	LAN to use the NAT interface.
Modem IP Address	Displays VersaLink'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.

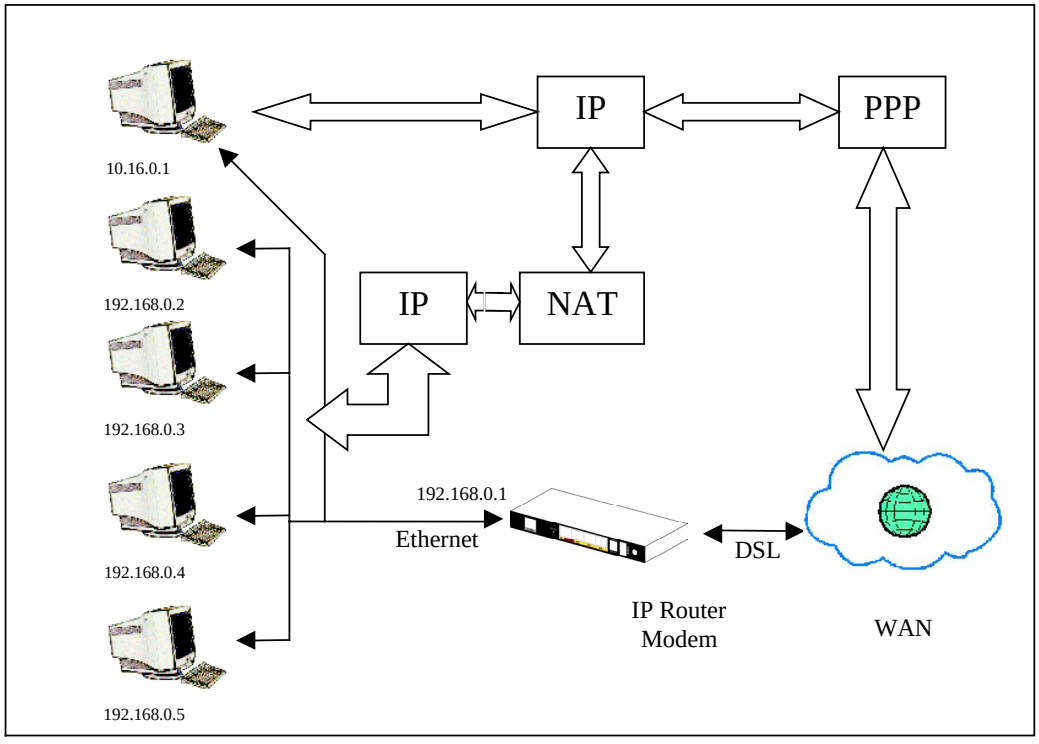
Warning Message	Check Private LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field
Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 53	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

12.5.6 Public LAN Configuration

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 service provider, allows VersaLink 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 VersaLink, your ISP must support Public LAN and Static IP. Contact your ISP for details.

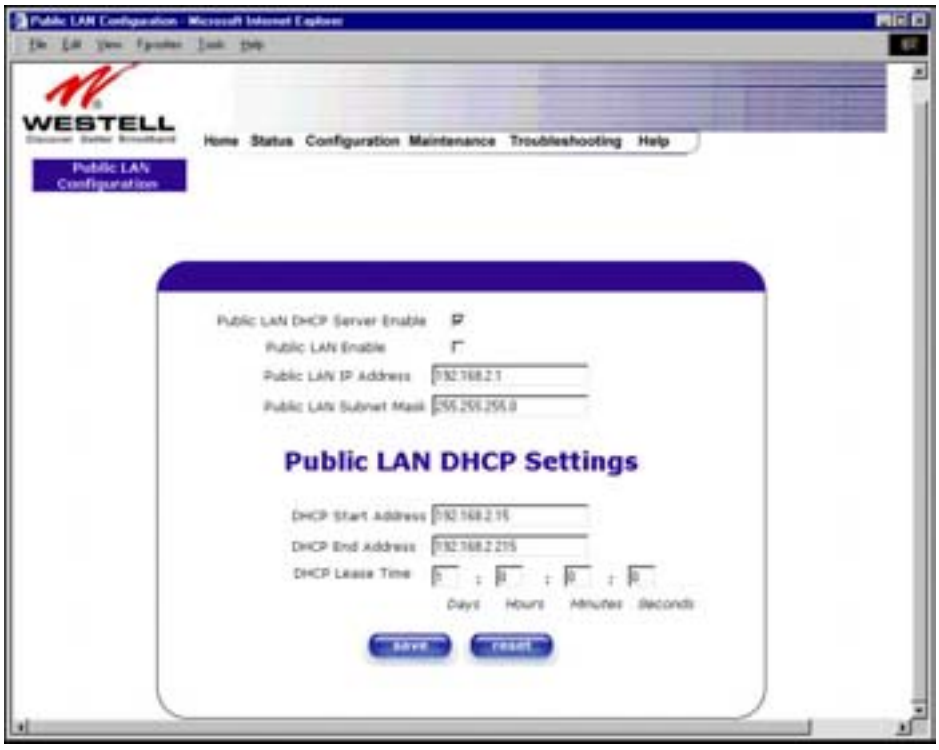
The public devices are visible on the Internet unlike a local NAT'ed PC. The example below shows four NAT'ed PCs and one global PC. The arrows show the data path for each flow.



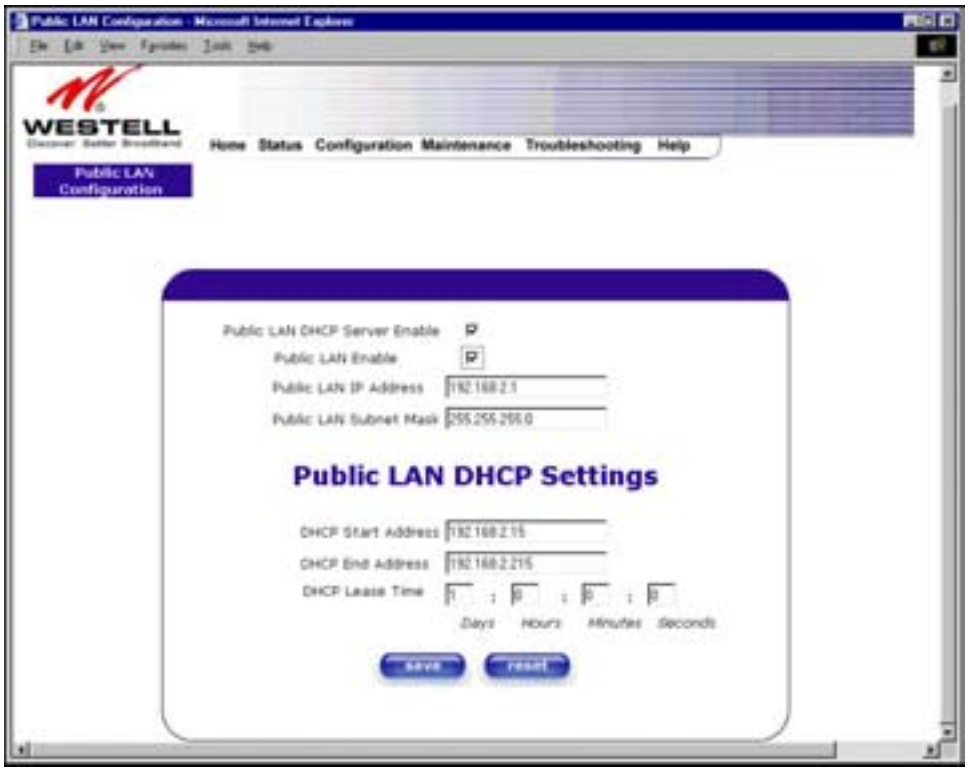
Public LAN DHCP Server Enable	Default = NOT CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Public LAN pool.
Public LAN Enable	Default = NOT CHECKED If this box is CHECKED, it enables the addresses from the Public LAN to bypass the NAT interface.
Public LAN IP Address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

If you clicked 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 DHCP Server, you automatically disable the Private LAN DHCP Server on VersaLink.



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.

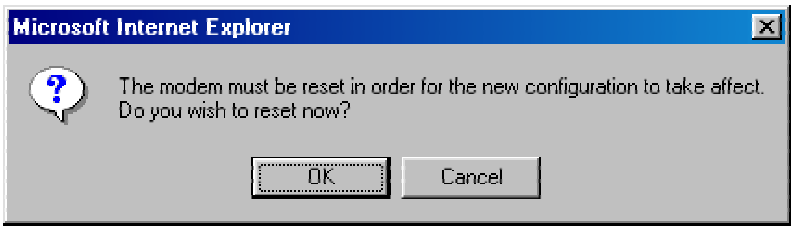
NOTE: DHCP Lease Time is displayed in the following format: (dd:hh:mm:ss)*. This value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.
*(dd = days, hh = hours, mm = minutes, ss = seconds).

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

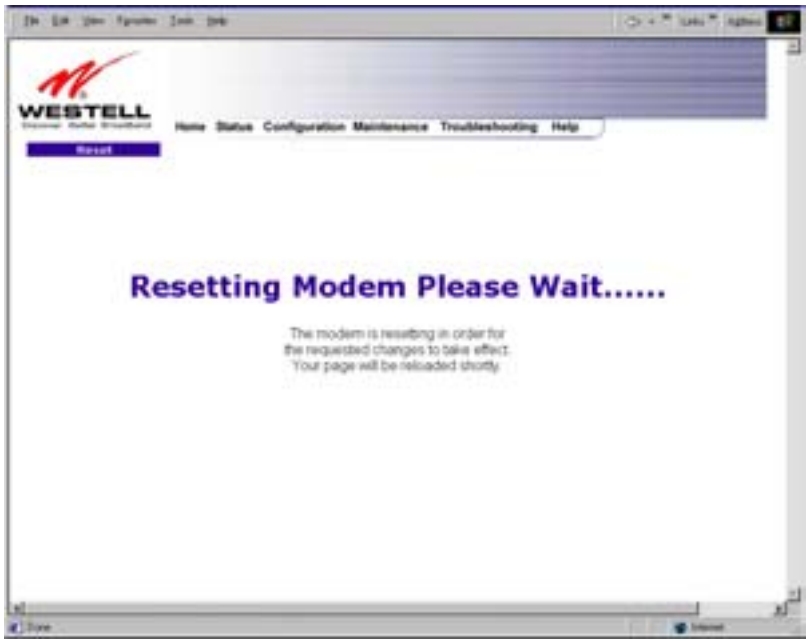
Warning Message	Check Public LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field

Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 53	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.**



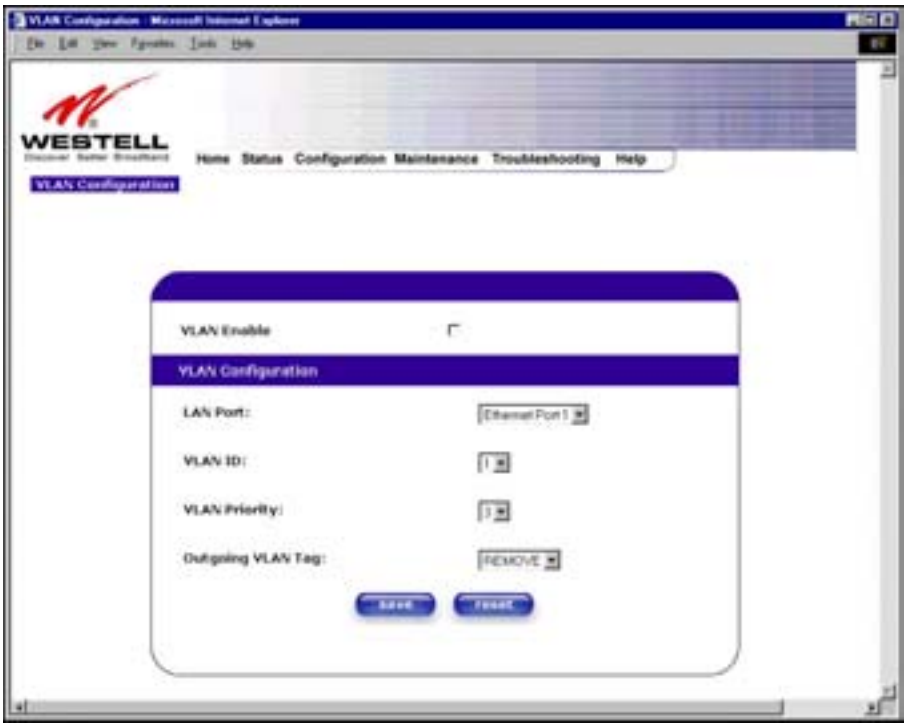
If you clicked on **OK** in the preceding screen**,** the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.



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

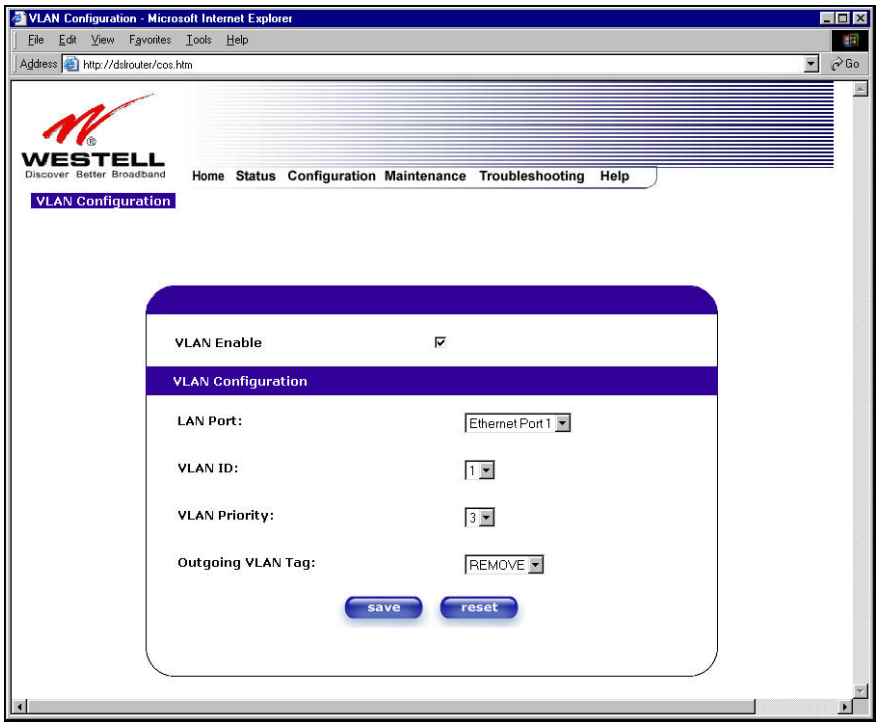
12.5.7 VLAN

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
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.

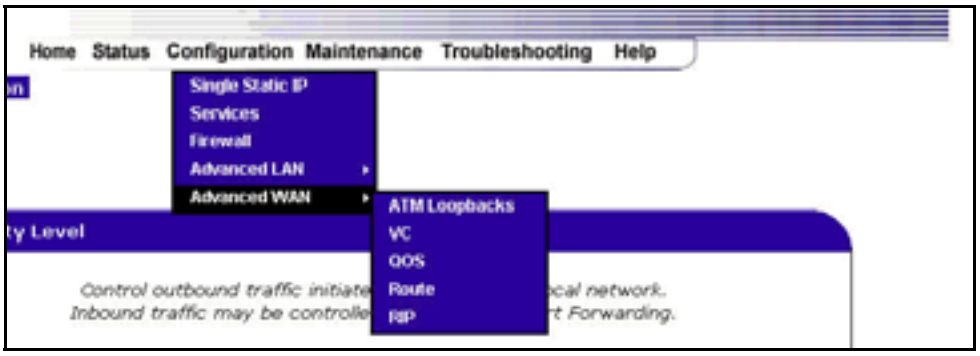
To enable VLAN click on the box adjacent to the **VLAN Enable** field. A check mark will appear in the box. Click on **save.**



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

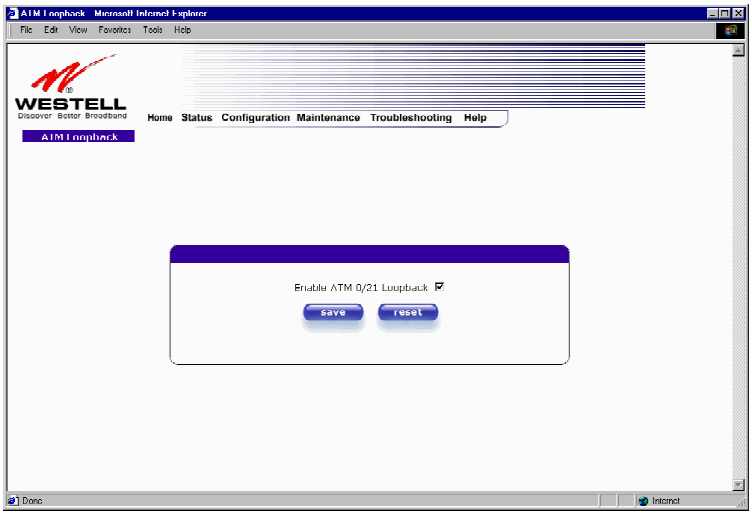
12.6 Advanced WAN

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



12.6.1 ATM Loopbacks

If you select **ATM Loopbacks** from the **Configuration** menu, the following settings will be displayed.

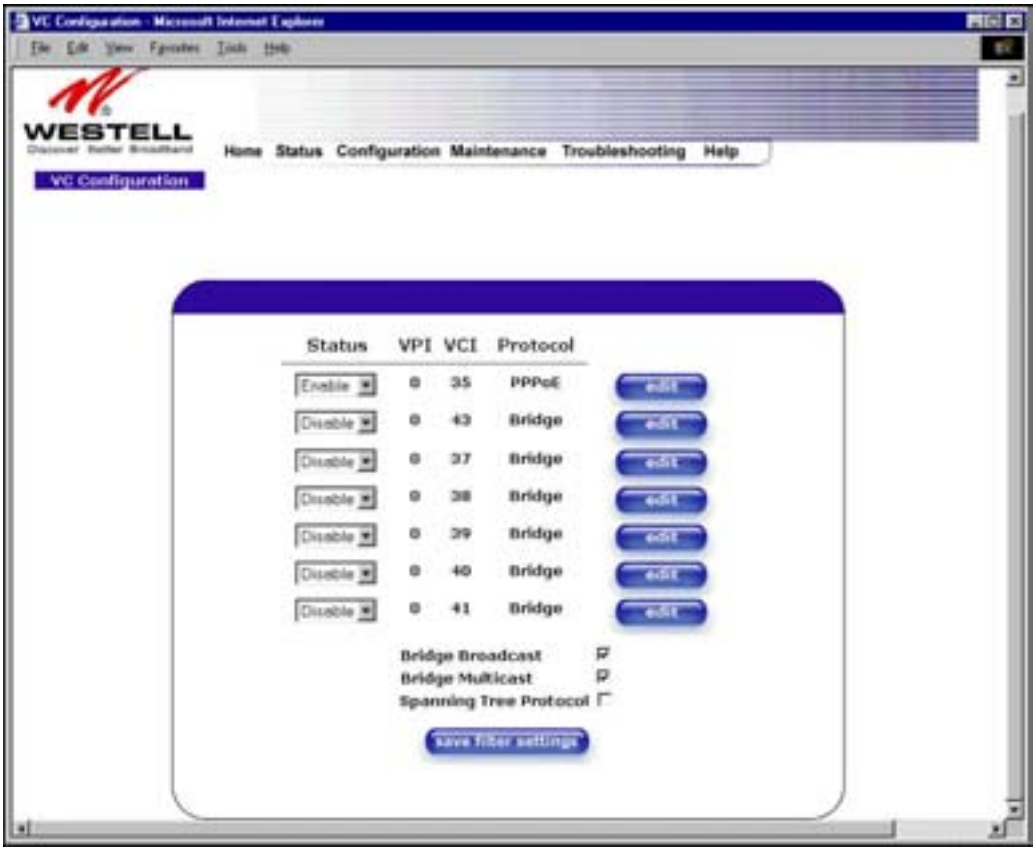


Enable ATM 0/21 Loopback:	Factory Default = ENABLED This option enables the 0/21 loopback , which is used by your ISP. NOTE: Westell does not recommend that you change this setting.

12.6.2 VC Configuration

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

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



NOTE: If you experience any problems, please reset VersaLink via the external hardware reset button or via the procedure defined under the **Maintenance** menu.

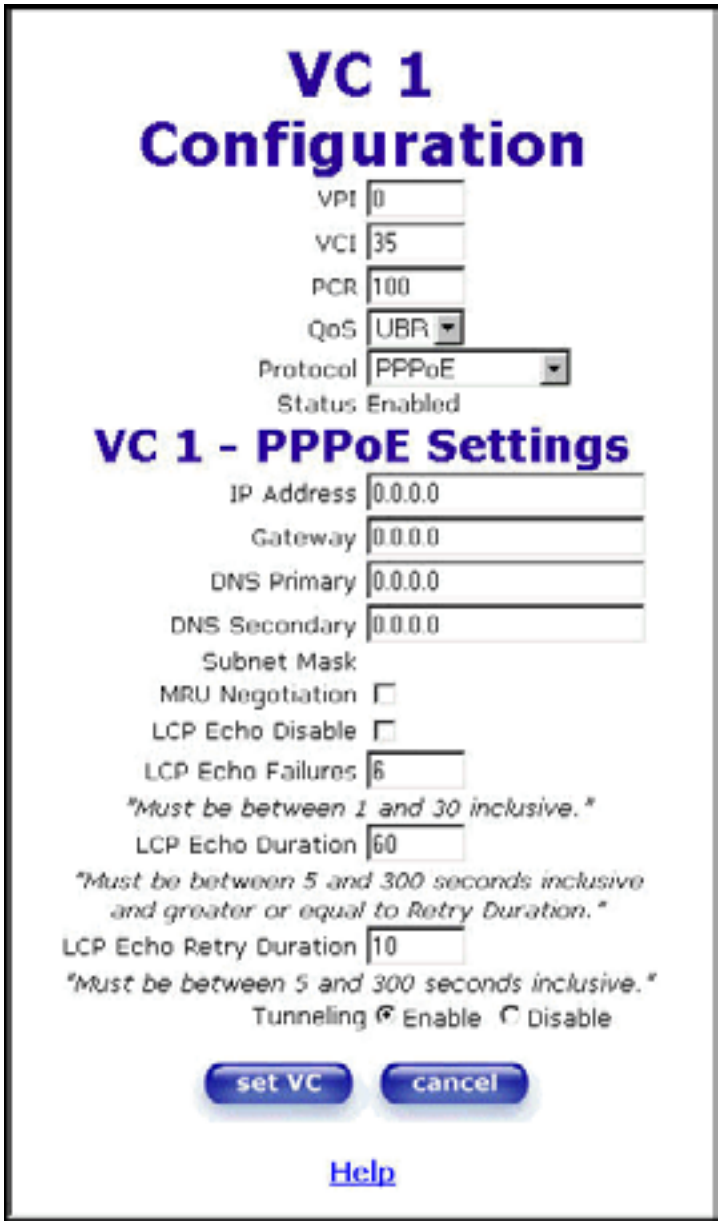
Status	Allows you to enable or disable your VC (Virtual Connection)
VPI	Displays the VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	Displays the VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.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

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

The following settings will be displayed if you select **edit** from your **VC Configuration** menu on any of your existing VC (Virtual Connections) settings. If you change any of your existing VC settings, click on **Set VC**.

NOTE: If you experience any problems, please reset VersaLink via the external hardware re-set button or via the procedure defined under the **Maintenance** menu.

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

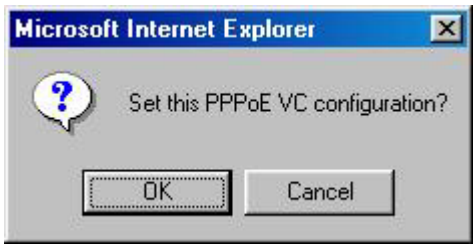


VC 1 Configuration	
VPI	This setting allows you to change your VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	This setting allows you to change your VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
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.

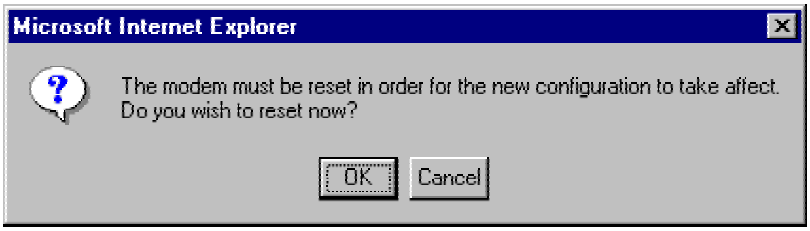
	This value is a percentage of the current data rate. 100 allows this VC to use 100% of the available bandwidth. 80 allows this VC to use 80% of the available bandwidth.
QoS	Quality of Service, which is determined by your Service Provider. CBR = Constant Bit Rate UBR = Unspecified Bit Rate VBR = Variable Bit Rate
Protocol	The Protocol for each VC, which is specified by your Service Provider. 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.
VersaLink	Displays VersaLink IP VersaLink address
DNS Primary	Provided by your Service Provider
DNS Secondary	Provided by your Service Provider
MRU Negotiation	Factory Default = DISABLED If ENABLED, the Maximum Received Unit (MRU) would enforce MRU negotiations. (NOTE: enable this option only at your Internet Service Provider's request.)
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 the Internet Service Provider, by bypassing VersaLink's capability to do this.

NOTE: The values for IP Address, VersaLink, 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 Internet Service Provider instructs you to change them.

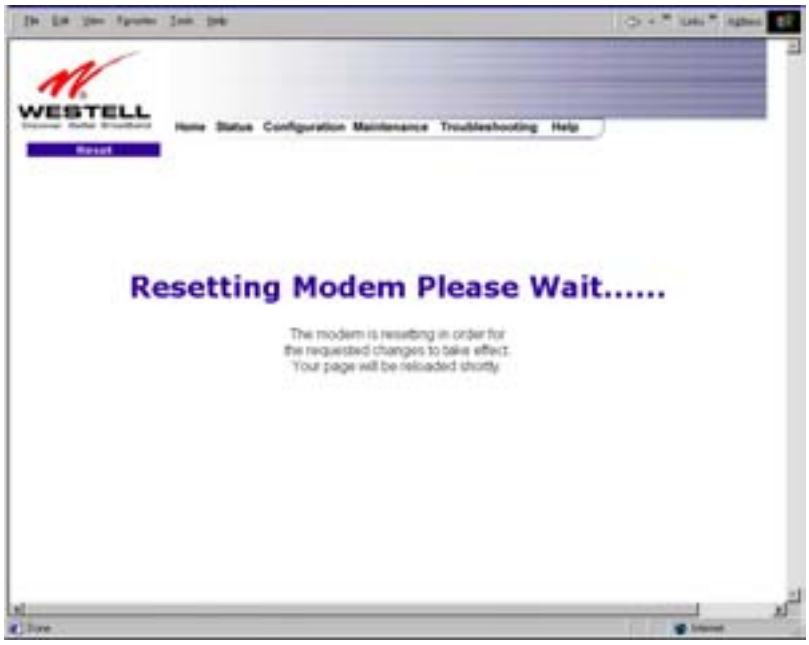
If you have made any changes to your VC settings, you need to save them. To save the new VC settings, click on **OK** when asked **Set this PPPoE VC configuration?** If you click on **cancel**, the new VC settings will not be saved.



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



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

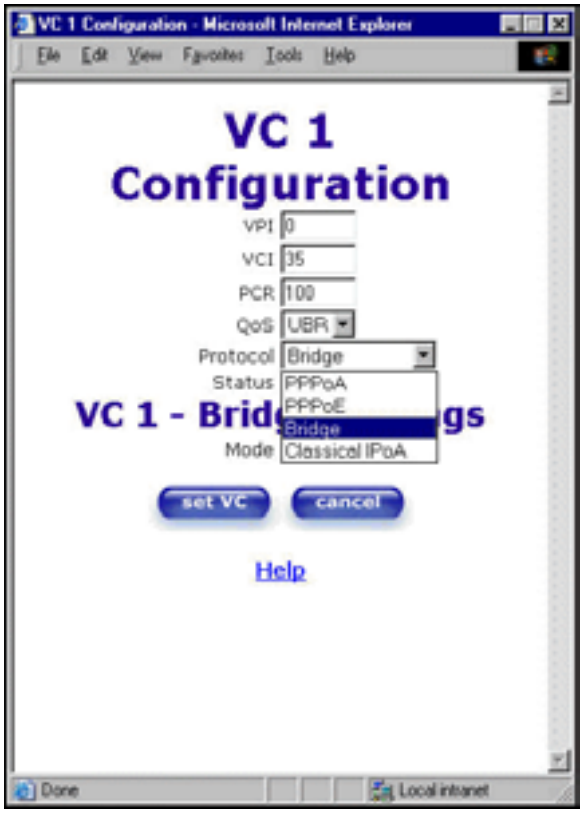


After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP.** (Click on the **connect** button to establish a PPP session).

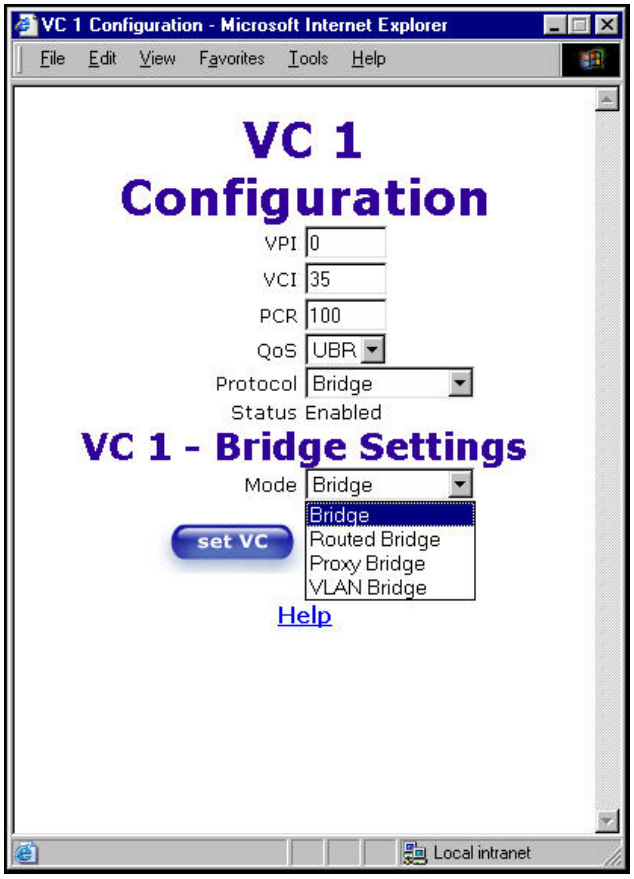
12.6.2.1 Configuring VersaLink's Protocol Settings

If you want to change VersaLink's protocol settings, select **VC** from the **Advanced WAN** menu. The **VC Configuration** screen will be displayed. Next, click on the **edit** button adjacent to any of the existing VC (Virtual Connection) settings.

If you clicked on **edit** in the **VC Configuration** screen, the following screen will be displayed. Select a Protocol from the options listed in **Protocol** drop-down arrow.



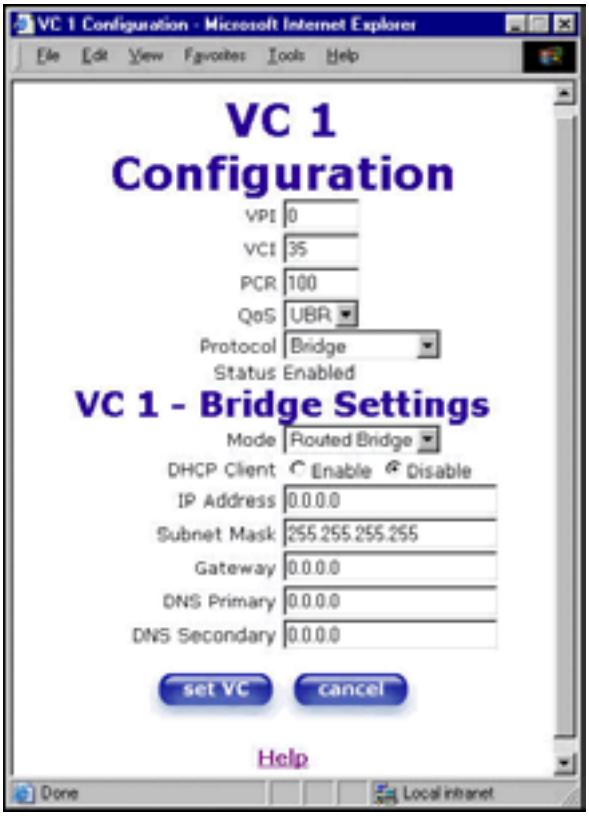
For example, if you selected the **Bridge** protocol, the following screen will be displayed. Select a mode from the options listed in the **Mode** drop-down arrow under **VC 1 – Bridge Settings**.



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 Service Provider.
VCI	This setting allows you to change your VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
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 Service Provider. CBR = Constant Bit Rate UBR = Unspecified Bit Rate VBR = Variable Bit Rate
Protocol	The Protocol for each VC, which is specified by your Service Provider. 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 form a DHCP server in the network or it can be assigned statically.
	Routed Bridge = Routed Bridged Encapsulation (RBE) is the process by which a bridged segment is terminated on a routed interface. Specifically, VersaLink 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 a VersaLink, which is configured statically. VersaLink address must not reside within VersaLink's assigned public subnet. All traffic will be sent via VersaLink'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.



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.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
Gateway	Displays the modem's IP gateway address.
DNS Primary	Provided by your Service Provider.
DNS Secondary	Provided by your Service Provider.

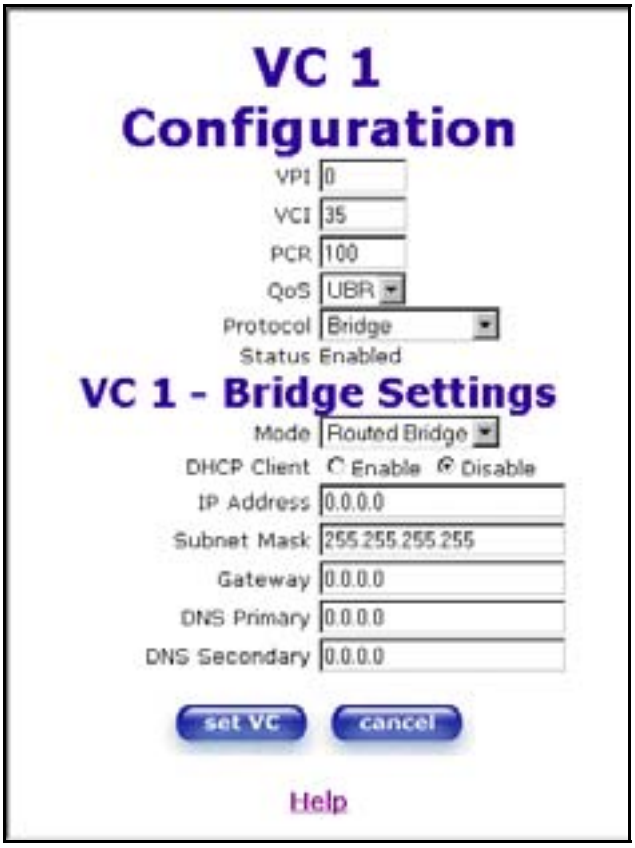
If you selected **Proxy Bridge** mode under **VC 1- Bridge Settings,** the following screen will be displayed.

VC 1 - Bridge Settings (Proxy Bridge)	
Mode	The Mode you have selected to use with Bridge protocol.
Gateway	Displays the modem's IP address.
DNS Primary	Provided by your Service Provider.
DNS Secondary	Provided by your Service Provider.

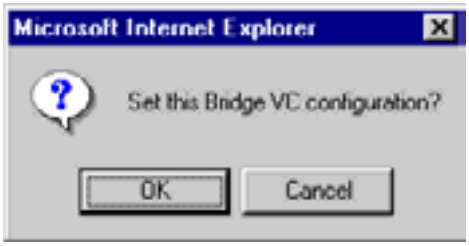
If you selected **VLAN** mode under **VC 1- Bridge Settings,** the following screen will be displayed.

VC 1 - Bridge Settings (VLAN Bridge)	
Mode	The Mode you have selected to use with Bridge protocol. VLAN is used to assign VLAN tags to individual data ports on the modem.
VLAN ID	Assigns a VLAN ID to the port.
VLAN Priority	This will set the VLAN priority for the port.
VLAN on WAN	Factory Default = DISABLE Selecting Enable allows VLAN tagging to occur according to the data port's configuration.

Once you have selected a **Mode**, click on the **set VC** button to save your VC settings.



If you clicked on **set VC**, the following pop-up screen will be displayed. Click on **OK**. If you click on **cancel**, the new VC settings will not be saved.



12.6.3 QOS

The following settings will be displayed if you select **QOS** from the **Advanced WAN** menu. Click on **save.**

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, expressed as a percentage of the DSL rate.
Committed Information Rate (%)	The committed rate for this priority, expressed as a percentage of the DSL rate.
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.

12.6.4 Route

The following settings will be displayed if you select **Route** from the **Advanced WAN** menu.

To add a Route, enter a **Netmask** 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 address and mask. Eth0 is the local LAN interface. Lo0 is the loopback interface. MainPPP is the main protocol interface.
Address	The IP interface address.
Netmask	The IP interface netmask 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.
Netmask	If the Route is a network route, netmask is used to specify the subnet mask. If the Route is a Host route, then the Host Route check box is used.
VersaLink	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.
Netmask	If the Route is a network route, netmask is used to specify the subnet mask. If the Route is a Host route, then the Host Route check box is used.
VersaLink	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.
Netmask	If the Route is a network route, netmask is used to specify the subnet mask. If the Route is a Host route, then the Host Route check box is used.
VersaLink	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.
Netmask/ Host Route	If the Route is a network route, netmask is used to specify the subnet mask. If the Route is a Host route, then the Host Route check box is used.
VersaLink/IP Address	The interface to use for sending the packet, if it matches this route. (Only active VersaLinks 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.

12.6.5 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.**

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 VersaLink	Factory Default = DISABLED If this box is check (Enabled), this feature will determine whether the modem advertises itself as a VersaLink (i.e., the default route)
Border VersaLink 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 changed any settings in the **RIP Configuration** screen and clicked on **save,** the following screen will be displayed. Click on **OK** to save your new RIP settings.

13. SETTING UP ADVANCED SERVICE CONFIGURATION

You can set up additional Service Configuration options for VersaLink 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 VersaLink via the external hardware re-set 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.

13.1 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.

13.2 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.

13.3 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.

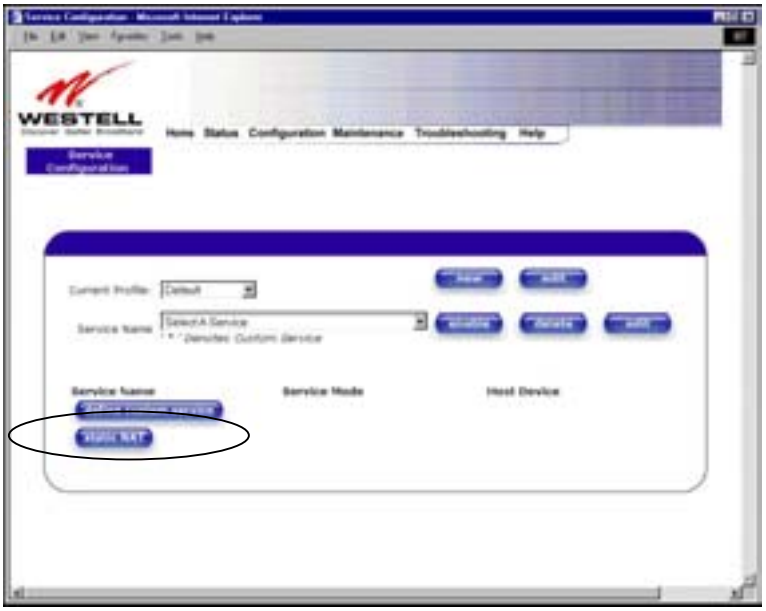
Service Name	The NAT service you selected.
Local Trigger Port Range	The local LAN side TCP/UDP port.
Global Port Range	The WAN side TCP/UDP port range.

13.4 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.

13.5 Static NAT

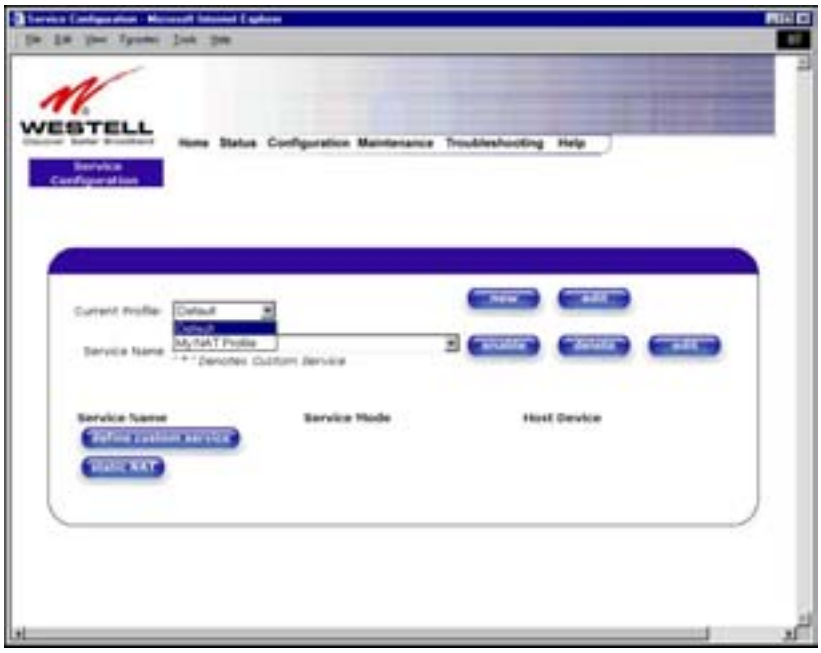
Static NAT will allow you to configure VersaLink to work with the special NAT services.



13.6 Enabling Static NAT

At the **Service Configuration** screen, select VersaLink's default account profile from the **Current Profile** drop-down box. Click on 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 name you created as the default.



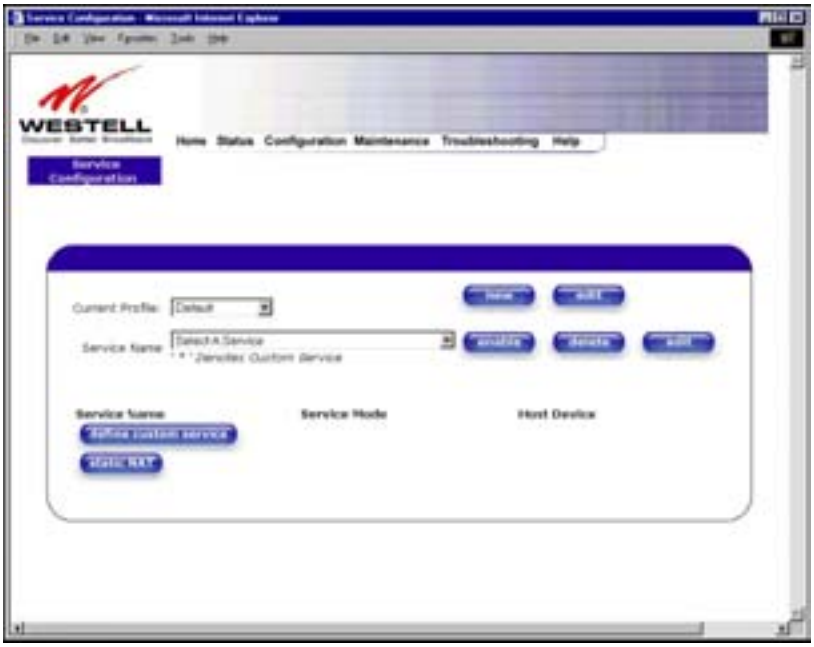
If you clicked on the **static NAT** button in the **Service Configuration** screen, the following screen will be displayed. Select your device from the **Static NAT Device** drop-down arrow, or type the IP address of the device in the field labeled **IP Address**. Click on **enable**. This will automatically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

This following screen shows Static NAT enabled.

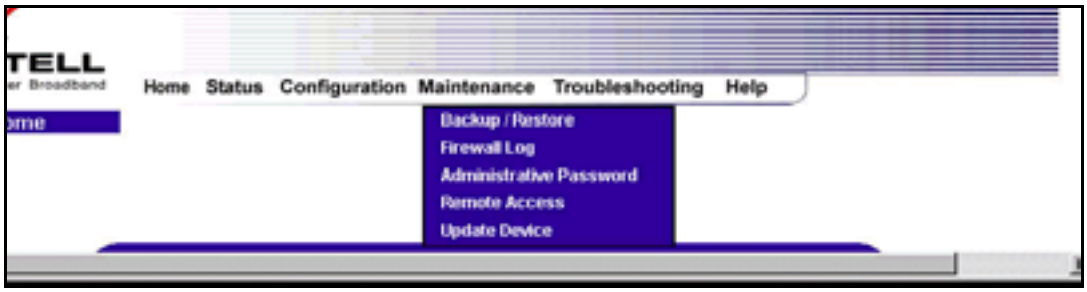
13.7 Disabling Static NAT

If you clicked 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.

The following screen shows Static NAT disabled (No device is displayed in the field adjacent to the **static Nat** button.)



14. MAINTENANCE



14.1 Backup/Store

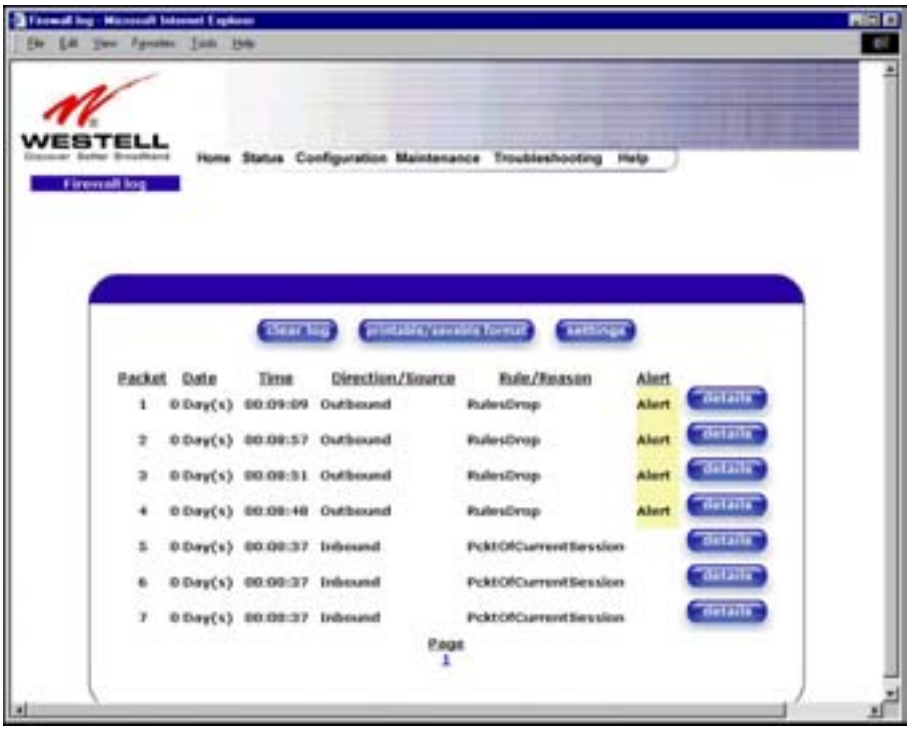
The following settings will be displayed if you select **Backup/Restore** from the **Maintenance** menu.

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.

14.2 Firewall Log

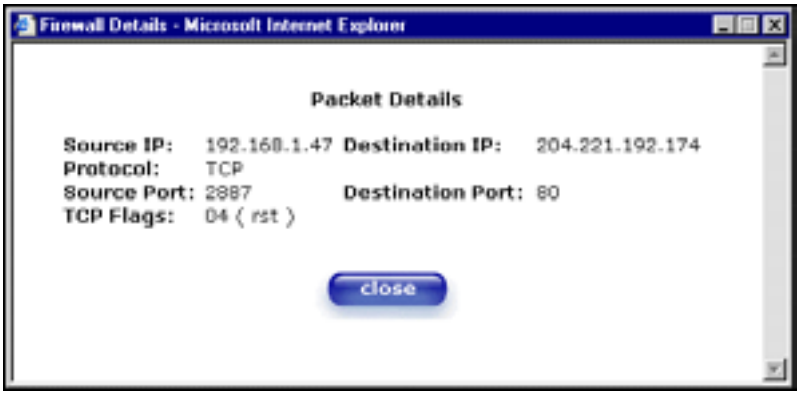
The following settings will be displayed if you select **Firewall Log** from the **Maintenance** menu.

This screen is an advanced diagnostics screen. It alerts you of noteworthy information sent to VersaLink 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.



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.**

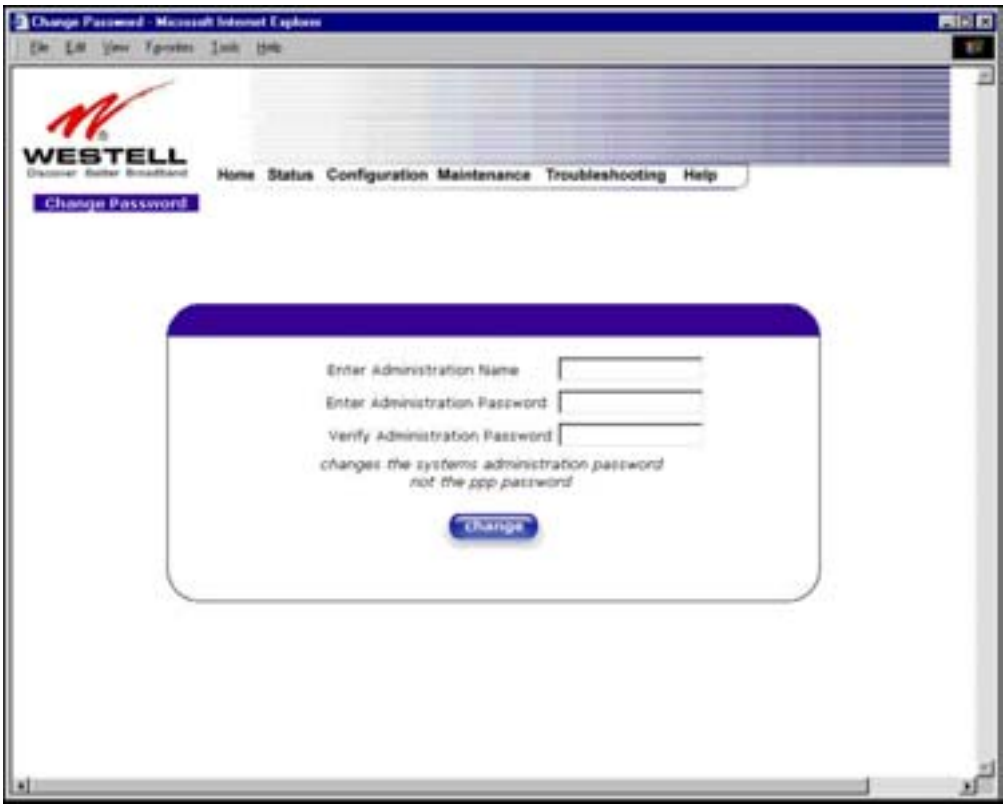


To clear the Firewall log, click **clear log** in the **Firewall Log** screen. The following pop-up screen will be displayed. Click **OK** when asked "**Do you wish to clear the Firewall log file?"** If you click **Cancel**, the firewall log will not be cleared.

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.

14.3 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**.



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.

14.4 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 VersaLink

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.

14.5 Update Device

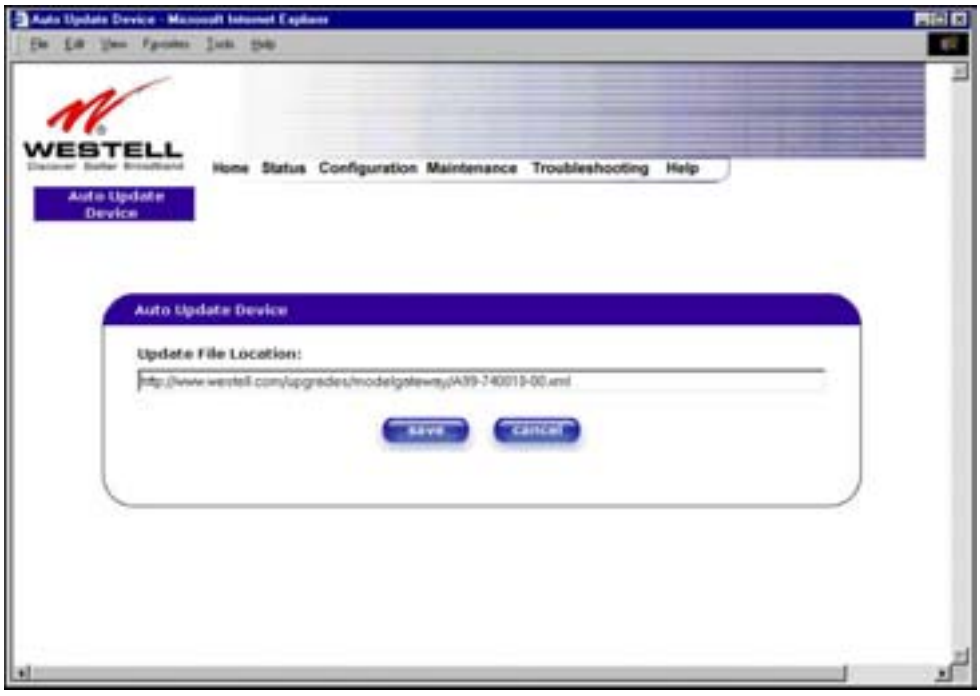
The following screen will be displayed if you click on **Update Device** from the **Maintenance** menu. This screen is used to update the firmware that controls the operation of VersaLink. The updated firmware may be loaded from either a file that is located on your PCs hard drive or from update files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

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.

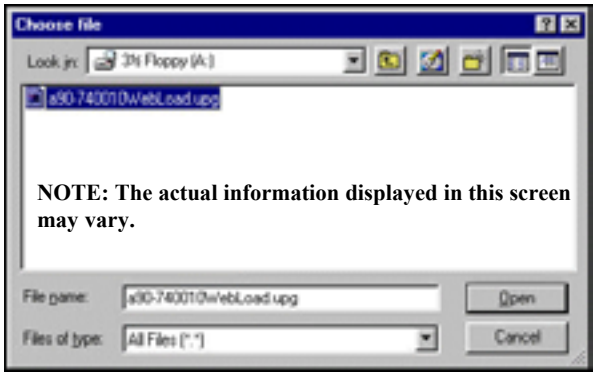
NOTE: If you click on check for web update and the page returns a “page not found” message, this indicates that the software update file is not available. Go back to the previous screen to continue.

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.



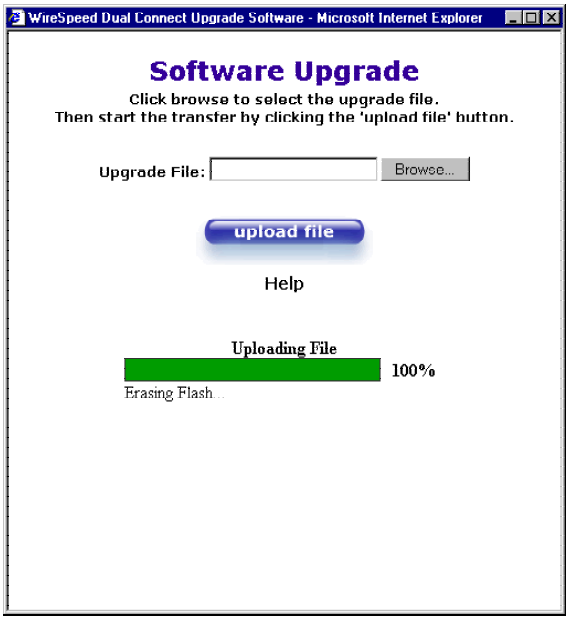
Click on the **local update now** button in the **Update Device** screen to select the upgrade file from your PC's hard drive. This screen allows you to upgrade the software on VersaLink. Click **Browse…** and go to the location where the upgrade file is stored.

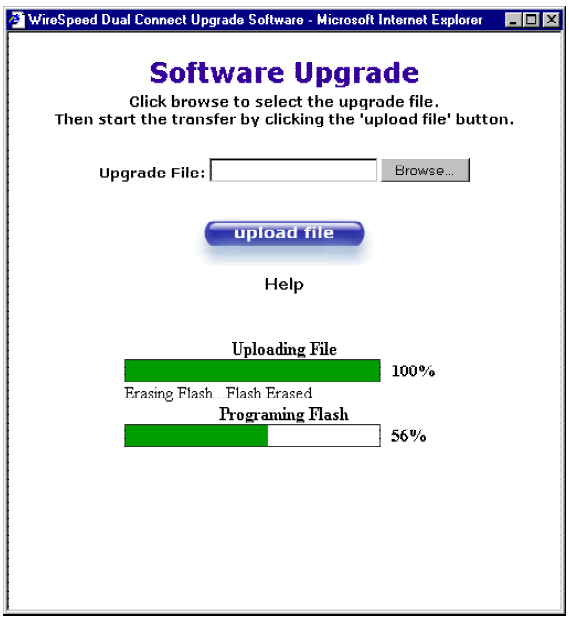


Select the appropriate upgrade file from your browser. The file name will appear in the field labeled **Upgrade File**. Click on **upload file.**

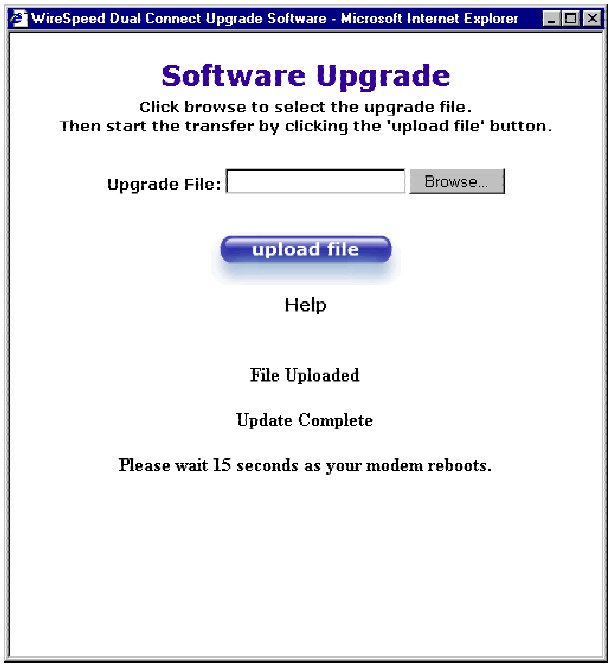
This screen shows that the file is being uploaded to VersaLink.

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.)

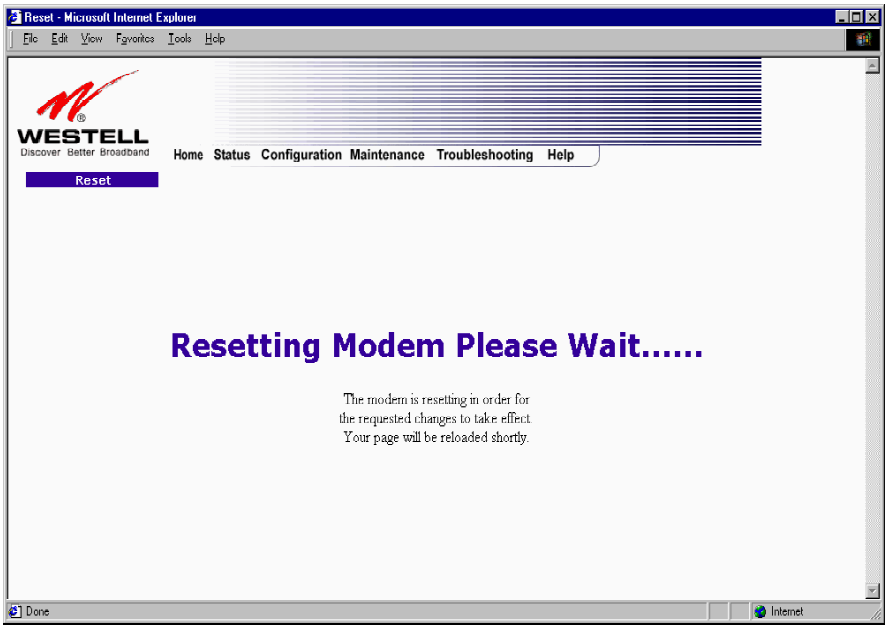




The screen below shows that the upload was successful. The modem will now reboot.

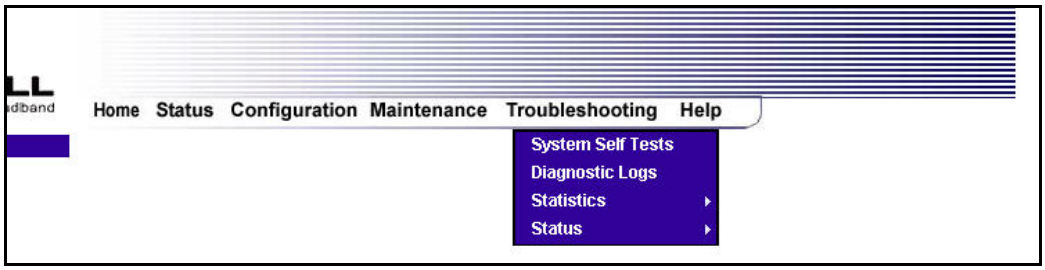


The following screen will be displayed as VersaLink is being reset.



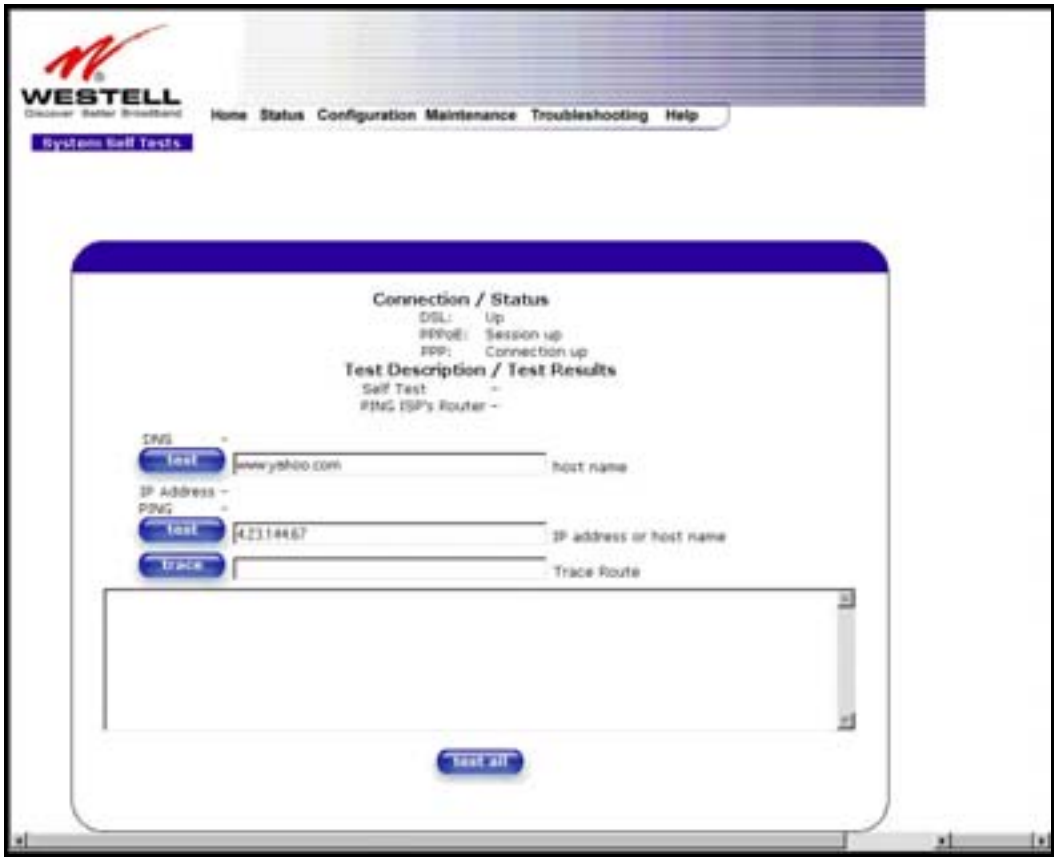
After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that the PPP Status displays **UP.** (Click on the **reset** button to re-establish your PPP session.)

15. TROUBLESHOOTING



15.1 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 VersaLink'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.

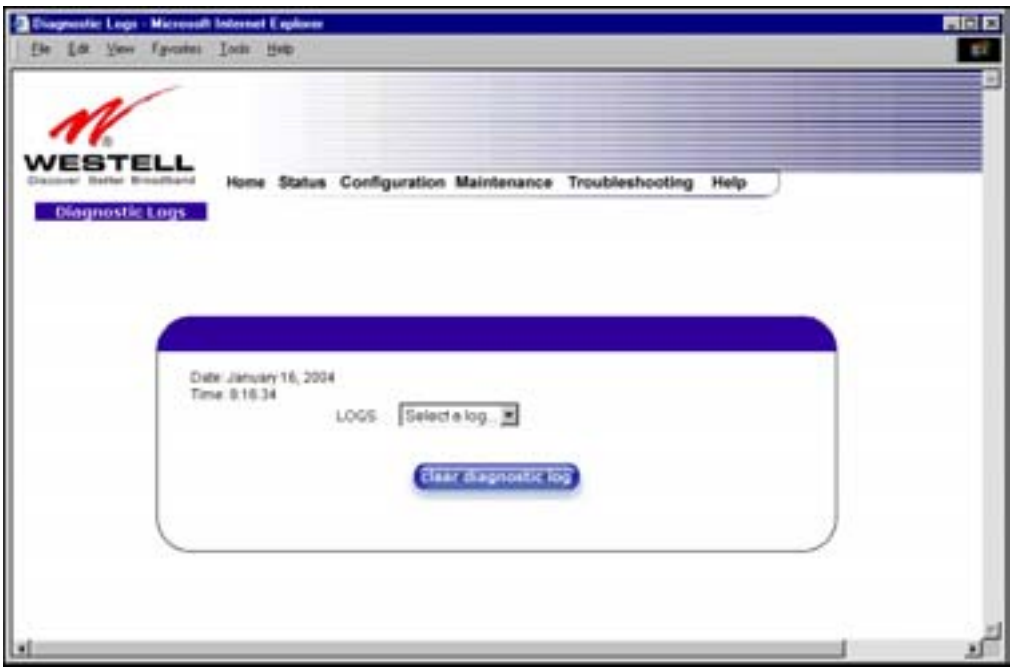
If you want to PING using the MS-DOS (shell) window, first you will need to check your firewall security setting. (If you PING via DOS shell you are susceptible to firewall rules, as this PING is dependent on VersaLink's firewall settings.) If your firewall is set to **Medium** or **High**, you will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

Connection/Status	
DSL	VersaLink checks the status of the DSL connection. Possible responses are: UP: VersaLink is operating correctly and has obtained synchronization with the opposing network device. DOWN: VersaLink is operating correctly, but has not synchronized with the opposing device.
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: VersaLink 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 VersaLink.
PING ISP's VersaLink	Performs an IP network check (i.e., an IP Ping) of the Service Provider's VersaLink. This test verifies that VersaLink can exchange IP traffic with an entity on the other side of the DSL line. Possible responses are: Success: VersaLink has detected an IP Remote VersaLink connection. No Response: The IP Remote VersaLink does not answer the IP Ping. Could not test: The test could not be executed due to VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.
DNS	Performs a test to try to resolve the name of a particular host. The host name is entered in the input box.

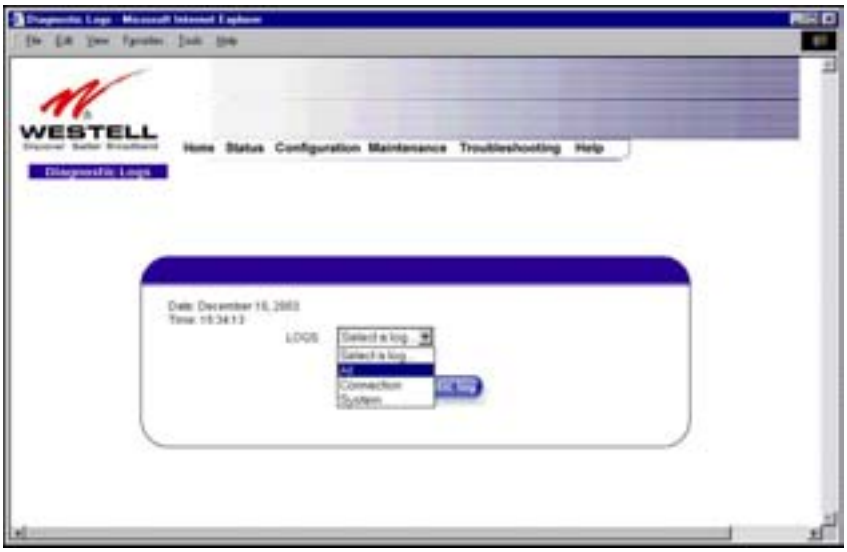
	Possible responses are: Success: VersaLink has successfully obtained the resolved address. The IP address is shown below the host name input box. No Response: VersaLink has failed to obtain the resolved address. Host not found: The DNS Server was unable to find an address for the given host name. No data, enter host name: No host name is specified. Could not test: The test could not be executed due to VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.
IP Address	IP Address of the Host Name.
PING	Performs an IP connectivity check to a remote computer either within or beyond the Service Provider'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 VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.
Trace Route	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.

15.2 Diagnostic Logs

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



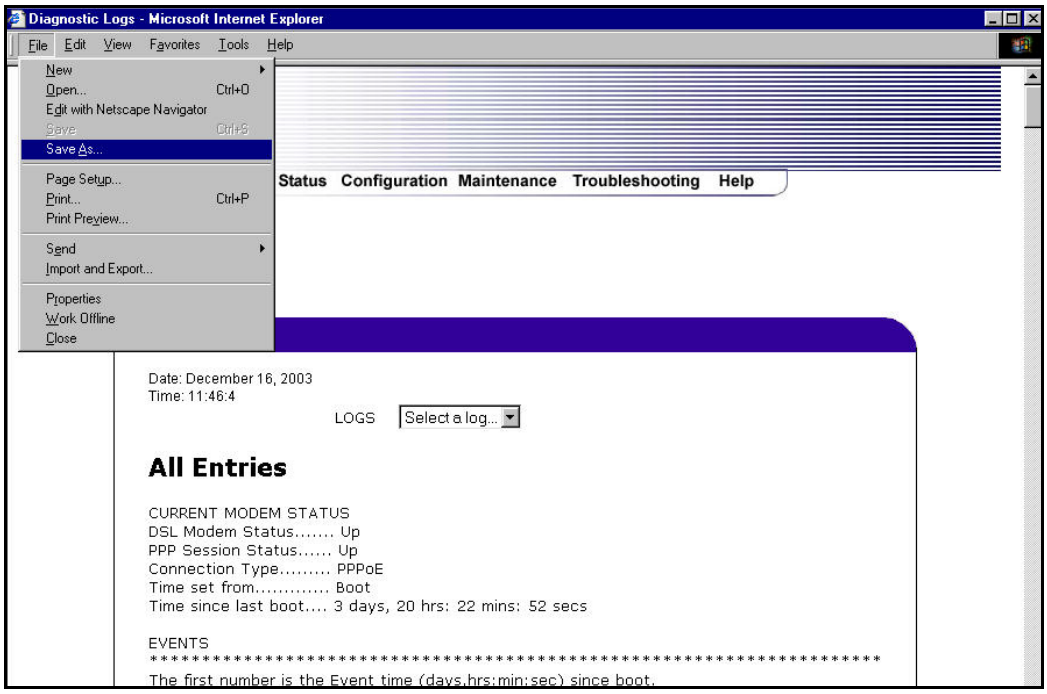
To see a list of the log options, click on the arrow at the **LOGS** drop-down menu. Select an option from the list provided at the **Diagnostics Logs** screen.



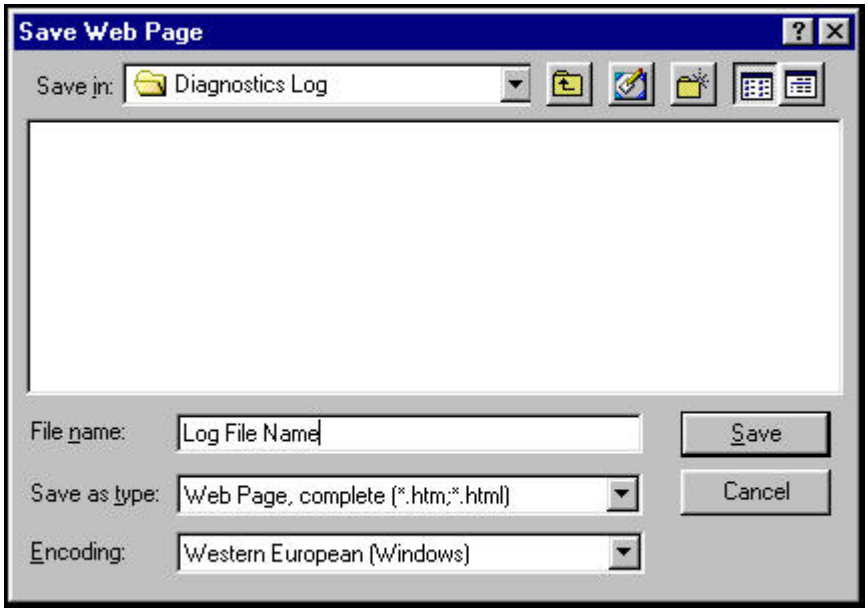
If you clicked on **All,** the following screen will be displayed. This screen provides a detailed list of VersaLink's connection status and system information. Click on **clear diagnostic log** to clear the diagnostic log information.

15.2.1 Saving the Diagnostic Log File

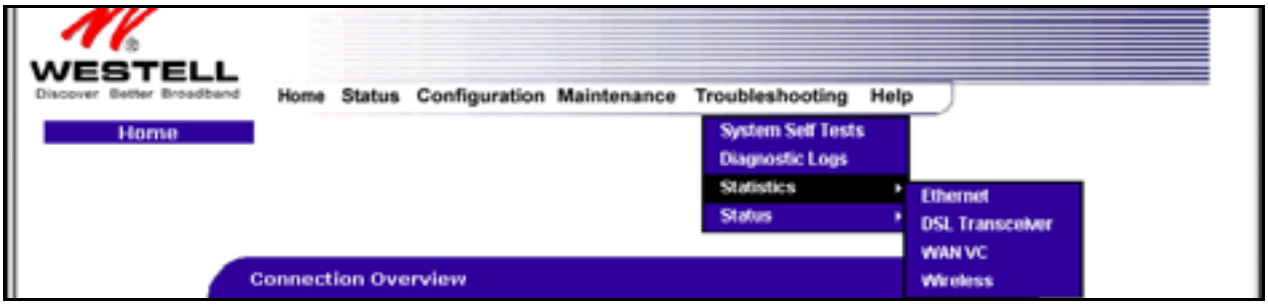
If you want to save the diagnostic log file, go to your Browser's menu and select **File,** then select **Save As** from the drop-down menu.



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**.

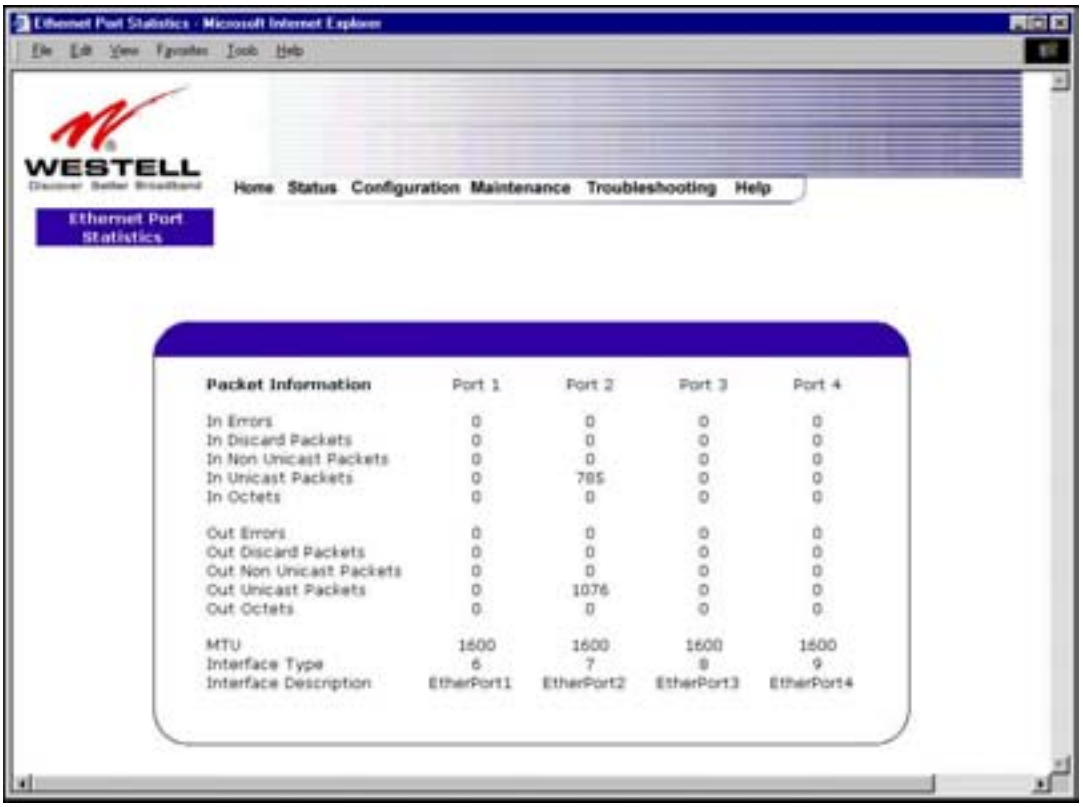


15.3 Statistics



15.3.1 Ethernet Port Statistics

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

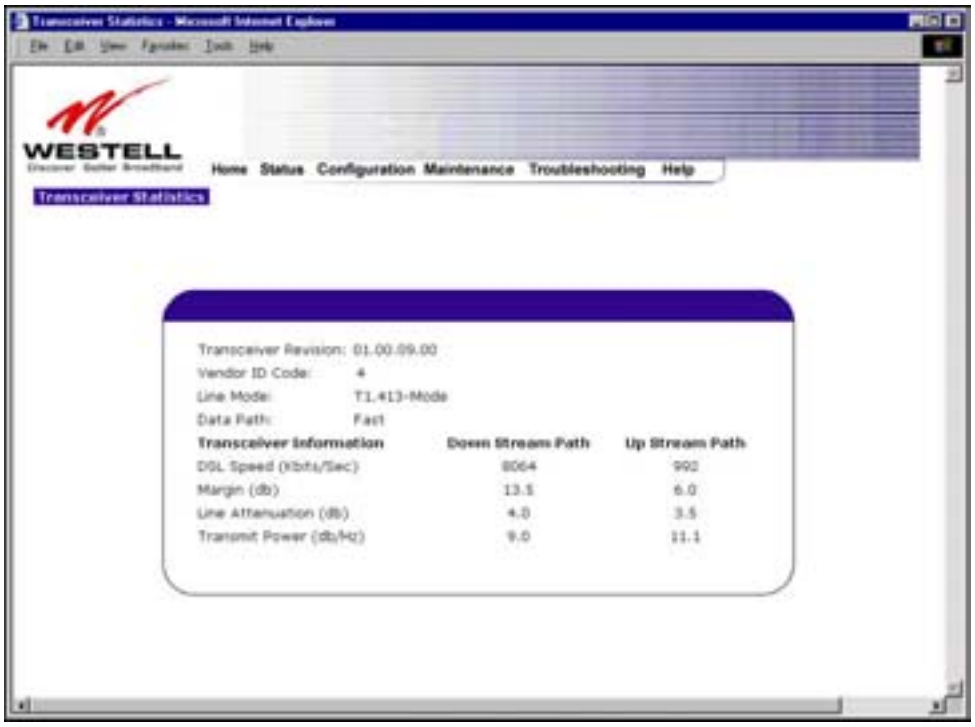


In Errors	The number of error packets received on the Ethernet interface.
In Discard Packets	The number of discarded packets received.
In Non Unicast Packets	The number of non-Unicast packets received on the Ethernet interface.
In Unicast Packets	The number of Unicast packets received on the Ethernet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

15.3.2 DSL Transceiver Statistics

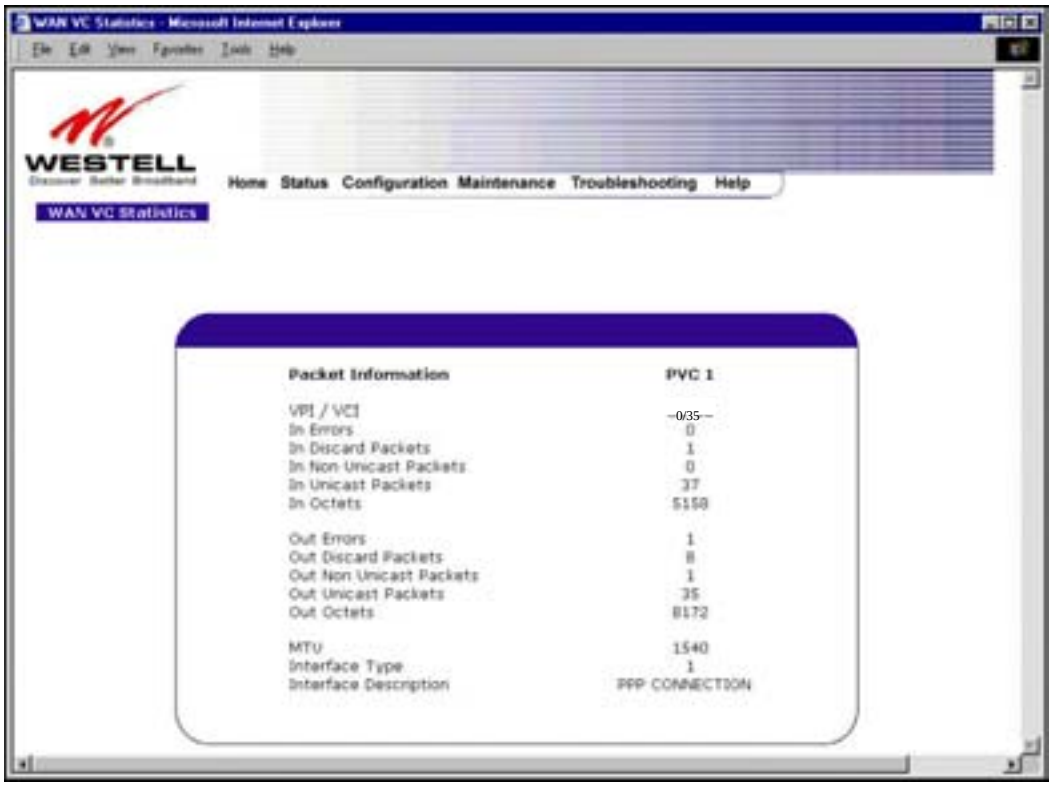
The following settings will be displayed if you select **DSL Transceiver** from the **Statistics** menu.



Transceiver Revision	The transceiver software version number.
Vendor ID Code	The CPE Vendor's ID code for their chipset.
Line Mode	The operational mode. Modes supported are No Mode, Multi Mode, T.1413 Mode, G.DMT Mode, and G.LITE Mode.
Data Path	The data path used (either Fast or Interleaved).
Transceiver Information-Down Stream/Up Stream Path	
DSL Speed (Kbits/Sec)	The transmission rate that is provided by your Internet Service Provider (ISP).
SNR Margin (db)	The Signal-to-Noise Ratio (S/N) where 0 db = $1x10^{-7}$, which inhibits your DSL speed.
Line Attenuation (dB)	The DSL line loss.
Transmit Power (db/Hz)	The transmitted signal strength.

15.3.3 WAN VC Statistics

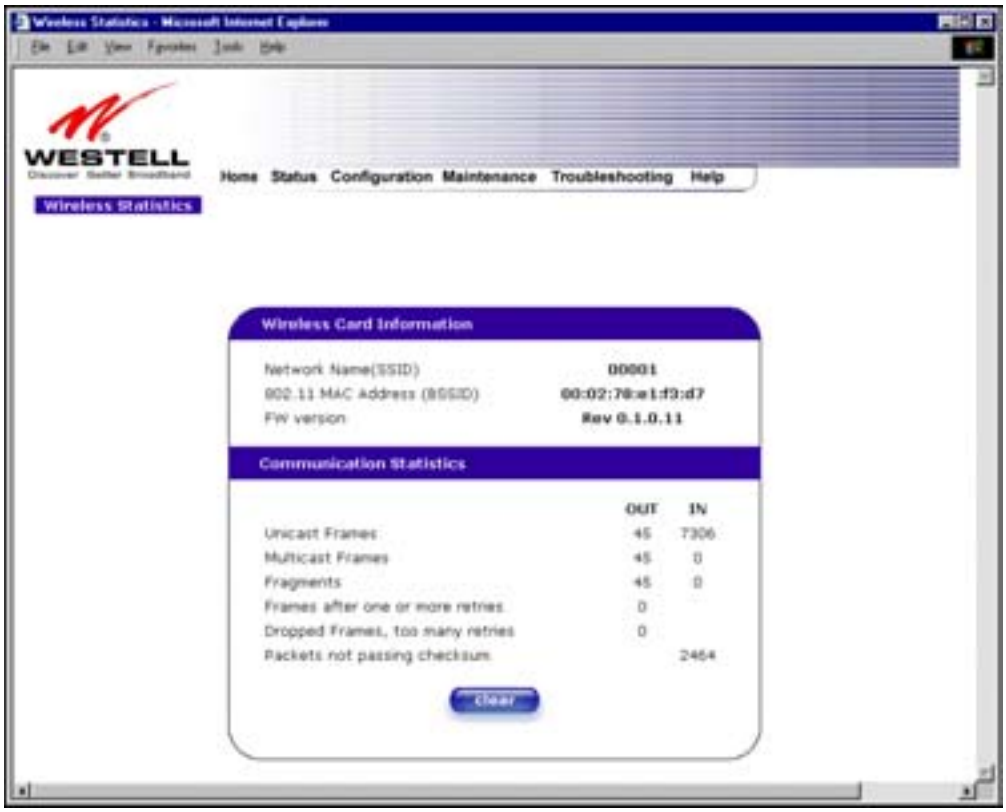
The following settings will be displayed if you select **WAN VC** from the **Statistics** menu.



VPI/VCI	Displays the VPI/VCI values obtained from your Internet Service Provider.
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.

15.4 Wireless Statistics

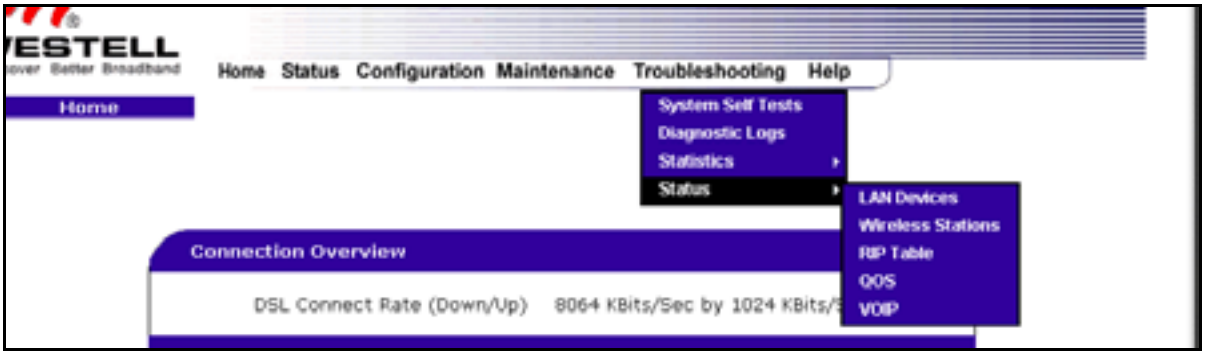
The following settings will be displayed if you select **Wireless** from the **Statistics** menu.



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 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.
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 the VersaLink to a station; VersaLink is the source. Data preceded by **IN** pertain to data received by VersaLink; VersaLink 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

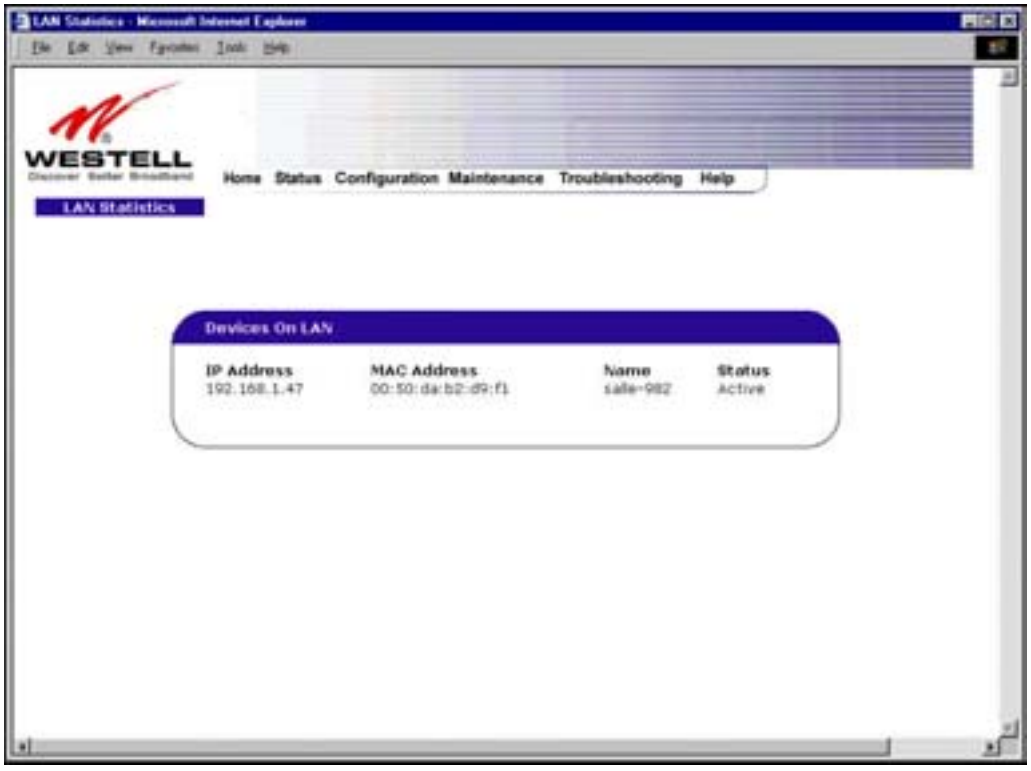
	broadcast to all stations, but more than a single station. Broadcast messages are included in the count.
OUT-Fragments	The number of successful transmissions made. This will typically be greater than the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable).
OUT-Frames after single retry	The number of frames that were successfully transmitted after one, and only one, retry. All fragments of the frame must have met this requirement if the frame was fragmented.
OUT-Frames after many 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.
OUT-Discarded Frames	The number of transmit requests that were discarded to free up buffer space on the NIC. This count is incremented when one of the following occurs: 1) A transmit request is queued too long on the transmit queue due to excessive retries, deferrals, scans, etc. 2) A transmit request is queued too long on the Power-Save queue because the station did not poll or wake up in time.
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-Drops due to insufficient Rx buffers	The number of received frames discarded due to lack of buffer space.
IN-Packet not passing checksum	The number of received frames with a Frame Check Sequence (FCS) error.

15.5 Status



15.5.1 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 VersaLink 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.

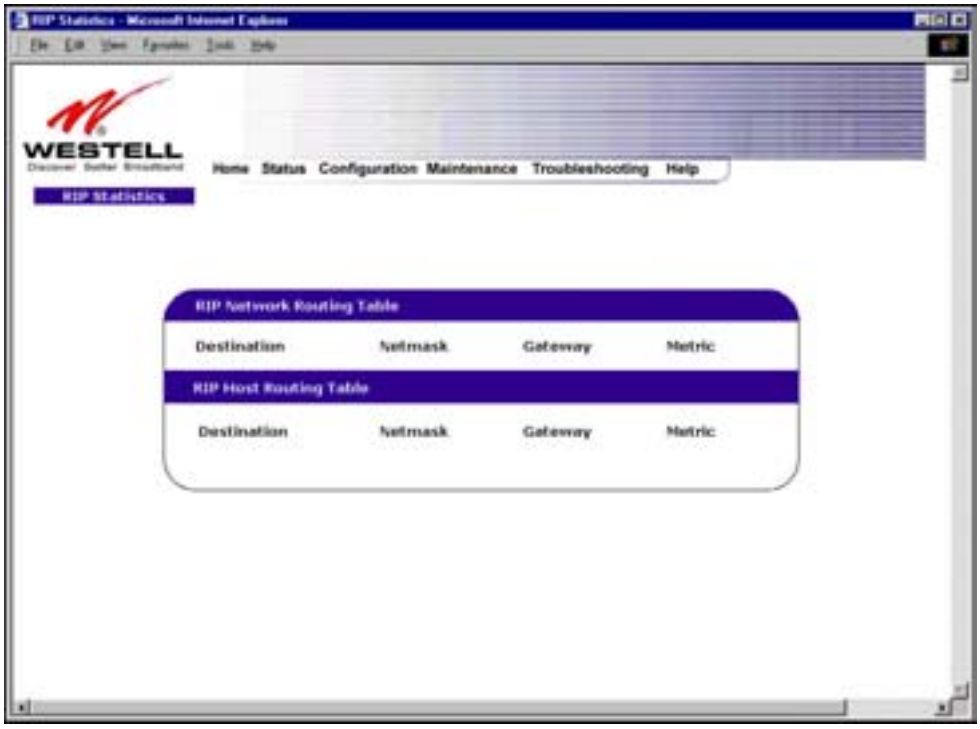
15.5.2 Wireless Stations

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

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

15.5.3 RIP Table

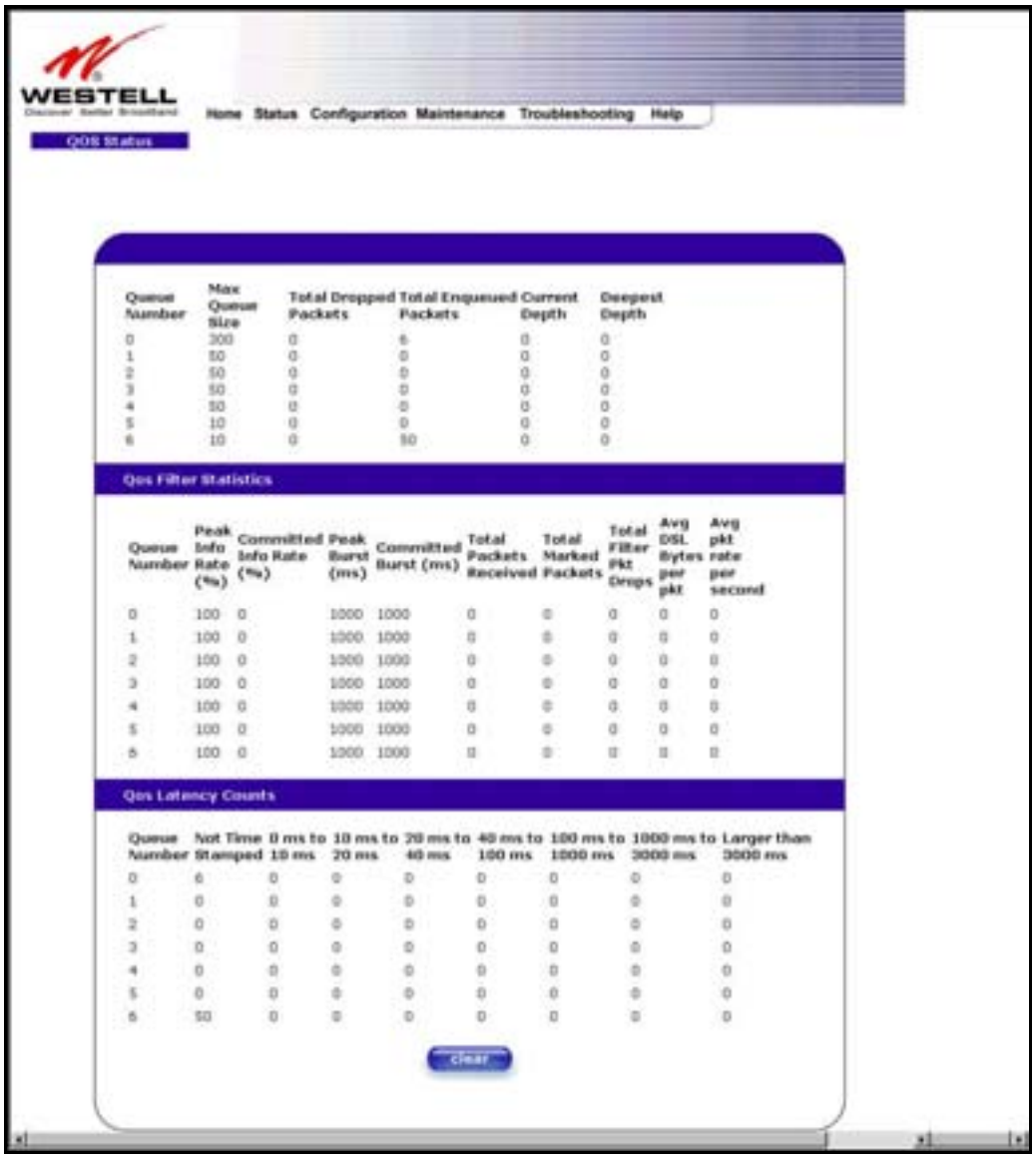
The following settings will be displayed if you select **RIP Table** from the **Status** menu.



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.

15.5.4 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.



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, expressed as a percentage of the DSL rate.
Committed Info Rate (%)	The committed rate for this priority, expressed as a percentage of the DSL rate
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. DSL 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

15.5.5 VOIP Status

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

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.

16. NAT SERVICES

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

NOTE: To configure VersaLink for a service or application, follow the steps in section 13 (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 VersaLink from your ISP.
USENET News Service	143 TCP
VNC, Virtual Network Computing	5500 TCP, 5800 TCP, 5900 TCP
Westwood Online, C&C	4000 TCP/UDP, 1140-1234 TCP/UDP
World Wide Web (HTTP)	80 TCP 443 TCP (SSL) 8008 OR 8080 TCP (PROXY)
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.

17. HELP

If you select **Help** from the menu bar, a message from the help screens will be displayed. The type of message displayed depends on the menu that you are viewing. If you are viewing a pop-up screen, click the **help** link in the pop-up screen to obtain help messages.

A

About

This screen provides information about VersaLink. The following settings are displayed.

About	
Model Number	VersaLink manufacturer's model number.
Serial Number	VersaLink manufacturer's serial number.
MAC Address	Ethernet MAC (i.e., hardware) Address of VersaLink.
Software Version	VersaLink application software version number.
Software Model	VersaLink application type.
Description	Description of VersaLink protocol processing application software.
Boot Loader	VersaLinks boot loader version number.

Advanced Home Page

The advanced home page offers the same functionality as the home page but adds the ability to change the connection profile settings defined in VersaLink.

About	
Edit	An “Edit” link is added for each connection profile. Selecting this link will pop up a window that allows the connection profile settings to be changed.
New Connection	The “New Connection” link will pop up a window to allow the creation of a new connection profile.

ATM Loopback

ATM Loopback	
ATM Loopback	This setting enables 0/21 loopback. Westell recommends that you do not change this setting.

B

Backup/Restore

This option allows VersaLink configuration to be backed up to or restored from a secure location in flash. The following options are displayed.

Backup/Restore	
Current becomes Back-up	Selecting this command button will backup the current active configuration to the secure flash location.
Back-up becomes Current	This command button will restore the previously stored configuration from the flash location.
Factory becomes Current	This option will restore VersaLink to the state that it arrived in from the factory.

C

Change Administration Password

VersaLink has an administrator password. This password protects VersaLink from any unauthorized modifications to the configuration setting in VersaLink. The following settings are displayed.

Change Administration Password	
Enter Administration Name	This field specifies the Administrator's name. Only one administrator can be defined.
Enter/Verify Administration Password	This field specifies the password required to enable administrator access. The password must be entered twice to ensure that the password has been entered correctly.

Connection Summary

Connection Summary	
Connection Summary	The connection profile screen displays summary information about VersaLink. The connection state is shown along with the amount of traffic has passed through VersaLink. Each connection profile is listed with its associated usage information.

D

Diagnostics Help

This screen provides tools for diagnosing PPP connection problems. Some tests depend on VersaLink's status and the capabilities exercised by previous tests, which may prevent other types of testing.

Beginning of Diagnostics Help screens

DSL
VersaLink status checks the connection. The following is a list of the possible responses:

DSL	
Up	VersaLink is operating correctly and has obtained synchronization with the opposing modem.
Down	Explanation: VersaLink is operating correctly, but has not synchronized with the opposing DSLAM. Solution: First, check to be sure that the cable connecting VersaLink to the ADSL wall jack is properly connected at both ends. If the cable is properly connected and VersaLink does not synchronize, try another phone cable. Next, wait for VersaLink to train. It can sometimes take as long as two minutes for VersaLink to train. If it still has not come into synchronization, power cycle VersaLink. If you have tried the approach above and VersaLink still does not synchronize, contact your service provider.

PPPoE
The PPPoE status indicates if a PPPoE session is established (i.e., if the PPPoE Discovery procedure has completed). The following is a list of the possible responses:

PPPoE	
Session up	A valid PPPoE session has been detected.
no session	Currently there is no active PPPoE session. A PPP session must be connected from the homepage screen.
initiating session	The connection process for a PPPoE session has been initialized. It can sometimes take a few seconds for the PPPoE Discovery procedure to complete. Wait 10-15 seconds and try again. If the PPPoE Discovery still cannot complete, there may be a configuration issue with your service provider's equipment. Verify your VPI/VCI settings (on the LAN Advanced page) and contact your ISP provider.
Session halted	A successful PPPoE session was halted. A PPP session must be connected from the homepage screen.
passed	A valid PPPoE session was established.
Session failure	A PPPoE session could not be made. There may be a configuration issue with your service provider's equipment. Verify your VPI/VCI settings (on the LAN Advanced page) and contact your provider.

PPP
This field displays the PPP Connection status. A PPPoE or PPPoA session must already be established. The following is a list of the possible responses:

PPP	
Connection up	VersaLink has established a PPP connection.
no connection	There is no PPP connection. A PPP session must be connected from the homepage screen.
initiating connection	The PPP connection process has been initialized.
Connection halted	A successful PPP connection was halted. Solution: A PPP session must be connected from the homepage screen.
Cannot connect	Explanation: A PPP connection could not be made because of a PPPoE session failure.
Authorization failure	The username or password is incorrect. Verify that the username and password your Service Provider issued are entered correctly.
Link control protocol failed	Try re-establishing the session (from the home page). If this doesn't help, there may be a configuration issue or other failure with your provider's equipment. Contact your service provider.

Self Test
The Self Test performs an integrity check of certain internal components of VersaLink. The following is a list of the possible responses:

Self Test	
Success	VersaLink is operating correctly.
Flash Corrupt	Explanation: The self-test process has detected a problem with internal flash memory. Solution: Restart VersaLink. If the error persists, contact your service provider.

PING ISPs' VersaLink
The IP remote VersaLink test performs an IP network check (i.e., an IP Ping) of the Service Provider's VersaLink. This test verifies that VersaLink can exchange IP traffic with an entity on the other side of the DSL line. The following is a list of the possible responses:

PING ISP's VersaLink	
Success	VersaLink has detected an IP remote VersaLink connection.
No Response	Explanation: This message will occur when an IP remote VersaLink does not answer the IP Ping. Solution: This test fails when the provider's VersaLink does not give its IP address to VersaLink during session establishment. Try Pinging another host, using the Ping test near the bottom of the Diagnostic screen. If you are able to Ping any host, or even if you are able to find an IP address for a given host name (try "www.yahoo.com"), then the failure of the "IP Remote VersaLink" test is moot, because the success of the Ping demonstrates that you are getting IP traffic across the DSL line. If the separate Ping fails as well, contact your service provider.
could not test	Explanation: Test could not be executed because of VersaLink status.

DNS
The DNS test issues a request to try to resolve the name of a particular host. The host name is entered in the input box. The following is a list of the possible responses:

DNS	
Success	VersaLink has successfully obtained the resolved address. The IP address is shown below the host name input box
No Response	Explanation: VersaLink has failed to successfully obtain the resolved address. Solution: Determine the IP addresses of your DNS servers (from the home page, click "Edit" and then "Advanced"), and then use the Ping test near the bottom of the Diagnostic screen to try to Ping those addresses. This may provide useful information when you contact your service provider and speak with Technical Support.
Host not found	Explanation: The DNS Server was unable to find an address for the given host name. Solution: That host may no longer be available on the Internet. Try entering a different host name.
No data, enter host name	Explanation: There must be a host name entered in the input box.
could not test	Explanation: Test could not be executed because of VersaLink status.

PING
Select **PING** to check IP continuity to a remote computer either within or beyond the Service Providers network.

Enter either the IP address or the hostname of the remote host computer into the input box to the right of the Test button. If you Ping by name, DNS will be used to look up the appropriate IP address for that name.
The following is a list of the possible responses:

PING	
Success	The Remote Host Computer was detected.
No Response	Explanation: This message will occur when there was no response to the Ping from the remote computer. Solution: Bear in mind that many hosts on the Internet are configured for security reasons to not respond to IP Ping messages. If you get a success from the DNS test using the same host name, chances are good that your connection is fine, whether you can Ping the named host or not.
No name or address to PING	Explanation: There must be a host name or IP address entered in the input box in order for VersaLink to Ping.
could not test	Explanation: Test could not be executed because of VersaLink status.

End of Diagnostic Help Screens

DHCP Configuration

This screen contains the settings which control how VersaLink interacts with the local devices connected to VersaLink. Westell does not recommend that you change these settings. The following settings are displayed.

DHCP	
DHCP Server	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
DHCP Start Address (If DHCP is enabled)	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Lease (If DHCP is enabled)	This setting specifies the DHCP lease time.

Diagnostic Log

Diagnostic Log	
All	This option lists both the Connection and the System logs.
Connection	This option lists all events related to connection activity (any traffic on the Ethernet, or DSL ports).
System	This option lists all events related to system activity (time, errors, boot information, etc.)

DNS Configuration

VersaLink has a built-in DNS server. VersaLink has a feature called "Dynamic DNS." When an IP address is assigned, VersaLink will interrogate the new device for a machine name using several well-known networking protocols. Any names learned will dynamically be added to the DNS server's table of local hosts. A static host assignment is needed only if the new device does not support any of the well-known protocols. The following settings are displayed.

DNS Configuration Screen	
Domain Name	The name of your network. This uses the internet standard for delineating domain names.
Static Host Assignment	This table allows the creation and maintenance of manually configured DNS entries.
Dynamic Host Assignment	This table shows the current list of devices that have automatically provided information.

E

Edit Connection Profiles

This screen facilitates the changing of connection profile parameters. The following settings are displayed.

Edit Connection Profiles	
Connection Name	This field is a description of the default connection profile that VersaLink will use. Feel free to use whatever description you desire.
Account ID	Your account ID is supplied by your ISP. This text string uniquely identifies you with your ISP.
Account Password	The Account Password is a key phrase or text string that verifies your identity to the ISP.
Service Profile	VersaLink stores several service profiles. A service profile is a collection of settings for the built-in firewall and NAT. These settings control which applications are enabled to talk through VersaLink. This selection specifies which service profile is used when VersaLink is using this connection.
Manual/Auto/Always ON	These radio buttons specify how this connection profile is used. A manual setting requires that this connection must be manually established through the "homepage" connection button. When this is set to auto, VersaLink will monitor the network traffic and determine when a connection needs to be made. The connection process will happen automatically the "Always ON" selection causes VersaLink to aggressively establish a connection with your ISP. Whenever VersaLink detects that the connection to your ISP is down, it will try to re-establish that connection.
Time Out Enable/Connection Time Out	Selecting this option will enable the disconnect timeout. If this option is enabled VersaLink will monitor the ISP connection for activity. If there is no activity for the timeout period, VersaLink will disconnect from the ISP.
Edit VC Connection	This screen is an advanced screen. Modifying parameters identified on this screen can cause severe disruption of your service. VC stands for "Virtual Connection." A VC identifies a connection through the service provider's ATM network to your ISP. It is not recommended that you change anything on these pages unless explicitly instructed by your service provider.

F

Firewall Log

This screen is an advanced diagnostics screen. It alerts you of noteworthy information sent to your modem from the Internet. One thousand entries can be made, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for new entries as they occur.

Firewall Log	
Details	This option gives more information about the specific log entry
Page Numbers	This option navigates you to the corresponding range of entries. The most recent entries are always on the highest numbered page.
Clear Log	This option removes all entries from the log.
Print/Savable Format	This option opens a new window that contains a list of all logged packets that can be saved or printed.

Firewall Settings

This screen is an advanced configuration screen. It allows you to set the level of security you wish to have on your local network. All security levels except "None" protect against known Internet attacks and devices that attempt to gain remote access to VersaLink. The following settings are displayed.

Firewall Settings	
High	This security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. No other traffic is allowed. Another restriction of high security is that it can't be modified by NAT configuration options. With High security, you are guaranteed to only pass the previously mentioned traffic.
Medium	This security level only allows basic Internet functionality by default. Like High security, Medium security, allows customization through NAT configuration, so you can enable the traffic that you want to pass.
Low	The low security setting will allow all traffic except for known attacks. With low security, VersaLink is visible by other computers on the Internet.
Custom	Custom is a very advanced configuration option that allows you to edit the firewall configuration directly. Only the most expert users should try this.

H

Home Page

The home page gives you a quick summary of VersaLink's state. The following settings are displayed.

Home Page	
Connection Overview	The Connection Overview section displays the status of the DSL connection. The DSL must show a state of "**UP**" in order for VersaLink to communicate with your service provider's network.
Connection Name	The Connection Name section displays all of the connection profiles that are defined by VersaLink. A connection profile is information that VersaLink needs to establish a connection to your ISP. The "PPP Status" columns will show a status of "**UP**" if VersaLink is currently using that profile to communicate. The command button allows you to control the connection state.
Profile Editor	Selecting the "Profile Editor" link will allow you to define or change any of the connection profile settings.

L

LAN Configuration

This screen contains the setting that controls how VersaLink interacts with the local devices connected to VersaLink. Westell does not recommend that you change these settings. The following settings are displayed.

LAN Configuration	
Gateway IP Address	This controls the IP address that VersaLink uses for local communication.

Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address	This setting specifies the start of the IP address pool that VersaLink uses to assign IP addresses to local devices.
DHCP End Address	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DNS Server Enable	DNS stands for Domain Name System. This is an Internet standard that facilitates communication among devices. This allows a name to be used when specifying a device instead of an IP address. Normally you want this enabled.
DHCP Server Enable	DHCP stands for Dynamic Host Configuration Protocol. This is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this opt ion is set to Enabled.

LAN Statistics

This page contains information regarding the configuration and status of your Local LAN. The following settings are displayed.

LAN Configuration	
Device IP Address	This displays the IP address that VersaLink uses for local communication.
DHCP NetMask	This displays the subnet address that VersaLink's DHCP server issues in DHCP responses.
DHCP Start Address	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Server Status	Displays the status, "ON" or "OFF" of the DHCP Server
DHCP Server	Displays which network "Public" or "Private" the DHCP server is serving IP addresses for.
Devices on LAN	This page displays the current devices the modem has found on your LAN. The name of the device, the Ethernet MAC address, and the status, "Active" or "Inactive" is displayed in the table.

P

Private LAN

This page contains the settings that control how VersaLink interacts with the local devices connected to VersaLink. It is not recommended that these settings be changed. The following settings are displayed.

Private LAN	
Private LAN DHCP Server Enable	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
Private LAN Enable	This setting enables the Private NAT'ed interface. It is advised to leave this enabled.
Modem IP Address	This controls the IP address that VersaLink uses for local communication.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address (If	This setting specifies the start of the IP address pool that the modem uses to

DHCP is enabled for Private LAN)	assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled for Private LAN)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Lease (If DHCP is enabled for Private LAN)	This setting specifies the DHCP lease time.

Protocol

Protocol	
Protocol	This screen informs VersaLink which networking protocol to use when communicating with your ISP. This information is provided by your ISP.

Public LAN

This screen contains the settings that control how VersaLink interacts with the local devices connected to VersaLink. It is not recommended that these settings be changed. The following settings are displayed.

Public LAN	
Public LAN DHCP Server Enable	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
Public LAN Enable	This setting enables the Public interface. This feature allows a global subnet to exist behind your modem.
Modem IP Address	This controls the IP address that VersaLink uses for local communication.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address (If DHCP is enabled for Public LAN)	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled for Public LAN)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Lease (If DHCP is enabled for Public LAN)	This setting specifies the DHCP lease time.

Q

Quality of Service

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

R

Remote Access

This page allows you to configure your modem so that it can be configured remotely. Once enabled, this feature can be manually disabled, or it will automatically disable after 20 minutes of configuration inactivity.

Remote Access	
Password	This is the password a remote user must enter to access your modem's interface. It must be at least 4 characters long and contain no spaces.
URL	This field contains the URL that must be placed in a remote PC's web browser in order to communicate with your modem. If this field says "Not Connected," you are not currently connected to the Internet.
Enable Remote Access	When you have clicked on this button, entered a valid password, and connected to the Internet, Remote Access will be enabled.
Disable Remote Access	When you have clicked on this button, Remote Access will be disabled.

Routing Information Protocol

Remote Access	
RIP	RIP (Routing Information Protocol) is a widely-used protocol for managing VersaLink information within a self-contained network such as a corporate local area network or an interconnected group of such LANs.

S

Single Static IP

This page contains the settings that would allow the PPP address received from the network to be propagated to a single LAN device behind the modem.

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

T

Trace Route

The Trace feature allows you to perform an IP trace route to a remote computer either within or beyond the Internet service provider's network. Enter either the IP address or the hostname of the remote host computer into the input box to the right of the Trace button. If you trace by name, DNS will be used to look up the appropriate IP address for that name.

Trace	
Success	Trace will display its progress in the text box. Trace will show three round trip times and the DNS name (if available) of each intermediate VersaLink.
Failure	Trace will display "*" when it does not receive a response or cannot determine the DNS name of an intermediate Gateway. This is not necessarily an error, as some Gateways are configured to ignore trace route packets or do not have DNS name.

Turbo TCP

Turbo
Turbo TCP is a sophisticated network traffic prioritization and queuing method that dramatically improves the performance of downstream TCP/FTP/HTTP transfers under heavy upstream bandwidth utilization conditions. This feature first assigns a high priority to TCP signaling packets in the upstream direction, then places the packet in one of several transmit queues based on this priority. Packets of unspecified priority, like TCP or UDP data, are assigned a low priority and placed in a low priority queue. The packets in the high priority queues are then transmitted before packets in the lower priority queues minimizing any transmit delays. Minimizing the transmit delay of the TCP messages upstream enables the server to send the TCP data downstream faster, resulting in a substantial throughput gain.

U

Update Device

Update Device (Software Upgrade)	
Update Device (Software Upgrade)	This screen is used to upgrade VersaLink's application image. The application image is specified by entering in the filename or by using the browse button.

User Name

This screen is asks for information that will allow VersaLink to make a connection to the ISP on your behalf. VersaLink will need to know your Account ID and Account Password. This information is stored in VersaLink.

User Name	
Connection Name	This is a description of the default connection profile, which VersaLink will use. Feel free to use whatever description you desire.
Account ID	Your Account Id is supplied by your ISP and is a text string that uniquely identifies you with your ISP.
Account Password	The Account Password is a key phrase or text string that verifies your identify to the ISP.

V

VC Configuration

VC Configuration Screen	
VC Configuration	This screen is an advanced screen. Modifying parameters on this screen can cause severe disruption of your service. VC stands for "Virtual Connection." A VC identifies a connection through the service provider's ATM network to your ISP. It is not recommended that anything be changed on these pages unless explicitly instructed by your service provider.

VLAN

VC Configuration Screen	
VLAN	A virtual (or logical) LAN is a local area network with a definition that maps workstations on some other basis than geographic location.

VPI/VCI

VPI/VCI	
VPI/VCI	This screen asks for information that VersaLink needs to establish a communication channel to your ISP. The VPI and VCI values are supplied by your ISP.

W

Wireless Configuration

ACRONYMS	AP-Access Point BSSID-Basic Service Set ID FW-Firmware MAC-Media Access Controller NIC-Network Interface Card SSID-Service Set ID WEP-Wired Equivalent Privacy WLAN-Wireless Local Area Network
Network Name (SSID)	This string, (32 characters or less) is the name associated with the AP. To connect to the AP, the SSID on a Station card must match the SSID on the AP card or be set to "ANY."
Channel	The AP transmits and receives data on this channel. The number of channels to choose from is pre-programmed into the AP card. Station cards do not have to be set to the same channel as the AP; the Stations scan all channels, and look for an AP to connect to.
WEP Security **WEP (Wired Equivalent Privacy)**	The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. The WEP option can also be disabled. If so, any station can connect to the AP (as long as its SSID matches the AP SSID).
text only WEP Key	If selected, the WEP Key is treated as a string of text characters, and the number of characters must be either 5 (for 64-bit encryption) or 13 (for 128-bit encryption) or 29 (for 256-bit encryption). If not selected, the WEP key is treated as a string of hexadecimal characters, and the number of characters must be either 10 (for 64-bit encryption), 26 (for 128-bit encryption), or 58 (for 256-bit encryption). The only allowable hexadecimal characters are 0-9 and A-F. NOTE: The WEP key must be the same value and type for both Versa Link and the wireless network adapter. "Pass Phrase" is not the same as "text" and should not be used.
Enhanced Security	If selected, the SSID is hidden from detection in certain frames of the radio protocol. This makes the SSID harder to discover by external equipment capable of passively scanning the radio signal. Additionally, the station SSID must match the AP Network Name (SSID); the generic station SSID, "ANY" will be refused.

Data Rates (Mbits/s)	These are the allowable communication rates that the AP will attempt to use. The rates are broadcast within the connection protocol as rates supported by the VersaLink. If multiple rates are chosen, multi-rate communication and automatic optimum rate selection is possible. This is the default, and provides the most flexible system. If the Station signal strength or quality is poor, and the throughput of the connection is slow or intermittent, select only the lower two data rates (1 and 2 MB). This can improve performance by reducing the number of pad packets, re-tries and timeouts that could be occurring when the higher rates are automatically trying to be used. Lower rates can be maintained over longer distances and in a wider range of environments.

Wireless Station Configuration

The configuration of wireless stations must correspond with VersaLink's configuration. Typically, WLAN station cards come with a utility for changing the card configuration. Additionally, the WLAN driver might present configuration options as part of the Properties for the installed wireless network adapter. The following configuration items should be considered when setting up a station card.

SSID	This is a description of the default connection profile, which VersaLink will use. Feel free to use whatever description you desire.
Mode	The station's operating mode must be set to, Infrastructure. Most station configuration software will use this term to indicate operation with an AP. Other terms used are ESS or BSS. The terms Ad-Hoc or IBSS indicate operation without an AP; these terms should not be selected.
Tx Rate (Data Rate)	The station's transmission rate (data rate) should be set to Automatic. Selecting a specific data r ate is typically only done in difficult environments where conditions limit the maximum possible rate to less than 54 megabits per second.
Encryption	The station's encryption settings must match the AP's settings. This includes the settings for 64-bit, 128-bit, and 256-bit encryption (or none) and the WEP keys. Make certain that the key entries use the same format. The two typical formats provided are simple text entry and hexadecimal entry. Text entry is sometimes termed ASCII entry. **Hexadecimal entry is sometimes termed Hex or Manual entry. Do not use the Pass Phrase option if it is present.**
Authentication Algorithm	On the station, this setting is typically located under the Advanced properties for the wireless network adapter. Two or three algorithm settings are usually present. These might be termed: "Must use Shared for WEP," "Automatic based on WEP setting" and/or "WECA compliant." Select "Automatic based on WEP setting" or "Must use Shared for WEP."

Wireless Statistics

Network Name (SSID)	This string, (32 characters or less) is the name associated with the AP. To connect to the AP, the SSID on a Station card must match the SSID on the AP.
802.11b/g/g+ MAC Address (BSSID)	This is the Media Access Controller address of the AP. It is used as the Basic Service Set Identifier.
Primary FW	Primary firmware version number. This is read from the card and helps determine the AP firmware to use. The format of the number is: …>. The version number is also needed to identify existing errata.
Secondary FW	Secondary firmware version number. This is the station firmware that the

	card would use to operate as a wireless station. The format of the number is …>. The version number is needed to identify existing errata.
OUT and IN	Data preceded by **OUT** pertain to transmissions from VersaLink to a station; VersaLink is the source. Data preceded by **IN** pertain to data received by VersaLink; VersaLink 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 (an example would be a 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-Unicast Bytes	The number of bytes transmitted in Unicast Frames. This includes the header and body of each frame.
OUT-Multicast Bytes	The number of bytes transmitted in Multicast Frames. This includes the header and body of each frame or frame fragment.
OUT-Transmission Deferred	The number of frames (frame fragments) for which one or more transmission attempts were deferred to avoid a collision.
OUT-Frames after single retry	The number of frames that were successfully transmitted after one, and only one, retry. All fragments of the frame must have met this requirement if the frame was fragmented.
Wireless Statistics Cont.	
OUT-Frames after many 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. This number is a result of no acknowledgement or CTS received.
OUT-Discarded Frames	The number of transmit requests that were discarded to free up buffer space. This count is incremented when one of the following occurs: 1) A transmit request is queued too long on the transmit queue due to excessive retries, deferrals, scans, etc. 2) A transmit request is queued too long on the Power-Save queue because the station did not poll or wake up in time.
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 might 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-Unicast Bytes	The number of bytes received in Unicast Frames. This includes the header and body of each frame or frame fragment.
IN-Multicast Bytes	The number of bytes received in Multicast Frames. This includes the header and body of each frame of frame fragment.
IN-Packet not passing checksum	The number of received frames with a Frame Check Sequence (FCS) error.

IN-Drops due to insufficient Rx buffers	The number of received frames discarded due to lack of buffer space.
IN-Un-decryptable packets	The number of received frames (with the WEP sub-field set to one) that were discarded because the frame should not have been encrypted or the source station did not have privacy enabled.
IN-Messages received in message fragments	The number of frames received successfully while another good reception was going on above the carrier detect threshold (the message-in-message path #1 in the modem).
IN-Messages received in bad message fragments	The number of frames received successfully while another reception was going on above the carrier detect threshold, but with a bad or incomplete PLCP Preamble and Header (the message-in-message path #2 in the modem).

18. TECHNICAL SUPPORT INFORMATION

Contact your ISP for technical support.

19. WARRANTY AND REPAIRS

Westell warrants this product free from defects at the time of shipment. Westell also warrants this product fully functional for the period specified by the terms of the warranty. Any attempt to repair or modify the equipment by anyone other than an authorized Westell representative will void the warranty. For additional warranty information, contact your ISP, or contact the original provider of your DSL equipment.

20. PRODUCT SPECIFICATIONS

ADSL

- DSL Line Code: Discrete Multi-Tone (DMT)
- DSL Rates: 32 kbps to 8 Mbps downstream and 32 kbps to 800 kbps upstream
- Power spectral density: less than -34 dBm/Hz
- DSL Impedance: 100 Ohms
- DSL Performance: per ITU Recommendation G.991.2, ANSI T1.413
- Upgradeable to ADSL2, ADSL2+, READSL

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, 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, 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 card or USB adapter

LEDs

- Power
- LAN
- DSL
- Internet
- Ethernet
- Wireless

Connectors

- DSL: RJ-11, 6-pin modular jack-DSL
- Ethernet: RJ-45: 8-pin modular jack
- Power: Connector
- SMA antenna

Power

- Power Supply: External 120 VAC to 12 VDC 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

21. 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.

22. PUBLICATION INFORMATION

Westell ®VersaLink™ Small Business VersaLink (Model 327W15)
User Guide Part Number 030-300390 Rev. A
January 2004

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