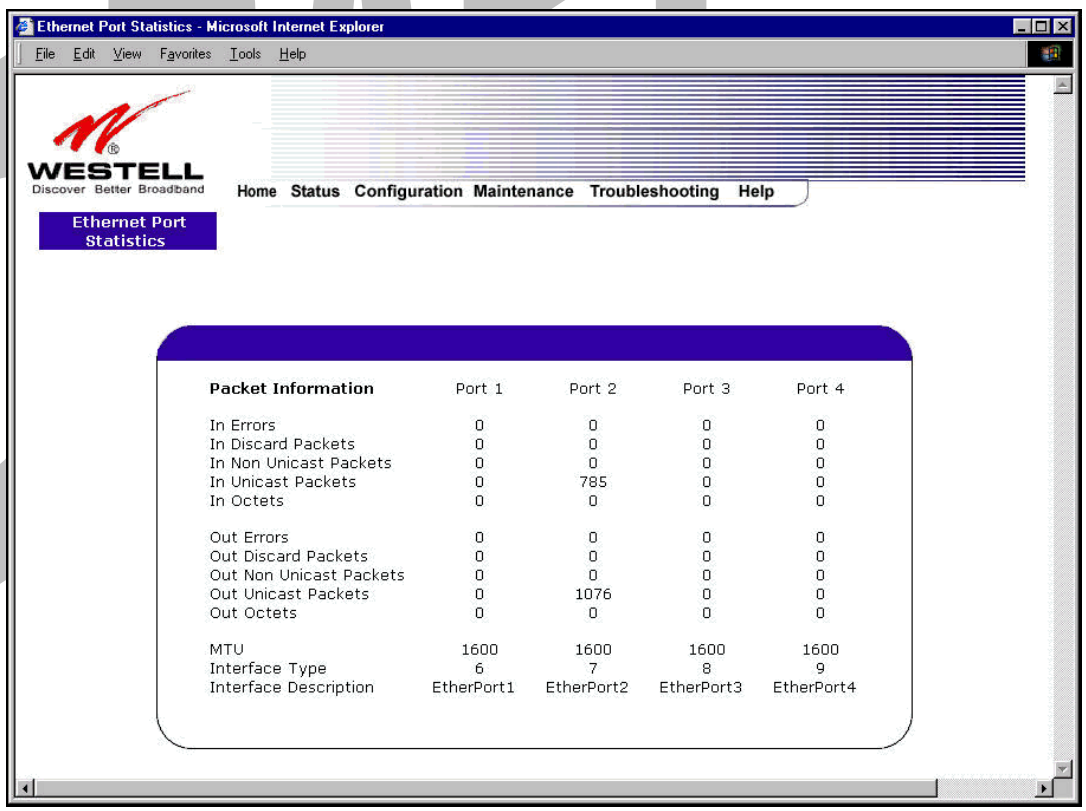


16.3 Statistics



16.3.1 Ethernet Port Statistics

The following settings will be displayed if you select **Ethernet** from the **Statistics** menu.



Packet Information	Port 1	Port 2	Port 3	Port 4
In Errors	0	0	0	0
In Discard Packets	0	0	0	0
In Non Unicast Packets	0	0	0	0
In Unicast Packets	0	785	0	0
In Octets	0	0	0	0
Out Errors	0	0	0	0
Out Discard Packets	0	0	0	0
Out Non Unicast Packets	0	0	0	0
Out Unicast Packets	0	1076	0	0
Out Octets	0	0	0	0
MTU	1600	1600	1600	1600
Interface Type	6	7	8	9
Interface Description	EtherPort1	EtherPort2	EtherPort3	EtherPort4

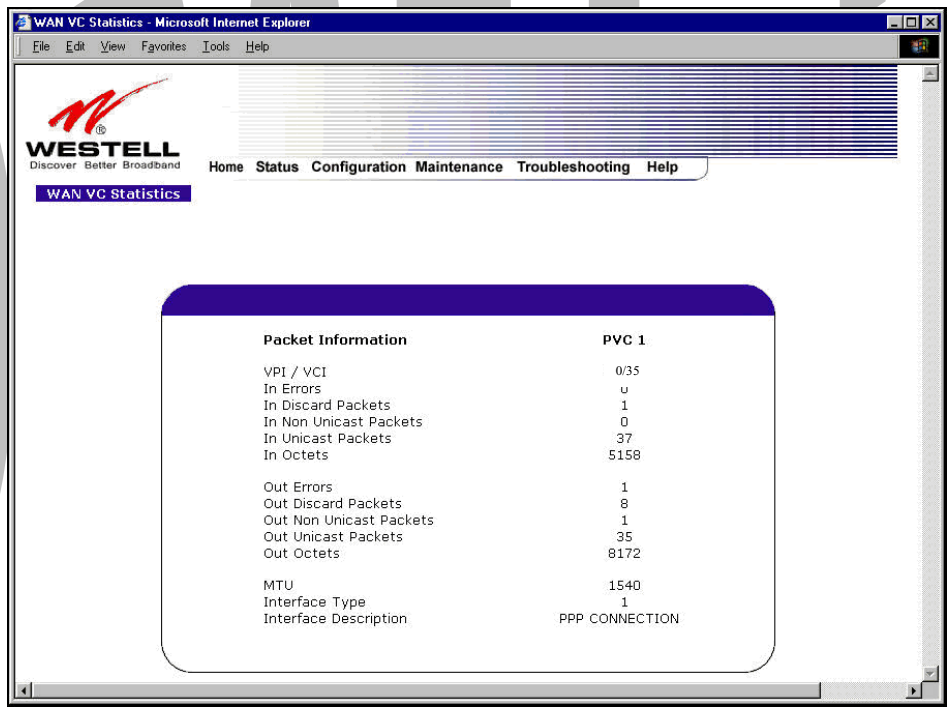
In Errors	The number of error packets received on the Ethernet interface.
In Discard Packets	The number of discarded packets received.
In Non Unicast Packets	The number of non-Unicast packets received on the Ethernet interface.
In Unicast Packets	The number of Unicast packets received on the Ethernet interface.

In Octets	The number of bytes received on the Ethernet interface.
Out Errors	The number of outbound packets that could not be transmitted due to errors.
Out Discard Packets	The number of outbound packets discarded.
Out Non Unicast Packets	The number of non-Unicast packets transmitted on the Ethernet interface.
Out Unicast Packets	The number of Unicast packets transmitted on the Ethernet interface.
Out Octets	The number of bytes transmitted on the Ethernet interface.
MTU	Maximum Transmission Unit- The number of data bytes contained in the Ethernet frame.
Interface Type	A unique identifier that represents the interface type.
Interface Description	A description field that refers to the interface type.

16.3.2 WAN VC Statistics

The following settings will be displayed if you select **WAN VC** from the **Statistics** menu.

NOTE: If Media Gateway is configured using **ETHERNET PORT 1**, the following screen will not be available.

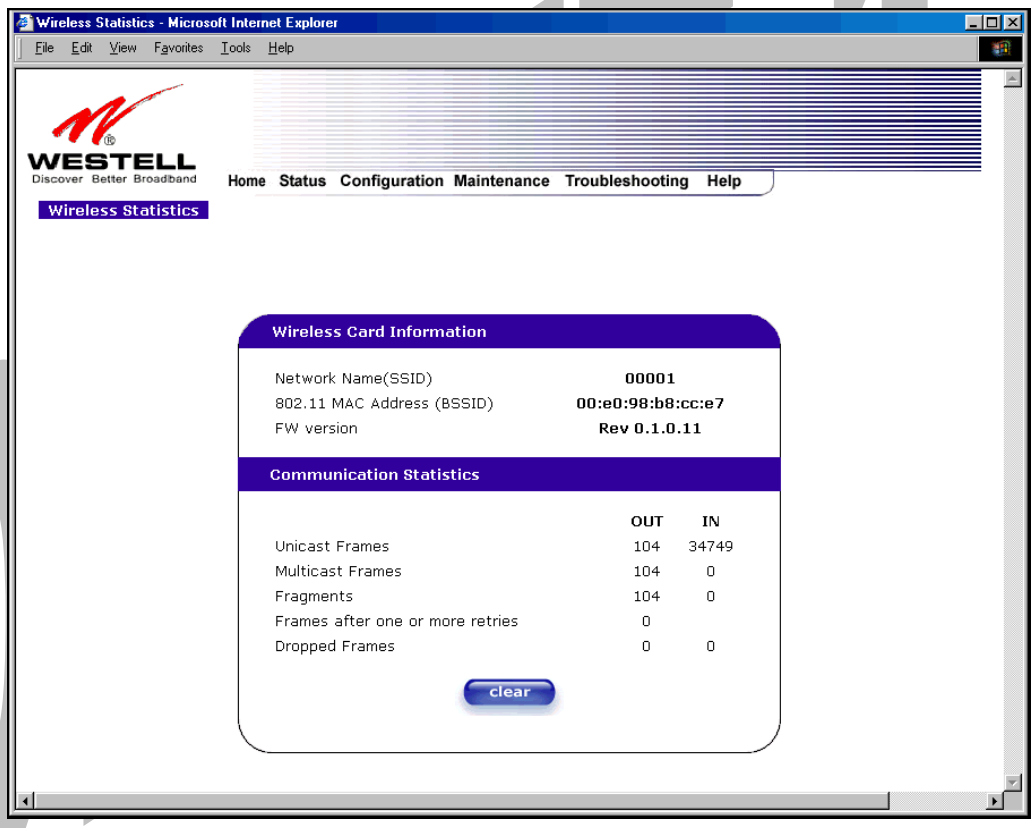


VPI/VCI	Displays the VPI/VCI values obtained from your ISP.
In Errors	The number of error packets received on the ATM port.
In Discard Packets	The number of discarded packets received.
In Non Unicast Packets	The number of non-Unicast packets received on the ATM port.
In Unicast Packets	The number of Unicast packets received on the ATM port.
In Octets	The number of bytes received on the ATM port.
Out Errors	The number of outbound packets that could not be transmitted due to errors.
Out Discard Packets	The number of outbound packets discarded.
Out Non Unicast Packets	The number of non-Unicast packets transmitted on the ATM port.
Out Unicast Packets	The number of Unicast packets transmitted on the ATM port.
Out Octets	The number of bytes transmitted on the ATM port.
MTU	Maximum Transmission Unit -The number of data bytes contained in the ATM frame.

Interface Type	A unique identifier that represents the interface type.
Interface Description	A description field that refers to the interface type.

16.4 Wireless Statistics

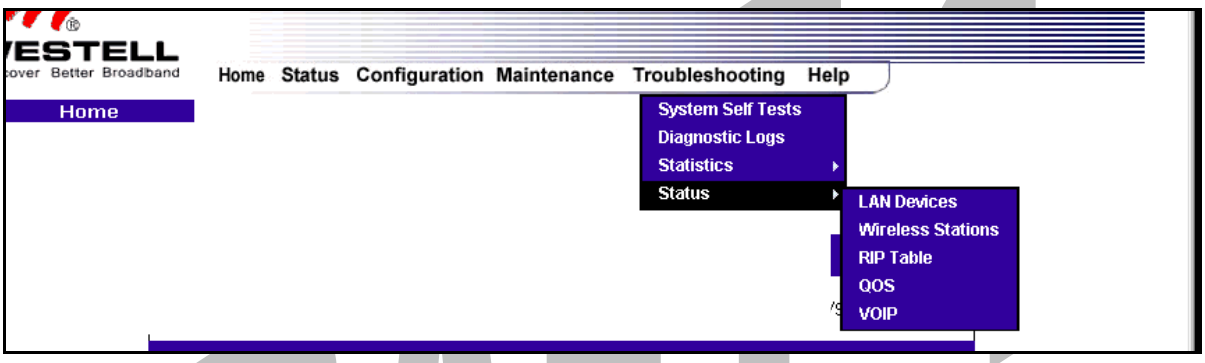
The following settings will be displayed if you select **Wireless** from the **Statistics** menu.



Wireless Card Information	
Network Name (SSID)	This string, (32 characters or less) is the name associated with the Access Point (AP). To connect to the AP, the Service Set ID (SSID) on a Station card must match the SSID on the AP.
802.11 MAC Address (BSSID)	This is the Media Access Controller address of the AP. It is used as the Basic Service Set Identifier (BSSID).
FW Version	This is the Network Interface Card Identifier. It uniquely identifies the hardware platform of the AP. This is used with other information to determine if the inserted card can be used as an AP, and if so, the version of AP firmware to be used. Not all makes of wireless station cards can be used as an AP.
Communication Statistics	
NOTE: Data preceded by **OUT** pertain to transmissions from Media Gateway to a station; Media Gateway is the source. Data preceded by **IN** pertain to data received by the Media Gateway; Media Gateway is the destination.	
OUT-Unicast Frames	The number of successfully transmitted frames whose destination address

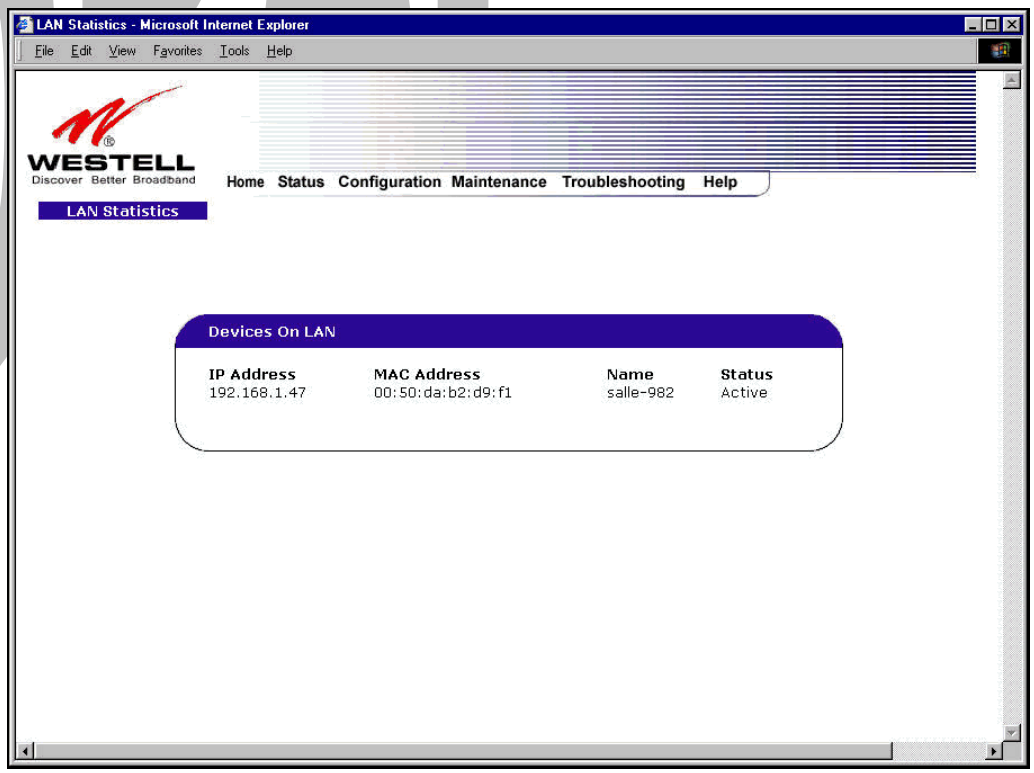
	was a single station; not necessarily the same station, but to any single station as opposed to a transmission that multiple stations would receive-as in the case of broadcast message.
OUT-Multicast Frames	The number of successfully transmitted frames whose destination address was a multicast address (received by more that one station): not necessarily broadcast to all stations, but more than a single station. Broadcast messages are included in the count.
OUT-Fragments	The number of successful transmissions made. This will typically be greater than the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable).
OUT-Frames after one or more retries	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
OUT-Dropped Frames, too many retries	The number of frames that did not transmit due to the short or long retry limit being reached because no acknowledgement or CTS was received.
IN-Unicast Frames	The number of successfully received frames whose destination address was a single location, not necessarily the same location, but to any single location as opposed to the broadcast address.
IN-Multicast Frames	The number of successfully received frames whose destination address was a multicast address. Broadcast messages are included in this count.
IN-Fragments	The number of fragments successfully received. This may not be equal to the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable) on the source station.
IN-Frames after one or more retrie	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
IN-Drops due to insufficient Rx buffers	The number of received frames discarded due to lack of buffer space.

16.5 Status



16.5.1 LAN Devices

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



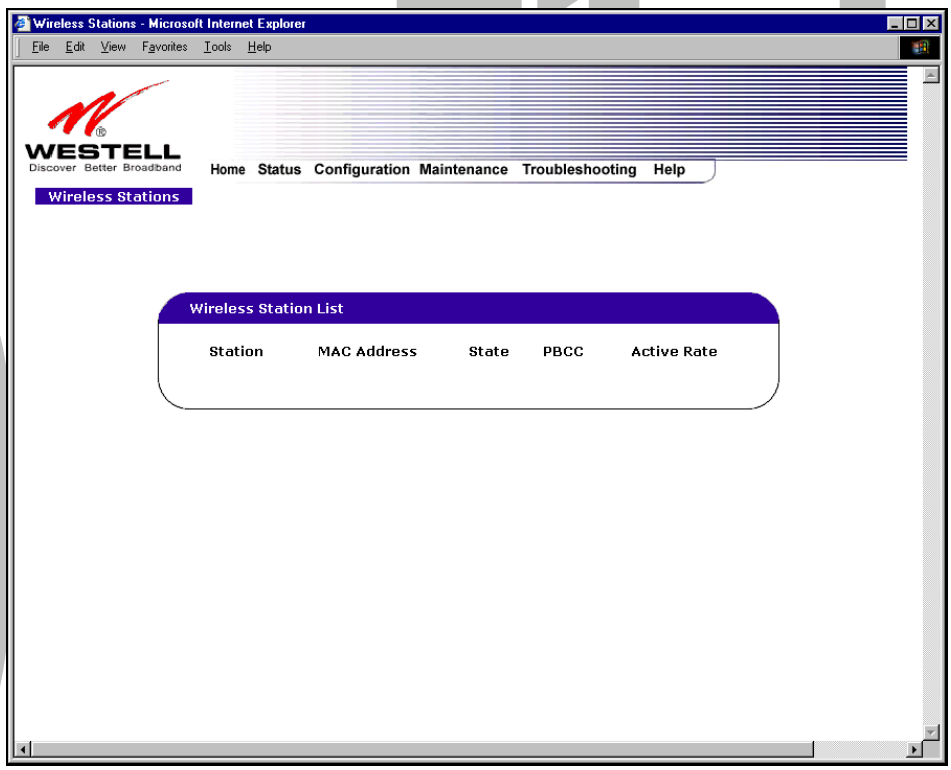
Devices on LAN	
IP Address	Displays the IP network address that Media Gateway is on.

MAC Address	Media Access Controller (MAC) address of this device.
Name	Displays the ASCII (text) name of the devices connected to the LAN.
Status	Displays the status of the devices connected to the LAN.

16.5.2 Wireless Stations

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

NOTE: A Wireless device must be connected to Media Gateway for the fields in this screen to be populated.

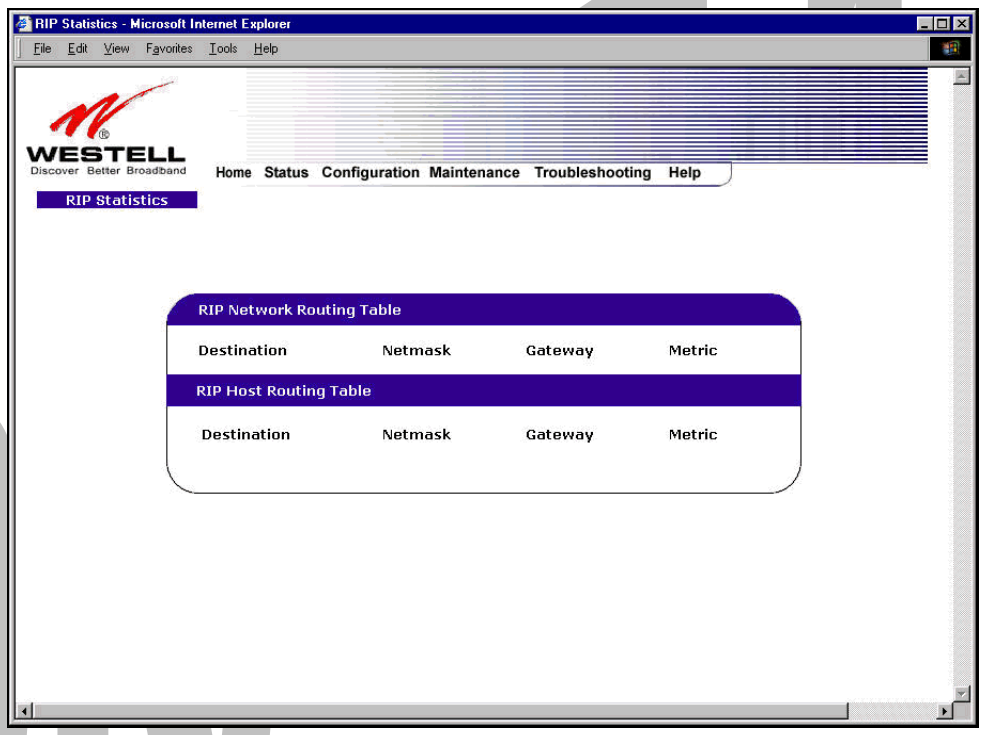


Wireless Stations List	
Station	This number indicates the order in which the stations are first accessed by the Gateway.
MAC Address	The Media Access Controller Address assigned to the station.
State	The current state of the negotiation between the station and the Media Gateway.
PBCC	Indicates whether the station that is associated with Media Gateway operates in PBCC (Packet Binary Convolutional Code) modulation.
Active Rate	The current transmit and receive rate.

16.5.3 RIP Table

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

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

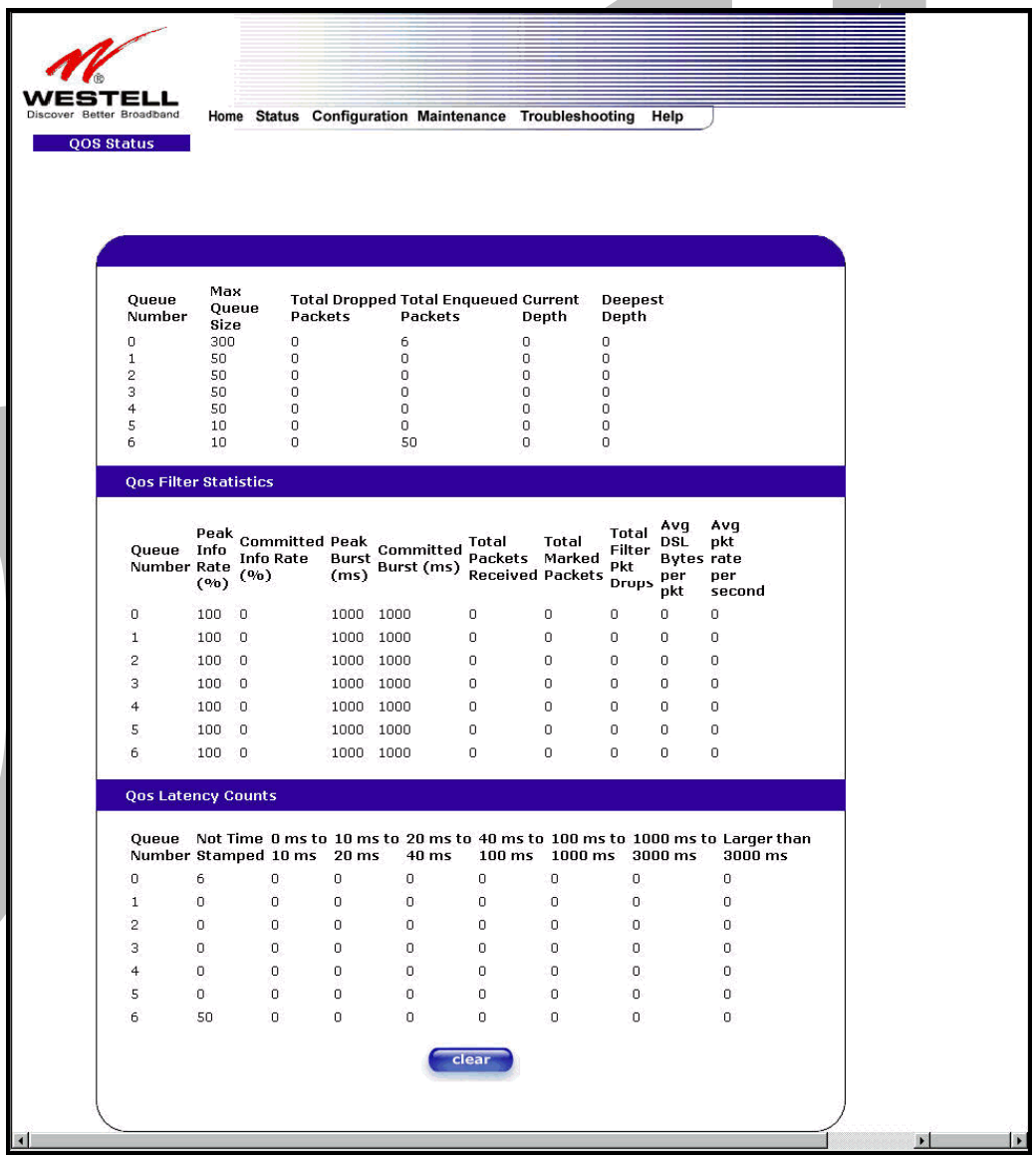


RIP Network Routing Table	Indicates Network routes received via RIP.
RIP Host Routing Table	The Host routes received via RIP.
Destination	The destination IP address of the route
Netmask	The IP mask of the route
Gateway	The gateway of the route
Metric	The RIP metric (0-15). A lower value is better.

16.5.4 QOS Status

The following settings will be displayed if you select **QOS** from the **Status** menu. Click on the **clear** button to clear all counts and statistics (not just latency counts). This does not affect the configuration values.

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



Queue Number	Max Queue Size	Total Dropped Packets	Total Enqueued Packets	Current Depth	Deepest Depth
0	300	0	6	0	0
1	50	0	0	0	0
2	50	0	0	0	0
3	50	0	0	0	0
4	50	0	0	0	0
5	10	0	0	0	0
6	10	0	50	0	0

Queue Number	Peak Info Rate (%)	Committed Info Rate (%)	Peak Burst (ms)	Committed Burst (ms)	Total Packets Received	Total Marked Packets	Total Filter Pkt Drops	Avg DSL Bytes per pkt	Avg pkt rate per second
0	100	0	1000	1000	0	0	0	0	0
1	100	0	1000	1000	0	0	0	0	0
2	100	0	1000	1000	0	0	0	0	0
3	100	0	1000	1000	0	0	0	0	0
4	100	0	1000	1000	0	0	0	0	0
5	100	0	1000	1000	0	0	0	0	0
6	100	0	1000	1000	0	0	0	0	0

Queue Number	Not Time Stamped	0 ms to 10 ms	10 ms to 20 ms	20 ms to 40 ms	40 ms to 100 ms	100 ms to 1000 ms	1000 ms to 3000 ms	Larger than 3000 ms
0	6	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	50	0	0	0	0	0	0	0

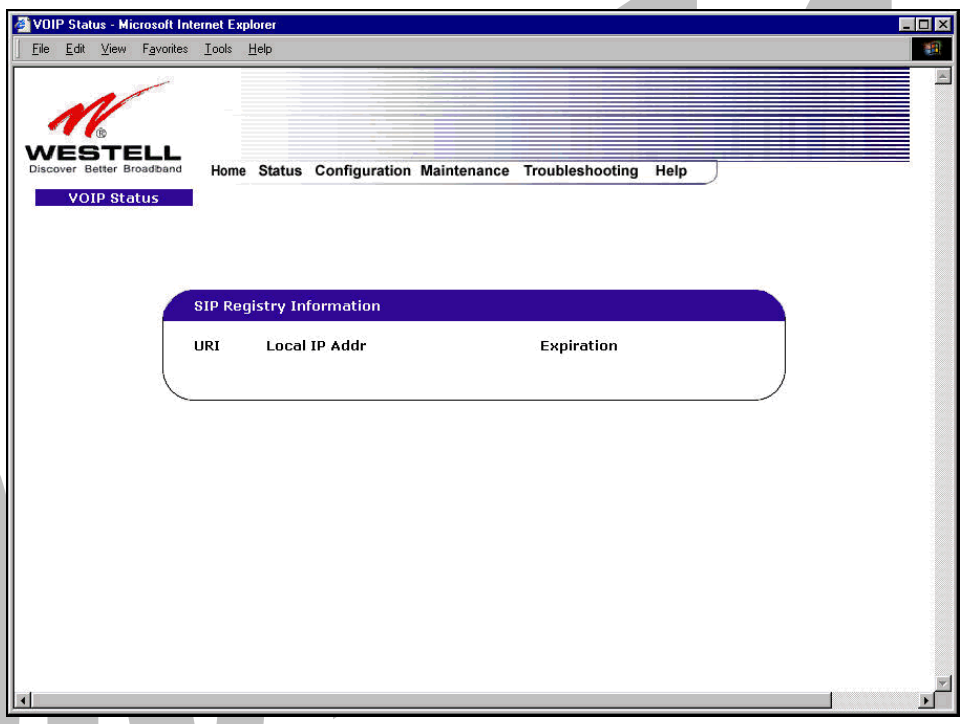
Queue Number	Indicates the DiffServ Queue. Possible responses are: 0 = Best Effort (BE) 1 = Assured Forwarding 1 (AF1) 2 = Assured Forwarding 2 (AF2) 3 = Assured Forwarding 2 (AF3) 4 = Assured Forwarding 2 (AF4)

	5 = Expedited Forwarding (EF) 6 = Routing Protocols (DiffServ priorities 6 and 7)
Max Queue Size	The maximum number of packets that can be queued for this priority.
Total Dropped Packets	Indicates how many packets of this priority have been dropped by QOS due to lack of buffer space or filtering rules.
Total Enqueued Packets	Displays the number of packets, destined for the WAN, that have been received.
Current Depth	Displays the current number of packets of this priority that are queued.
Deepest Depth	Displays the most number of packets that have been queued at once for this priority.
QOS Filter Statistics	
Queue Number	The DiffServ Queue. (See Queue Number description above.)
Peak Info. Rate (%)	The maximum allowed rate for this priority.
Committed Info Rate (%)	The committed rate for this priority.
Peak Burst (ms)	Displays the interval in milliseconds for averaging the peak offered rate.
Committed Burst (ms)	Displays the interval in milliseconds for averaging the committed offered rate.
Total Packets Received	Displays the total number of packets of this priority that are destined for the LAN.
Total Marked Packets	Displays the number of packets of this priority that exceeded the committed rate, but not the peak rate, and were marked with a higher drop priority
Total Filter Packet Drops	Displays the number of packets of this priority that exceeded the peak rate and that were, therefore, dropped.
Avg. Bytes Per Packet	Displays the average size of packets for this priority, including all overhead.
Avg. Packet Rate Per second	Displays the average rate (in packets per seconds) for this priority.
QOS Latency Counts	
Queue Number	The DiffServ Queue. (See Queue Number description above.)
Not Time Stamped	The packets with no incoming time stamp. (Often these are generated internal to the modem.)
A ms to B ms	The number of packets of this priority whose time in the modem fell between A and B milliseconds. (Time is measured from the point the packet arrives at the modem's processor until is passed to the ATM hardware for transmission.) Possible ranges are (A ms to B ms): 0 ms to 10 ms 10 ms to 20 ms 20 ms to 40 ms 40 ms to 100 ms 100 ms to 1000 ms 1000 ms to 3000 ms Larger than 3000 ms

16.5.5 VOIP Status

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

NOTE: A VOIP device must be connected to Media Gateway for this table to be populated.



SIP Registry Information	
URI	The SIP URI that is trying to register. (This field only indicates that a SIP device tried to register, not that it succeeded.)
Local IP Address	The local, LAN IP address of the SIP device.
Expiration	Indicates how long (in seconds) until the registration expires.

17. NAT SERVICES

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

NOTE: To configure Media Gateway for a service or application, follow the steps in section 14 (Setting Up Advanced Service Configuration) of this User Guide.

Applications/Games/VPN Support

Application/Game	Port/Protocol
Aliens vs. Predator	80 UDP, 2300 UDP, 8000-8999 UDP
America Online	5190 TCP/UDP
AoE II: Conquors	47624 TCP/UDP, 6073 TCP/UDP, 2300-2400 TCP/UDP
AOL Instant Messenger	4099 TCP, 5190 TCP
Asheron's Call	9000-9013 UDP, 28800-29000 TCP
Battlecom	2300-2400 TCP/UDP, 47624 TCP/UDP
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

Application/Game	Port/Protocol
	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 TCP6700-6702 TCP, 6880 TCP, 1200-16090 TCP
IMAP	119 TCP/UDP
IMAP v.3	220 TCP/UDP
Internet Phone	22555 UDP
IPSEC ESP	PROTOCOL 50
IPSEC IKE	500 UDP
Ivisit	9943 UDP, 56768 UDP
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

Application/Game	Port/Protocol
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
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
Roger Wilco	TCP/UDP 3782 UDP 3783 (BaseStation)
ShoutCast Server	8000-8005 TCP
SSH Secure Shell	22 TCP/UDP
Starcraft	2346 TCP
Starfleet Command	2300-2400 TCP/UDP, 47624 TCP/UDP
Telnet	23 TCP
Tiberian Sun & Dune 2000	1140-1234, 4000 TCP/UDP
Ultima Online	5001-5010 TCP, 7775-7777 TCP, 8800-8900 TCP, 9999 UDP, 7875 UDP

Application/Game	Port/Protocol
Unreal Tournament server	7777 (default gameplay port) 7778 (server query port 7779,7779+ are allocated dynamically for each helper UdpLink objects, including UdpServerUplin 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 modem from the Gateway.
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)
XBOX Live	TCP/UDP 88 and 3074
Yahoo Messenger Chat	5000-5001 TCP
Yahoo Messenger Phone	5055 UDP
VPN Protocol	**Comments**
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. TECHNICAL SUPPORT INFORMATION

Contact your ISP's customer service representative for technical support on this product.

19. PRODUCT SPECIFICATIONS

Protocol Features

- Bridge Encapsulation per RFC2684 (Formerly RFC1483)
- Logical Link Control/Subnetwork
- Access Protocol (LLC/SNAP)
- Software Upgradeable
- PPPoE Support
- ATM SAR: Internal to Modem

System Requirements for 10/100 Base-T/Ethernet

- Pentium® or equivalent and above machines
- Microsoft Windows (98 SE, 2000, ME, NT 4.0, or XP) Macintosh OS X, or Linux installed
- Operating system CD
- Internet Explorer 4.x or Netscape Navigator 4.x or higher
- 64 MB RAM (128 MB recommended)
- Ethernet 10/100 Base-T interface
- 10 MB of free hard drive space
- TCP/IP Protocol stack installed

System Requirements for Wireless

- Pentium® or equivalent and above class machines
- Microsoft® Windows® (98 SE, 2000, ME, or XP) or Macintosh® OS X installed
- Operating System CD on hand
- Internet Explorer 4.x or Netscape Navigator 4.x or higher
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- IEEE 802.11b/g PC adapter

LEDs

- Power
- Ethernet
- Wireless
- Internet

Connectors

- Ethernet: RJ-45: 8-pin modular jack
- Power: Connector

Pin Assignments

- E1/WAN, E2, E3, E4 Port Pin Assignments

Pinout	Description
1	Rx+
2	Rx-
3	Tx+
4,5,7,8	Not Used
6	Tx-

Power

- Power Supply: External 120 VAC to 12V AC wall-mount power supply
- Power Consumption: Less than 6 watts typical, from 120 VAC

Environmental

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

EMC/Safety/Regulatory Certifications

- EMC: FCC Part 15, Class B
- UL Standard 60950, 3rd Edition
- CAN/CSA Standard C22.2 No. 60950
- UL
- CSA
- ACTA 968-A
- Industry Canada CS03

20. SOFTWARE LICENSE AGREEMENT

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

1. License Grant. Licensor hereby grants to you, and you accept, a nonexclusive license to use the Compact Disk (CD) and the computer programs contained therein in machine-readable, object code form only (collectively referred to as the "SOFTWARE"), and the accompanying User Documentation, only as authorized in this License Agreement. The SOFTWARE may be used only in connection with the number of systems for which you have paid license fees as dictated in your support agreement. You agree that you will not assign, sublicense, transfer, pledge, lease, rent, or share your rights under this License Agreement. You agree that you may not nor allow others to reverse assemble, reverse compile, or otherwise translate the SOFTWARE.

You may retain the SOFTWARE CD for backup purposes only. In addition, you may make one copy of the SOFTWARE in any storage medium for backup purposes only. You may make one copy of the User's Manual for backup purposes only. Any such copies of the SOFTWARE or the User's Manual shall include Licensor's copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the SOFTWARE or any portions thereof may be made by you or any person under your authority or control.

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

3. License Fees. The fees paid by you under the support agreement are paid in consideration of the licenses granted under this License Agreement.

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

5. Limited Warranty. Licensor warrants, for your benefit alone, for a period of 90 days from the date of commencement of this License Agreement (referred to as the "Warranty Period") that the SOFTWARE CD in which the SOFTWARE is contained are free from defects in material and workmanship. Licensor further warrants, for your benefit alone, that during the Warranty Period the SOFTWARE shall operate substantially in accordance with the functional specifications in the User's Manual. If during the Warranty Period, a defect in the SOFTWARE appears, you may return the SOFTWARE to Licensor for replacement. You agree that the foregoing constitutes your sole and exclusive remedy for breach by Licensor of any warranties made under this Agreement.

EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE SOFTWARE CD, AND THE SOFTWARE CONTAINED THEREIN, ARE LICENSED "AS IS," AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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

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

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

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

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

21. PUBLICATION INFORMATION

Westell® Media Gateway Communications Subsystem (Model WMT)
User Guide Part Number 030-300417 Rev. A

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