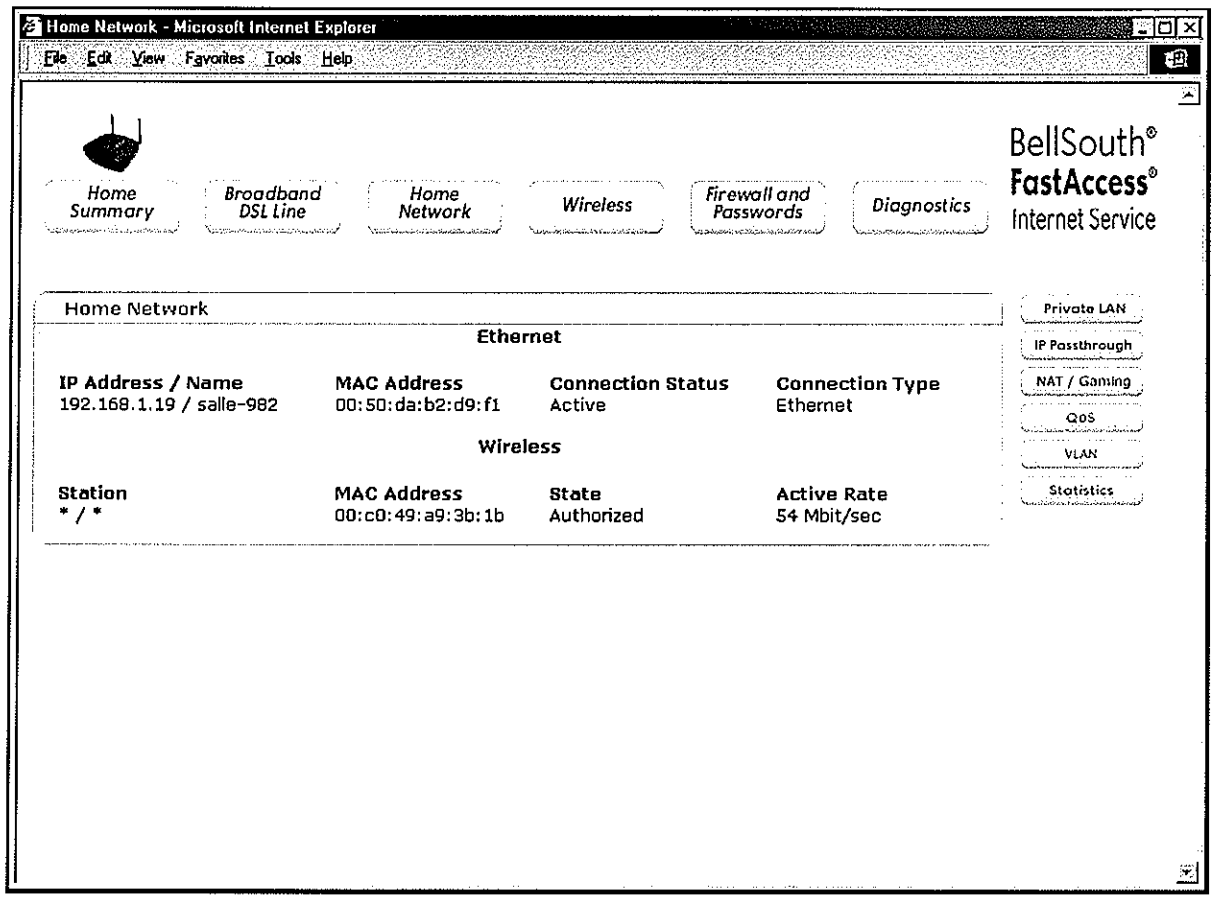
11. HOME NETWORK

If you click on **Home Network** at the main menu, the following page will be displayed. This page enables you to set up the network settings on your modem. To configure the settings, click the desired submenu button at the right of the page.

NOTE: If VersaLink is configured for **ETHERNET PORT 1** mode, the QoS and VLAN buttons will not be displayed in the **Home Network** page. You must configure VersaLink for **DSLATM PORT** mode to use these functions.

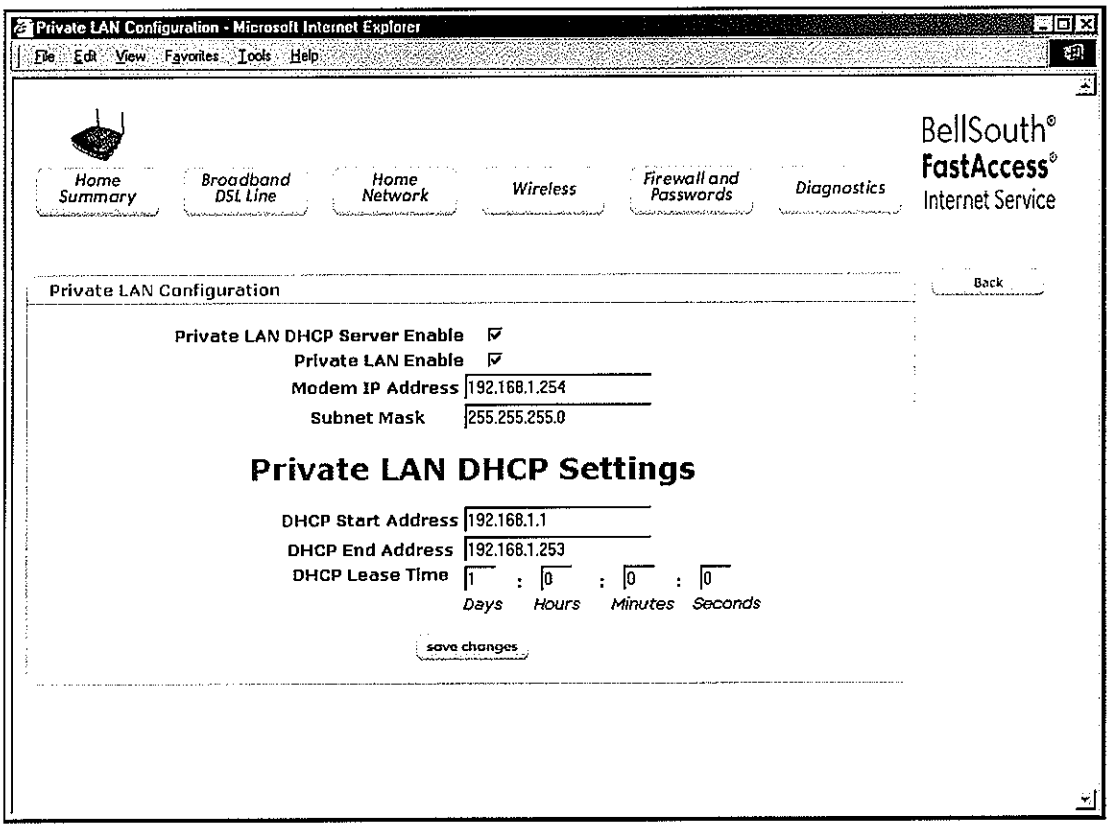


11.1 Private LAN

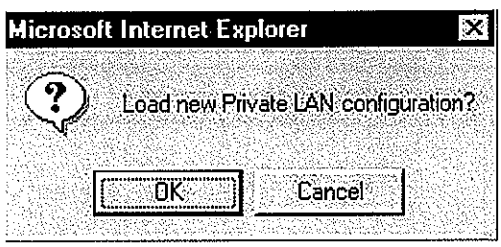
If you click the **Private LAN** button in the **Home Network** page, the following page will be displayed. (Private LAN is the default configuration for the VersaLink™ Gateway.)

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

If you change any settings in this page, click on **save changes** to allow the settings to take effect. Click the **Back** button to return to the **Home Network** page.



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



Private LAN Configuration	
Private LAN DHCP Server Enable	Default = CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Private LAN pool.
Private LAN Enable	Default = CHECKED If this box is CHECKED, it enables the addresses from the Private LAN to use the NAT interface.
Modem IP Address	Displays 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.
Private LAN DHCP Settings	
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: (Days:Hours:Minutes:Seconds). 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.

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

Warning Message	Check Private LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field
Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 59	Check the **Seconds** value in the DHCP Lease Time field
Minutes must be between 0 and 59	Check the **Minutes** value in the DHCP Lease Time field
Hours must be between 0 and 23	Check the **Hours** value in the DHCP Lease Time field

11.2 IP Passthrough/DMZ – Single Static IP Address Passthrough

If you click the **IP Passthrough** button in the **Home Network** page, the following **IP Passthrough/DMZ** page will be displayed. The **IP Passthrough/DMZ** page enables you to select the device on your LAN that will share your single static IP address. Before you begin this section, configure your PC settings to obtain an IP address from VersaLink automatically. (Refer to your Windows Help screen for instructions.)

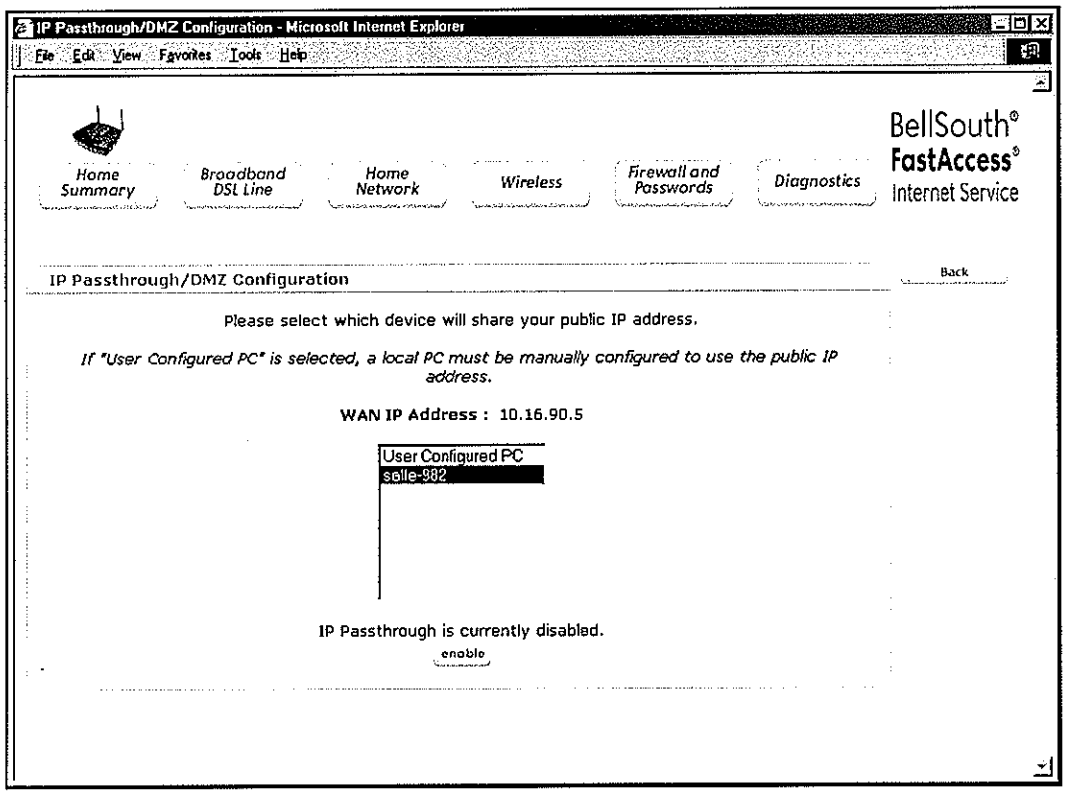
STOP: Static NAT must be disabled (if it has been previously enabled) before you can enable **IP Passthrough.** Refer to section 11.3.4.2 (Disabling Static NAT) for instructions on disabling Static NAT. After you have disabled Static NAT, return to the **IP Passthrough/DMZ Configuration** page.

NOTE: **IP Passthrough/DMZ** allows the user to share the WAN assigned IP address with one device on the LAN. When **IP Passthrough/DMZ** is configured on the modem, the device with the SSI becomes visible on the Internet. Network Address Translation (NAT) and Firewall rules do not apply to the device configured for SSI. If you are using the Bridge Ethernet protocol, **IP Passthrough/DMZ** configuration will not be available.

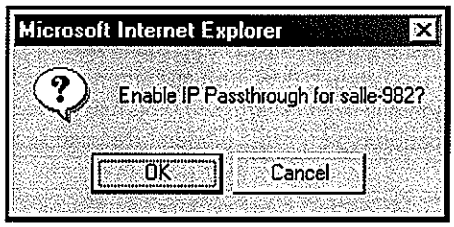
11.2.1.1 Enabling IP Passthrough/DMZ

To enable **IP Passthrough/DMZ,** go to the **Passthrough/DMZ Configuration** page and select a device from the options displayed in the window. Next, click on **enable.**

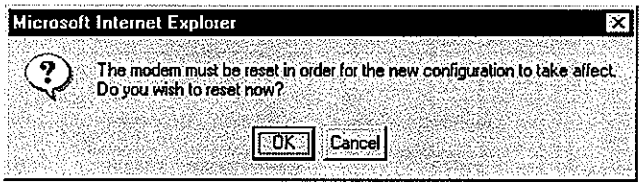
NOTE: If you select "User Configured PC," a local PC must be manually configured to have the Passthrough IP address.



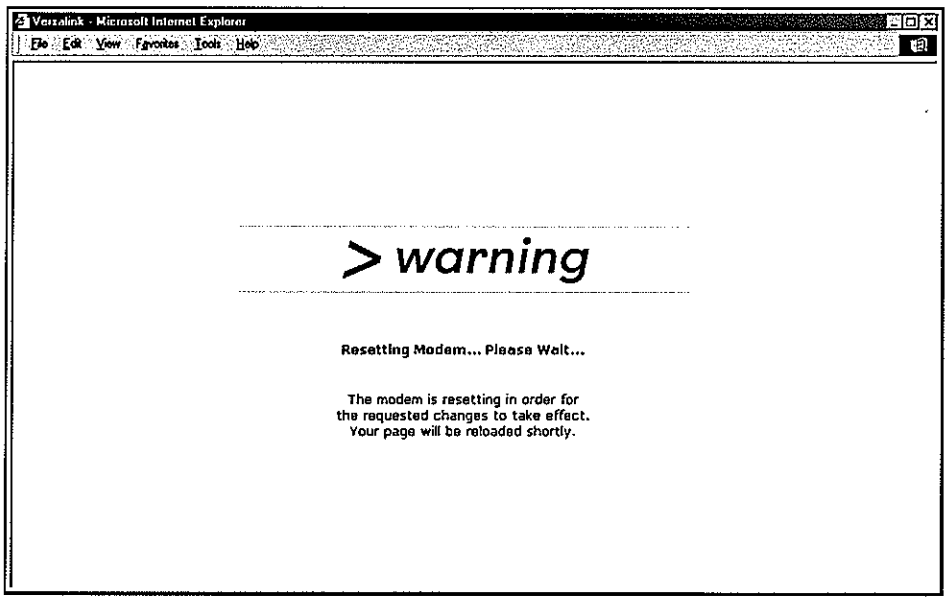
If you clicked on **enable,** the following pop-up screen will be displayed. Click **OK** to continue, or click **Cancel** to abort.



If you click **OK,** the modem must be reset in order for the new configuration to take effect. Click **OK** to reset now, or click **Cancel** to abort.

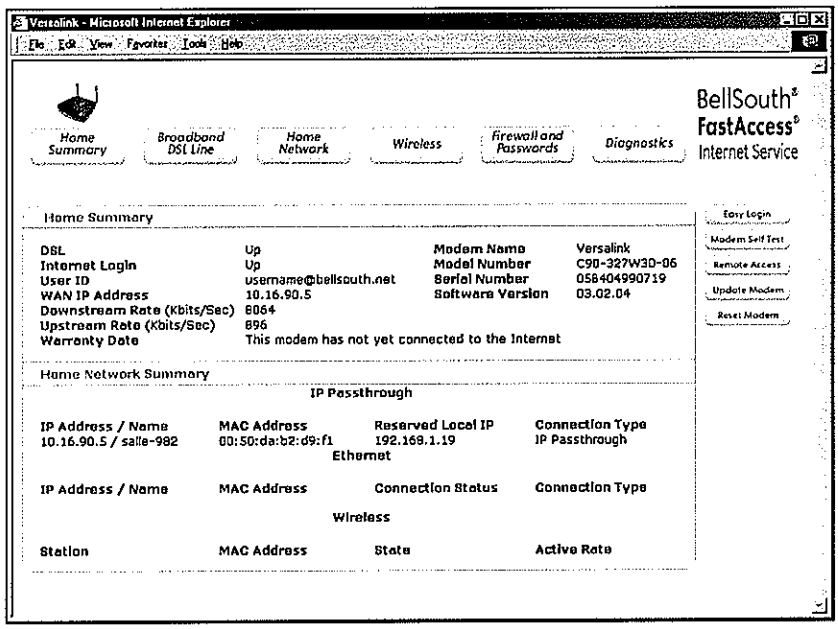


While the modem is resetting, the following screen will be displayed.

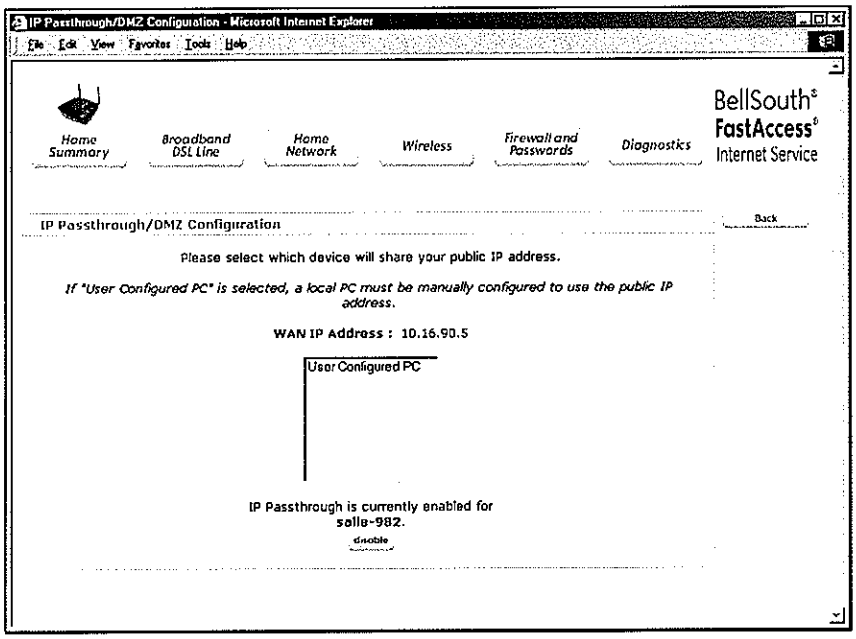


After the modem has been reset, the **Home Summary** page will be displayed. Confirm that the **DSL** and **Internet Login** fields display **Up**.

NOTE: If your Modem's connection type is set to "Always On" or "On-Demand," after a brief delay, an Internet connection (PPP session) will be established automatically and the **Home Summary** page will be displayed. If the connection type is set to "Manual," you must click the **Connect** button in the **Easy Login** page to establish an Internet connection. Once the Internet connection has been established, you may proceed with your modem's configuration. Always On is the factory default connection type for this modem. Refer to section 10.1 for details on connection type.

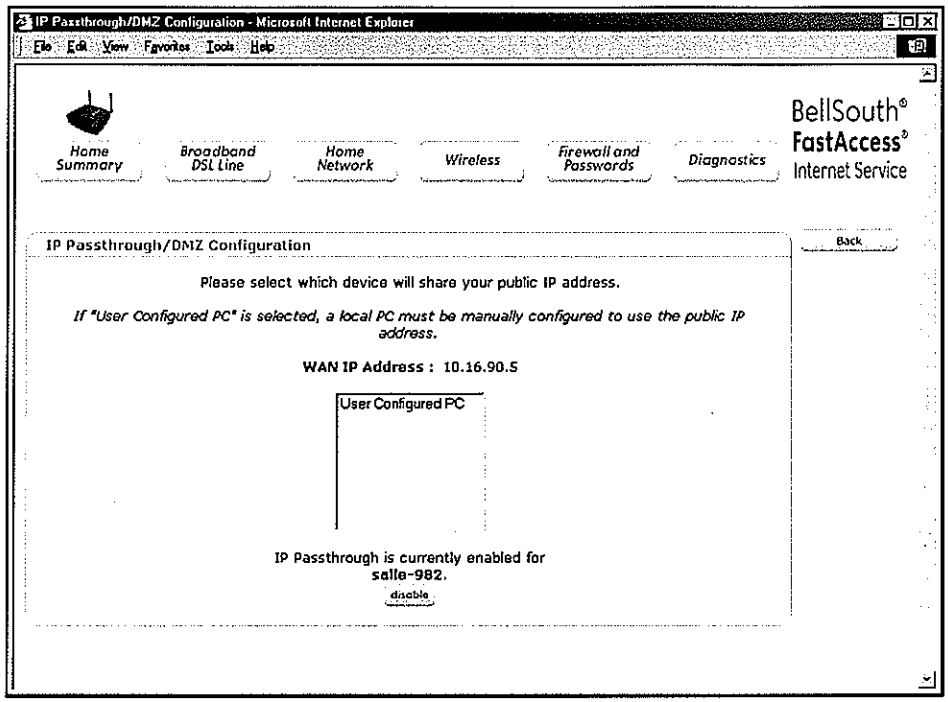


When IP Passthrough/DMZ is enabled, the following page will display the message "**IP Passthrough is currently enabled for**" and the device that you selected to share the public IP address.

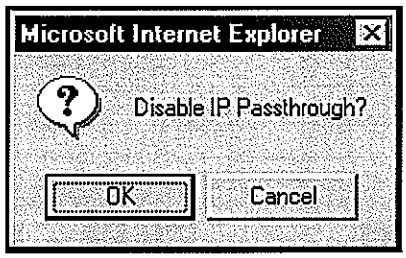


11.2.1.2 Disabling IP Passthrough/DMZ

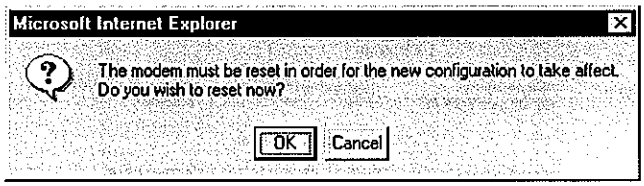
To disable **IP Passthrough/DMZ** (if it has been previously enabled), go to the **Passthrough/DMZ Configuration** page click on **disable.**



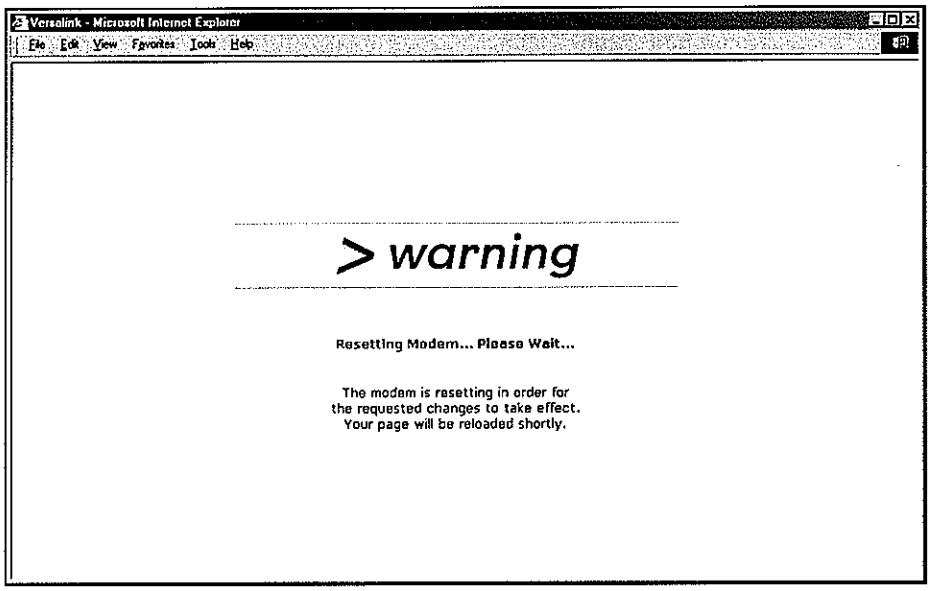
Next, click **OK** in the pop-up screen to disable IP Passthrough.



If you click **OK,** the modem must be reset in order for the new configuration to take effect. Click **OK** to reset now, or click **Cancel** to abort.

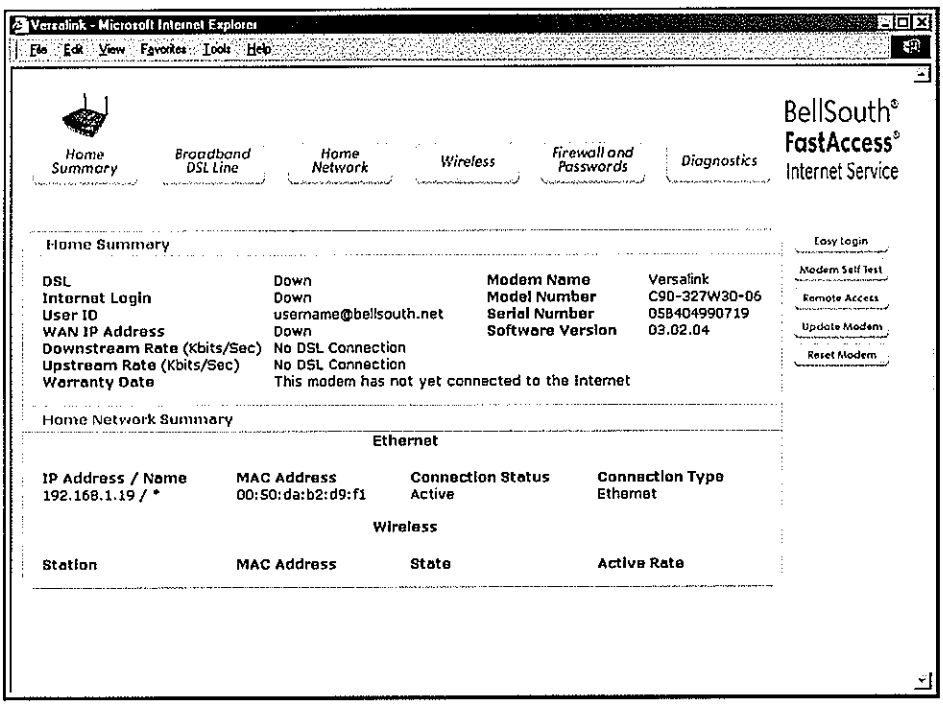


While the modem is resetting, the following screen will be displayed.

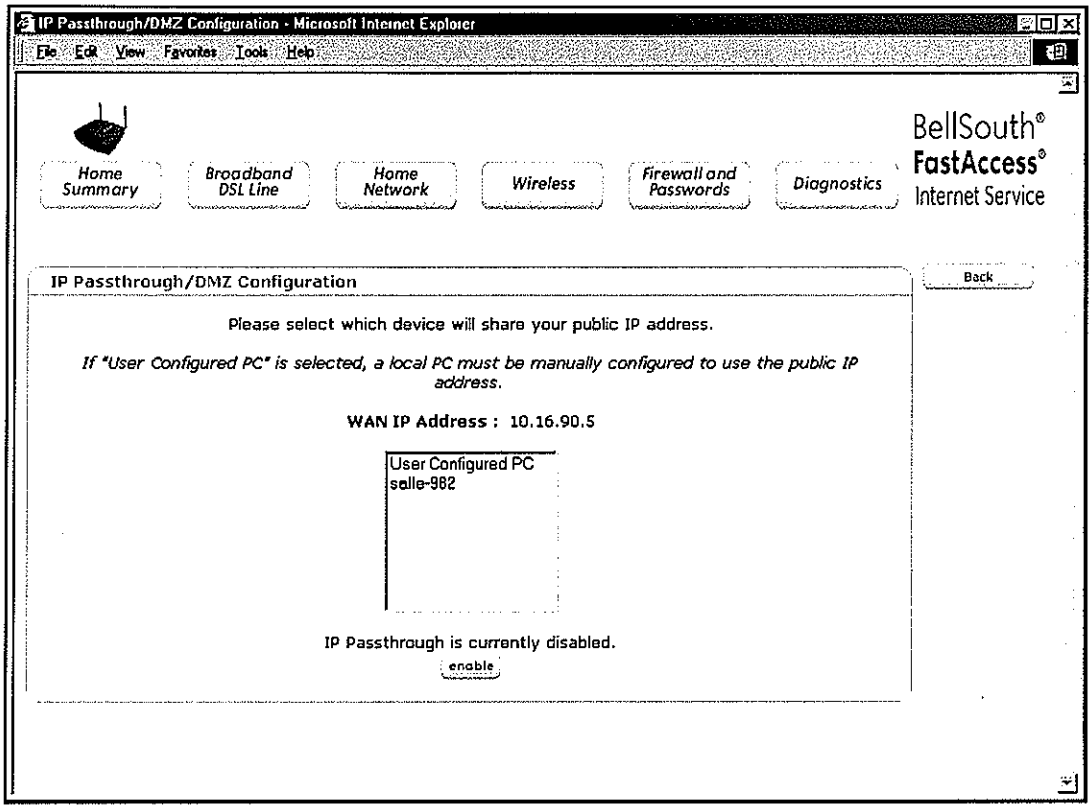


After the modem has been reset, the **Home Summary** page will be displayed. Confirm that the **DSL** and **Internet Login** fields display **Up** in the **Home Summary** page.

NOTE: If your Modem's connection type is set to "Always On" or "On-Demand," after a brief delay, an Internet connection (PPP session) will be established automatically and the **Home Summary** page will be displayed. If the connection type is set to "Manual," you must click the **Connect** button in the **Easy Login** page to establish an Internet connection. Once the Internet connection has been established, you may proceed with your modem's configuration. On-Demand is the factory default connection type for this modem. Refer to section 10.1 for details on connection type.



When IP Passthrough/DMZ is disabled, the following page will display the message "**IP Passthrough is currently disabled.**"

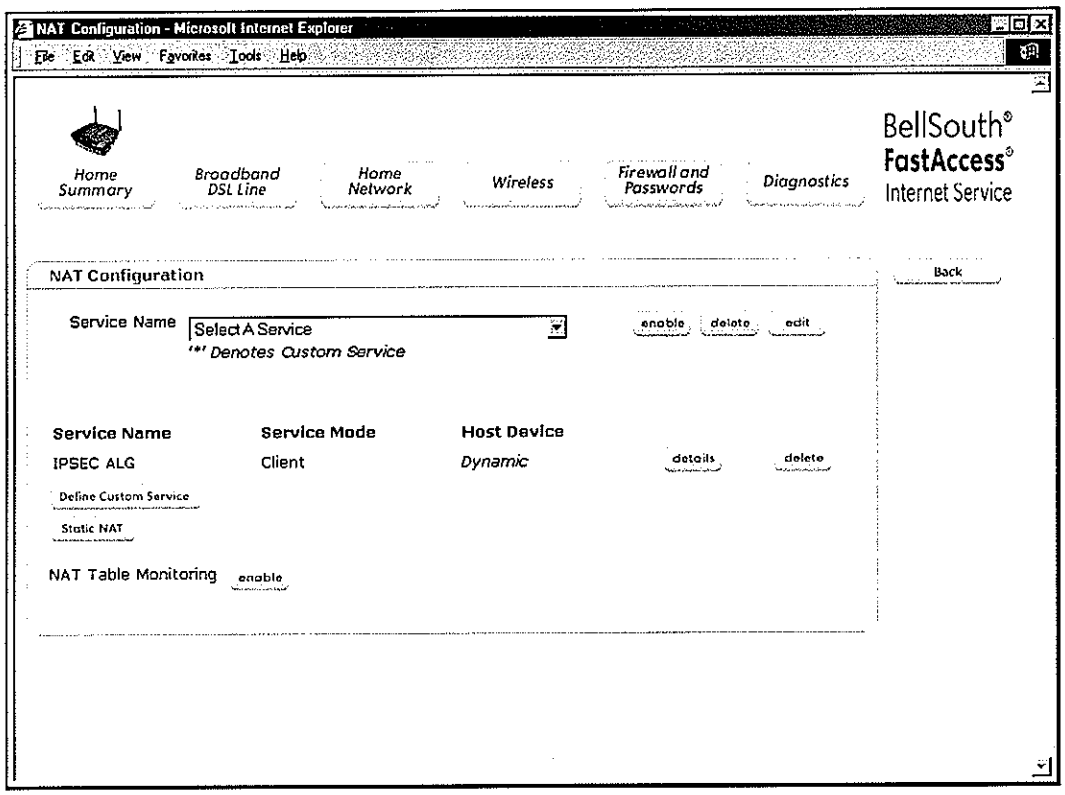


11.3 NAT/Gaming

If you click the **NAT/Gaming** button in the **Home Network** page, the following **NAT Configuration** page will be displayed. The **NAT Configuration** page enables you to set up NAT services for your modem.

Westell has developed an extensive list of NAT services, and you may select any service from this list. By selecting your specific NAT service and setting up a NAT profile, you will ensure that the appropriate ports on the modem are open and that the required application traffic can pass through your LAN. For a list of supported services, go to section 15 (NAT Services). You may add an unlimited number of NAT services.

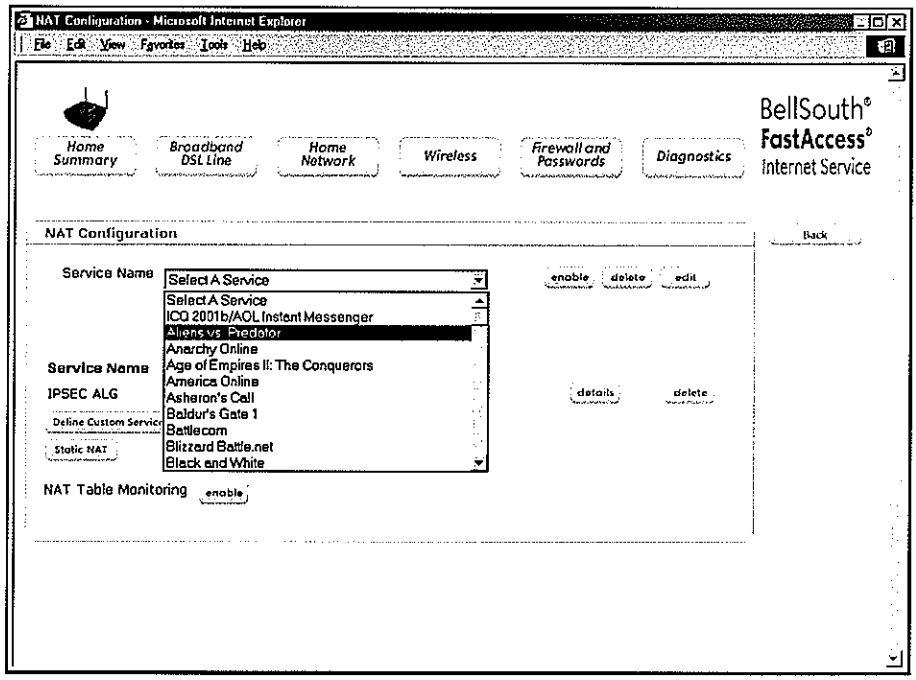
NOTE: The NAT/Gaming menu option will not be available if you are in Bridge Ethernet mode.



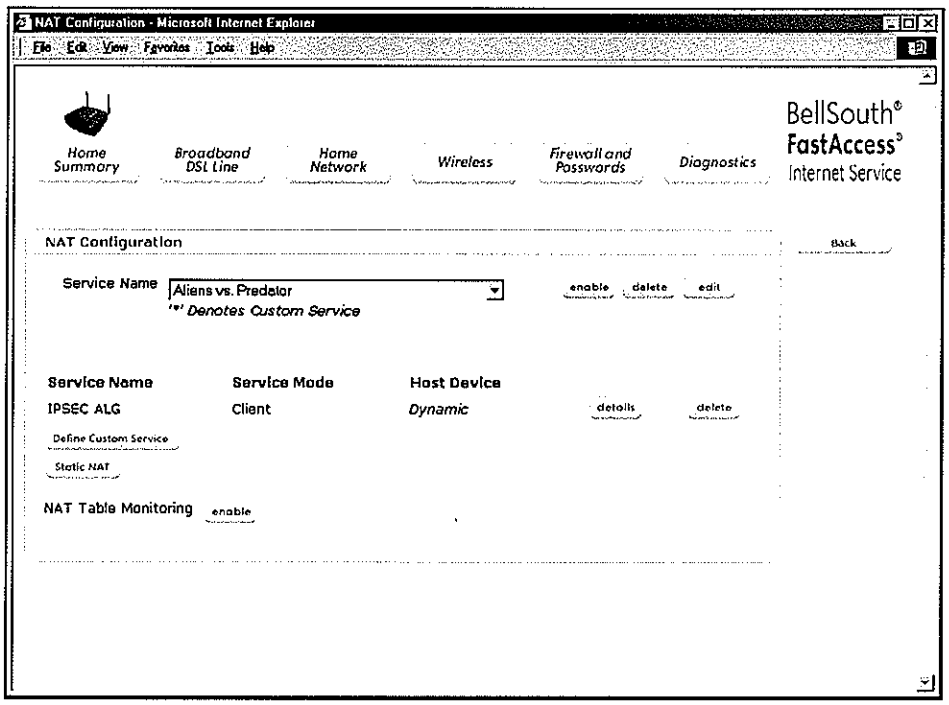
NAT Configuration	
Service Name	A drop-down menu of NAT (Network Address Translation) services that you can select from when you are ready to configure your modem for NAT service.
NAT Table Monitoring	Factory Default = Disabled If Enabled, this feature will monitor traffic on the ports.

11.3.1 Adding NAT Services

To add a NAT service, from the **NAT Configuration** page select a service from the **Service Name** drop-down menu.

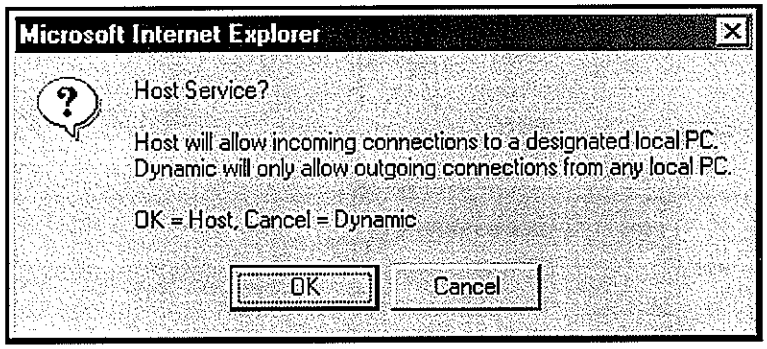


For example, the following page displays **Alien vs. Predator** as the NAT service selected. After you have selected a service, click the **enable** button adjacent to **Service Name.**



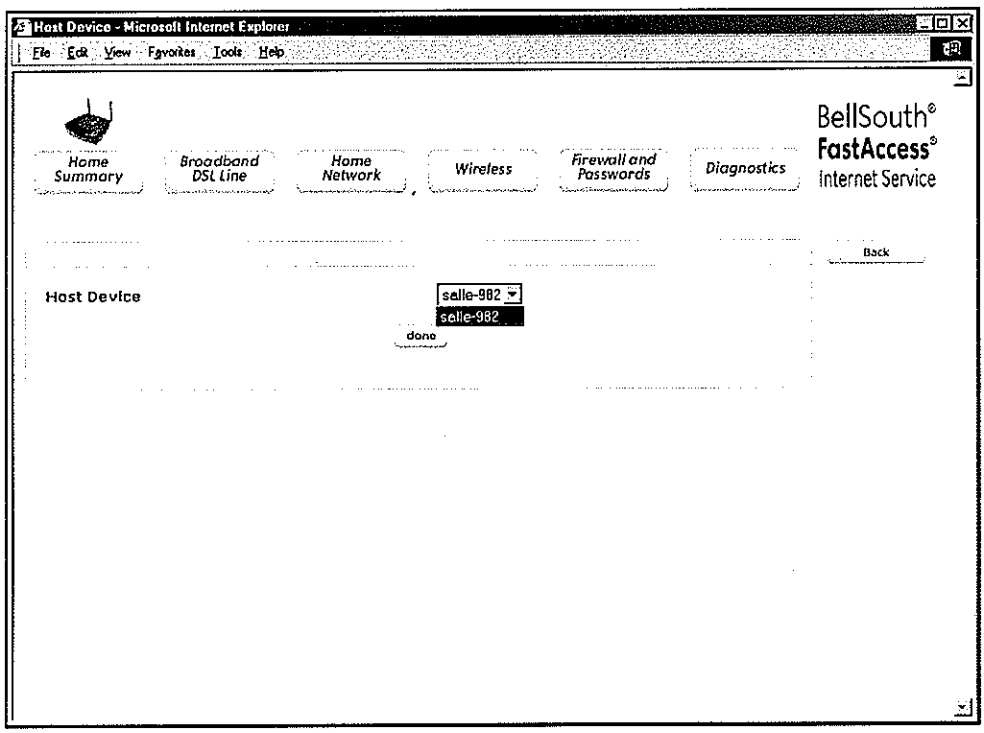
If you clicked **enable**, the following pop-up screen will be displayed. If you click **OK** in the pop-up screen, you will allow incoming connections to be forwarded to a designated local PC. If you click **Cancel**, you will allow only outgoing connections from any local PC. Click **OK** or click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

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

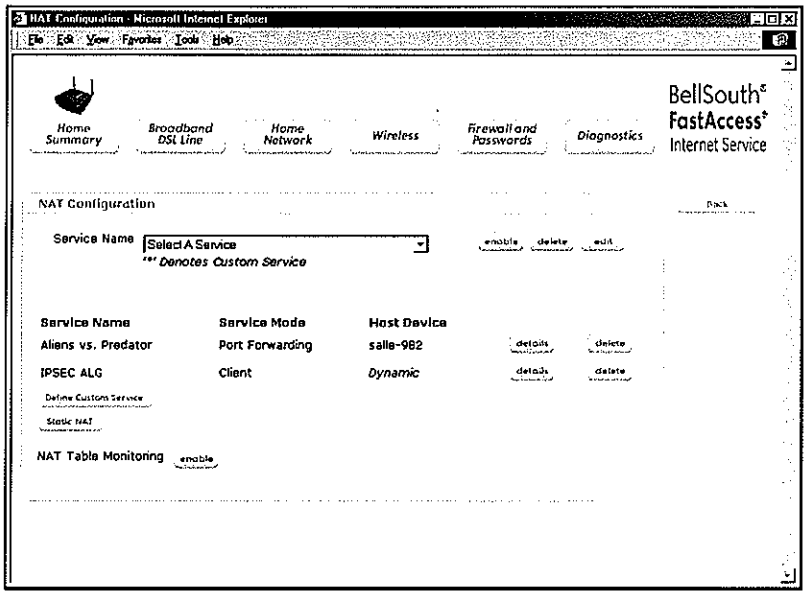


If you clicked **OK** in the preceding pop-up screen, the **Host Device** page will be displayed. The **Host Device** page will enable you to select which device will host the NAT service you selected on your local area network. After you have selected a device from the **Host Device** drop-down menu, click **done.**

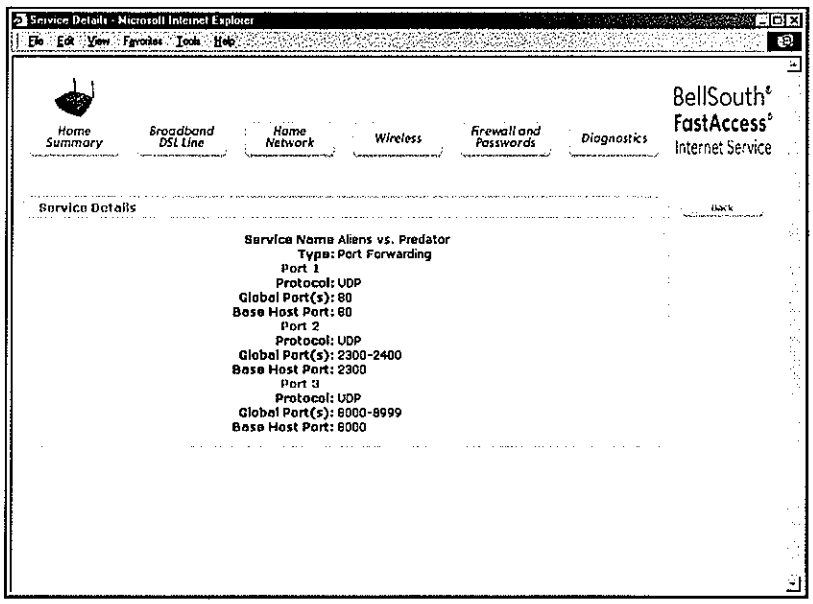
NOTE: You can add multiple NAT services. However, for each NAT service you want to add, you must first select the new NAT service as explained in the preceding paragraphs.



If you have selected a host device and clicked **done** in the preceding page, the following page will be displayed. It displays the NAT service that you have added.



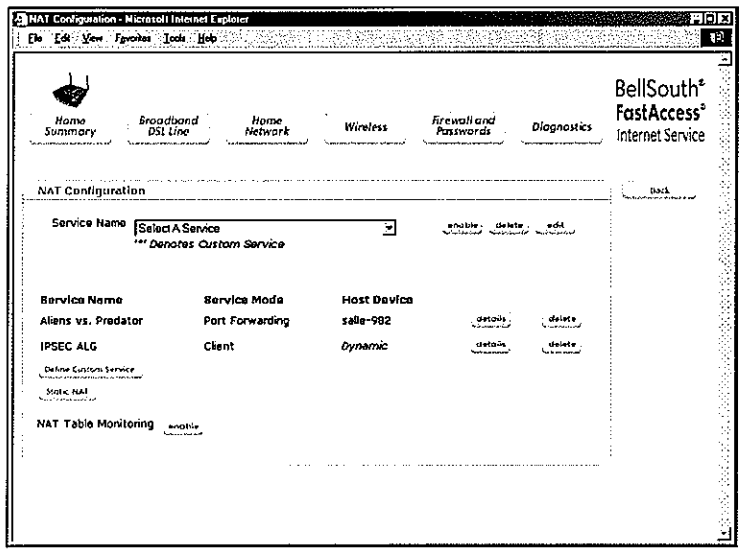
To view the details of a NAT service that you have added, click the **details** button adjacent to the desired NAT service. The following page will be displayed. It shows the details of the selected NAT service. Click the **Back** button to return to the **NAT Configuration** page.



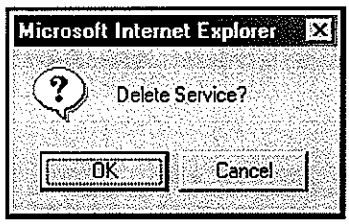
Service Details	
Service Name	The NAT service you selected
Type	The type of NAT service
Protocol	Traffic going from the modem to these ports
Global Port(s)	The type of Protocol used to run this NAT service
Base Host Port	Traffic going from the modem from these ports

11.3.2 Deleting NAT Services

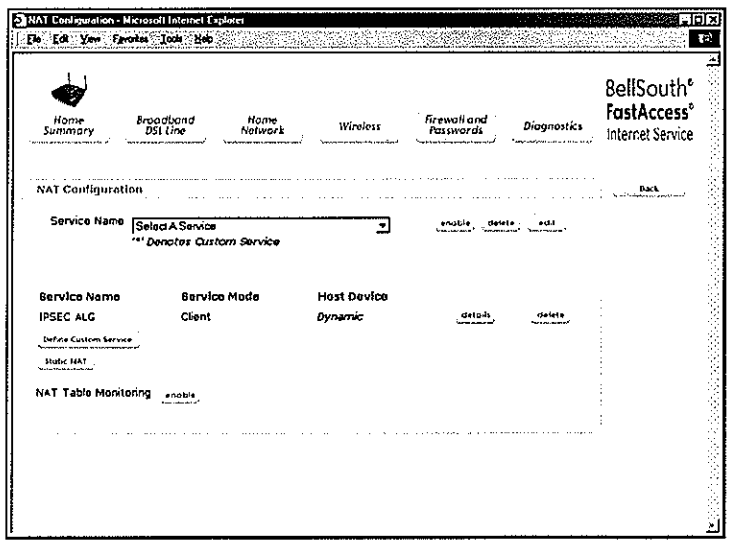
To delete a NAT service, at the **NAT Configuration** page click the **delete** button adjacent to the desired NAT service.



If you clicked on **delete,** the following pop-up screen will be displayed. Click **OK** to delete the service.



After the NAT service has been deleted, the following page will be displayed.

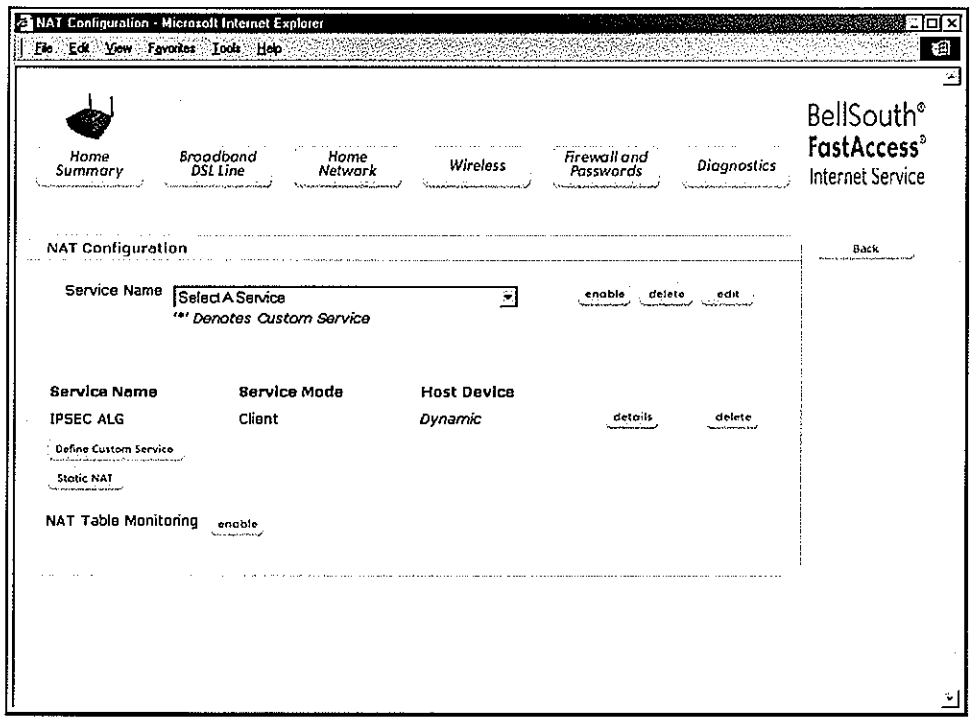


11.3.3 NAT Table Monitoring

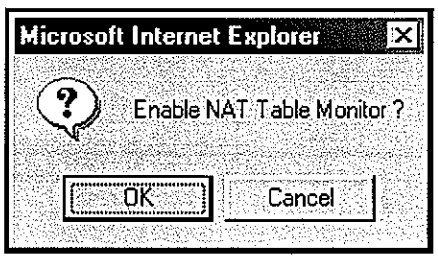
The **NAT Table Monitoring** feature enables all traffic on the ports to be monitored.

11.3.3.1 Enable NAT Table Monitoring

To enable NAT Table Monitoring, at the **NAT Configuration** page, click on the **enable** button adjacent to **NAT Table Monitoring.**

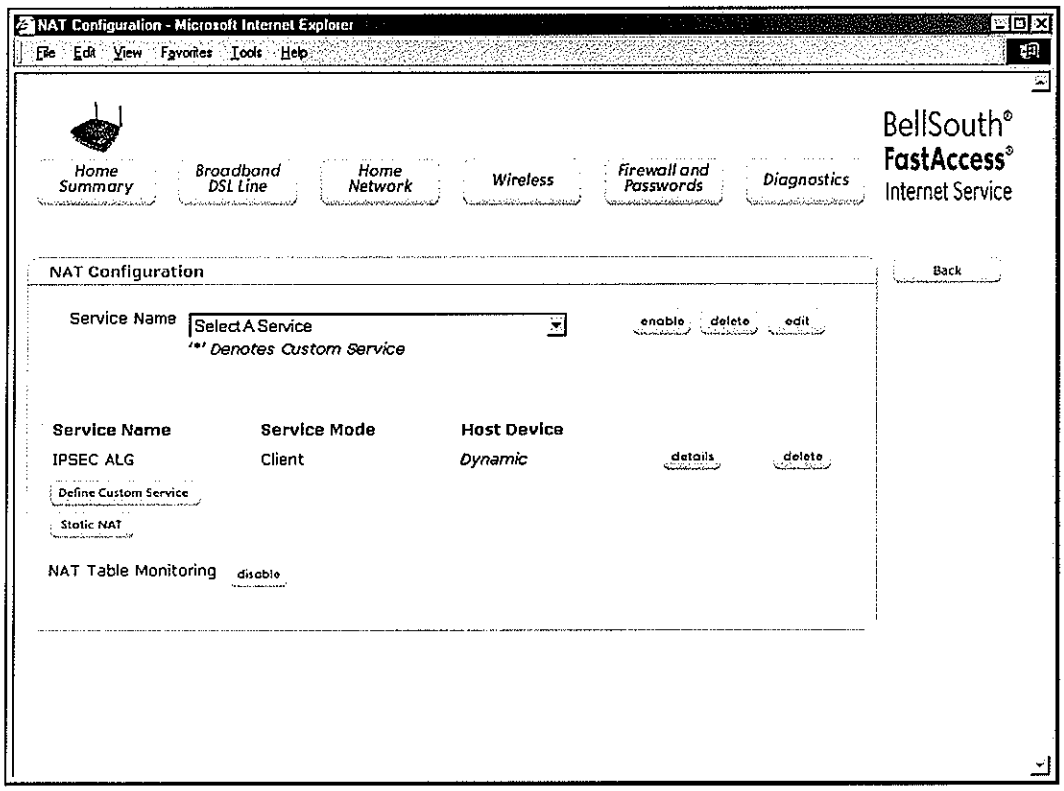


If you clicked the **enable** button, the following pop-up screen will be displayed. Click **OK** to enable NAT Table Monitoring.

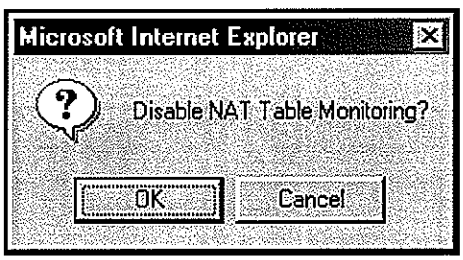


11.3.3.2 Disabling NAT Table Monitoring

To disable NAT Table Monitoring (if it was previously enabled), click the **disable** button adjacent to **NAT Table Monitoring**.



If you clicked the **disable** button, the following pop-up screen will be displayed. Click **OK** to disable NAT Table Monitoring.



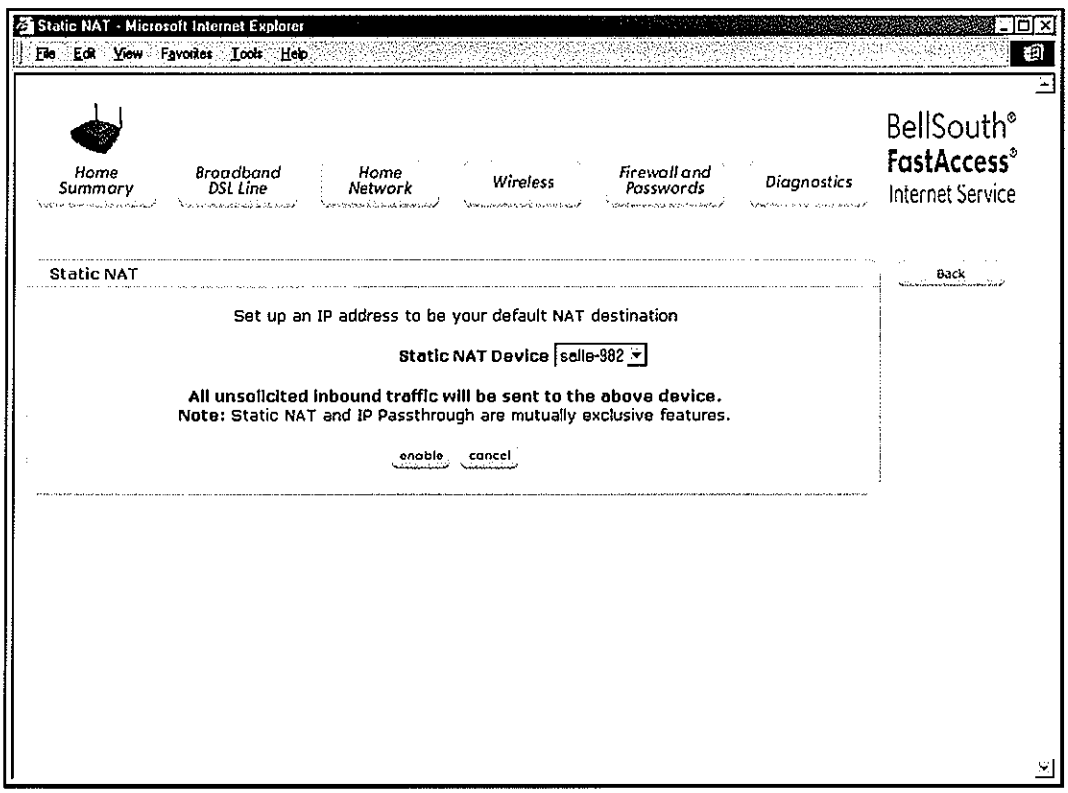
11.3.4 Static NAT

Static NAT enables you to configure the VersaLink to work with the special NAT services. This page enables you to select an IP address as your default NAT destination. When the modem is configured for Static NAT, any unsolicited packets arriving at the WAN will be forwarded to this device. This feature is used in cases where the user wants to host a server for a specific application.

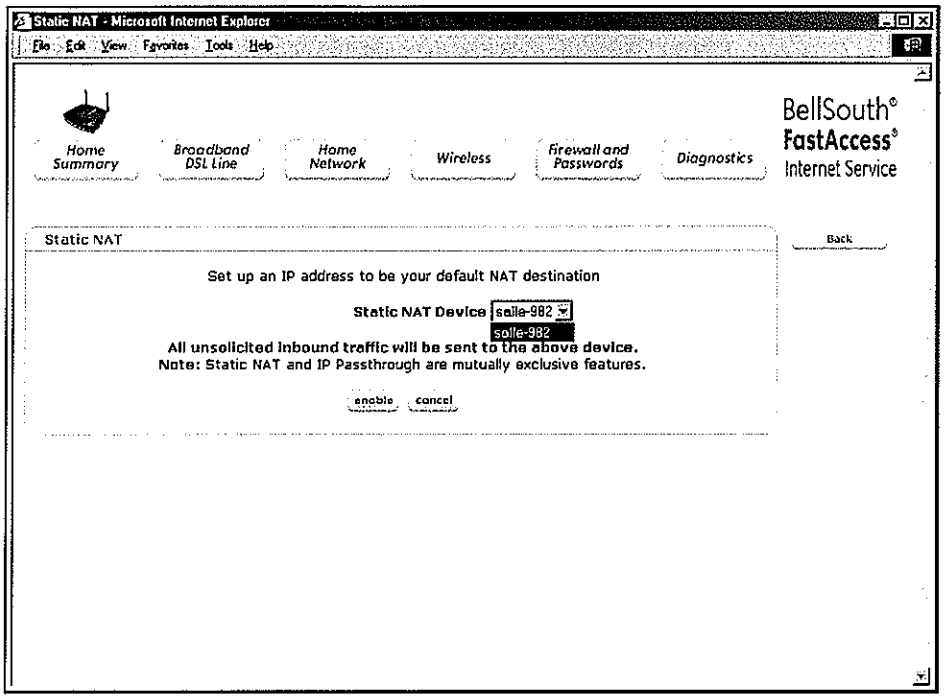
11.3.4.1 Enabling Static NAT

STOP: If Static NAT is enabled, all unsolicited inbound traffic will be sent to the device that you select as the Static NAT device. Static NAT and IP Passthrough are mutually exclusive features. **IP Passthrough/DMZ Configuration** must be disabled (if it has been previously enabled) before you configure **static NAT**. Refer to the section 11.2.1.2 (Disabling IP Passthrough/DMZ). After you have disabled IP Passthrough/DMZ and rebooted your computer, return to the **Static NAT** page by selecting **Home Network** at the main menu and then by clicking on **NAT/Gaming**.

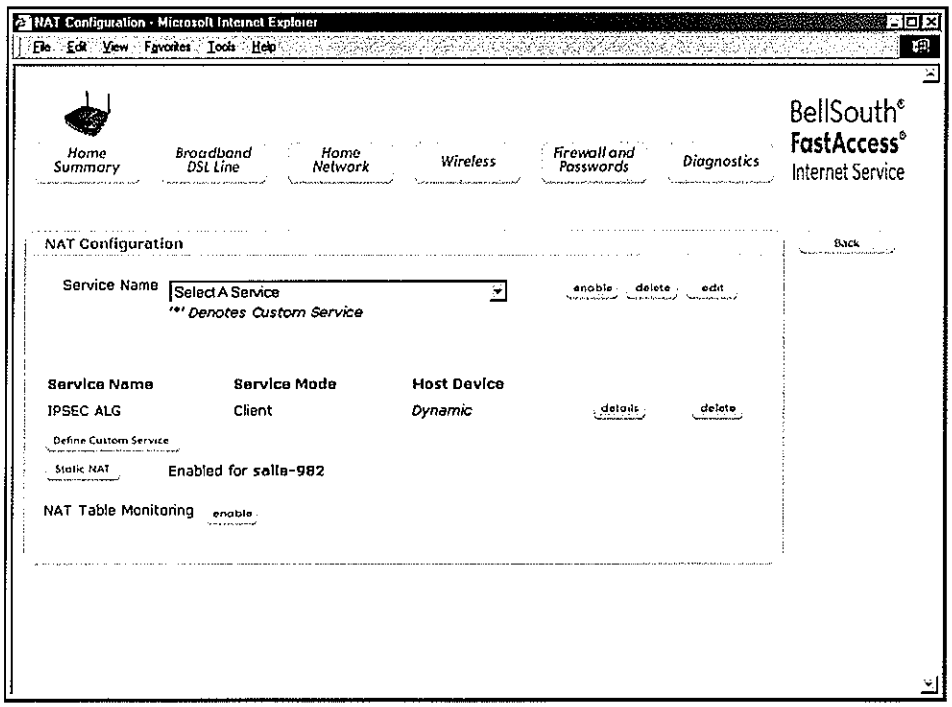
To enable Static NAT, click the **Static NAT** button at the **NAT Configuration** page. The following page will be displayed.



At the **Static NAT** page, choose the desired device from the **Static NAT Device** drop-down menu, and then click **enable**.

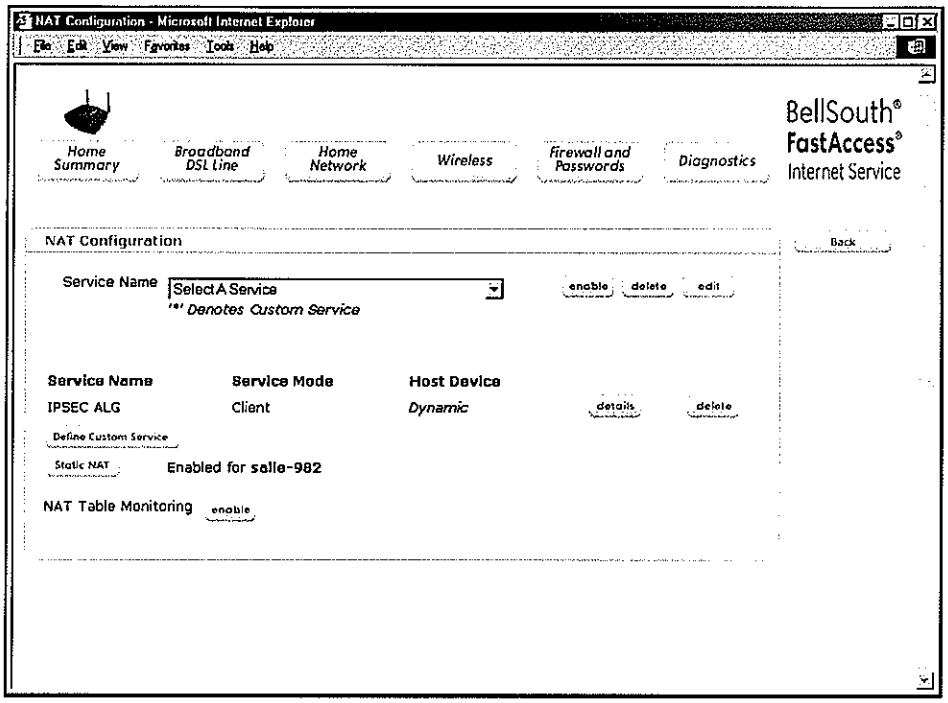


The following page displays the Static NAT device as enabled. If no devices are enabled for Static NAT, the field adjacent the **Static NAT** button will be blank.

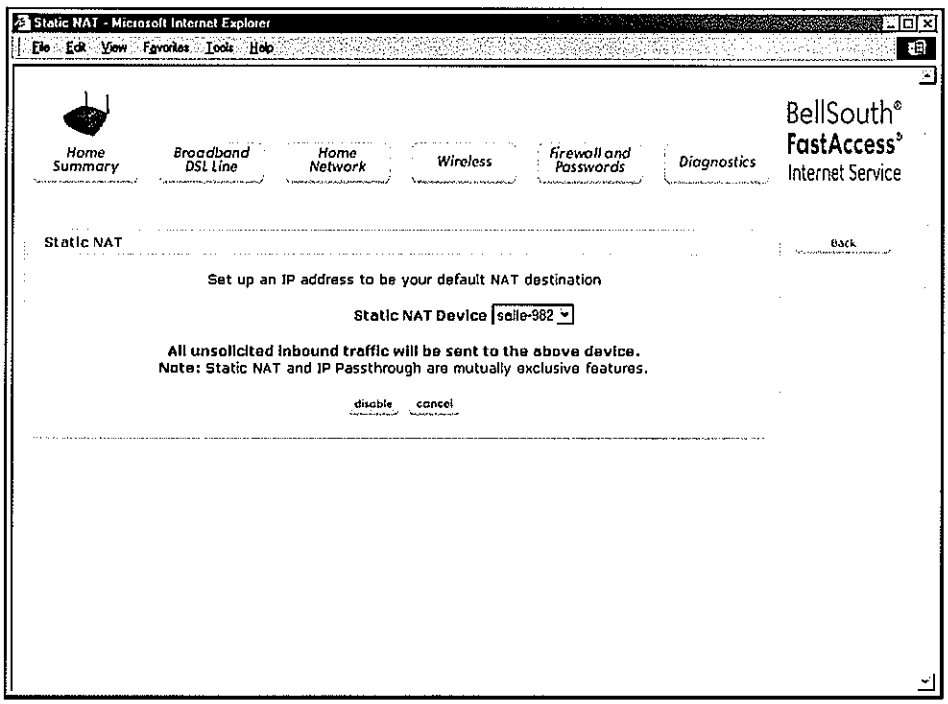


11.3.4.2 Disabling Static NAT

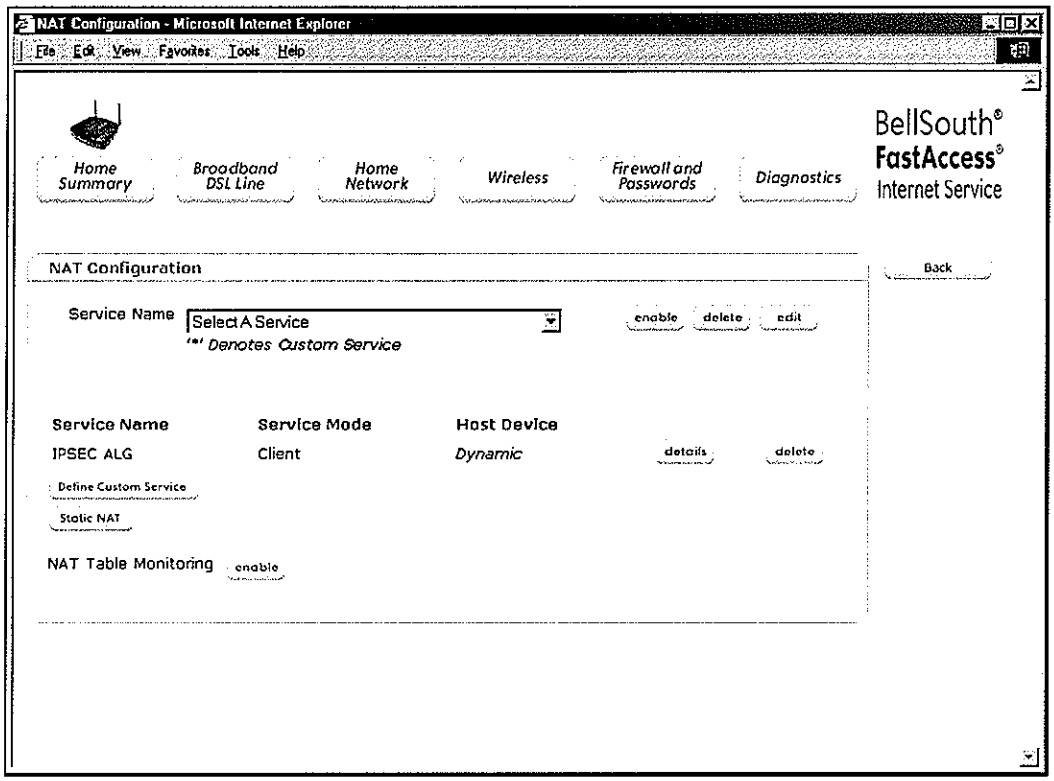
To disable Static NAT, click the **Static NAT** button at the **NAT Configuration** page.



If you clicked the **Static NAT** button, the following page will be displayed. Click the **disable** button to disable Static NAT.



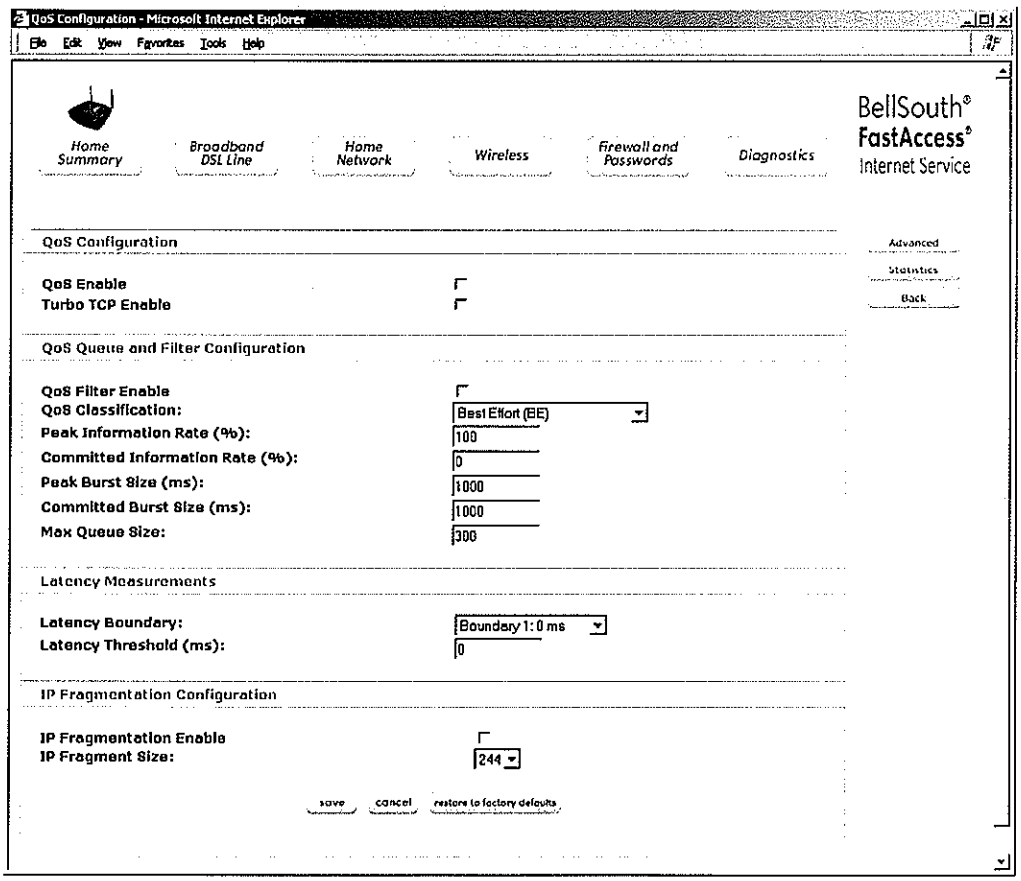
If you clicked **disable**, the following page will be displayed. (No device is displayed adjacent to the Static NAT button.)



11.4 QoS

If you click the **QoS** button in the **Home Network** page, the following page will be displayed. If you change any settings in this page, you must click the **save** button to allow the changes to take effect. If you click **cancel,** the changes that you have made to this page will not be saved and the previously saved settings will be displayed. If you click **reset to factory defaults,** the page will refresh and display the factory default QoS settings.

NOTE: The QoS feature helps ensure data integrity in high-speed transmissions. QoS provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QoS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay measurement bounds for each traffic class. If VersaLink is configured for **ETHERNET PORT 1**, mode the QoS function will not be available. You must configure VersaLink for **DSLATM** mode to use this function. Refer to section 10.4 for details. The QoS menu option will not be available if you are in Bridge Ethernet mode. QoS is only applied to packets being transmitted on the WAN.

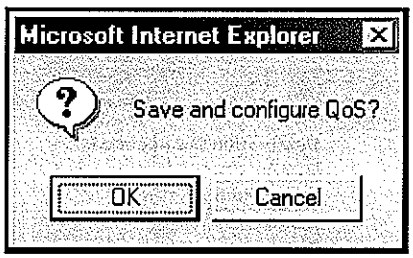


QoS Configuration	
QoS Enable	Factory Default = DISABLED If this box is checked, Quality of Service (QoS) will be Enabled.
Turbo TCP Enable	Factory Default = DISABLED If this box is checked, Turbo TCP will be Enabled. Turbo TCP does not function unless QoS is also Enabled.
QoS Queue and Filter Configuration	
QoS Filter Enable	Factory Default = DISABLED

	If this box is checked, this will Enable the QoS filters.
QoS Classification	This feature provides the capability to configure the bandwidth filter and queue size for a particular class of service. This menu selects which class of service is being configured. After packet classification, other QoS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay measurement 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 Rate (%)	The maximum allowed rate for this priority, expressed as a percentage of the DSL rate. This includes all overhead from the IP header to the ATM cell header. Packets received in excess of this rate are discarded.
Committed Information Rate (%)	The committed rate for this priority, expressed as a percentage of the DSL rate. Packets exceeding this rate but below the peak rate may have their Diffserv code point (DSCP) changed to increase the likelihood of their being dropped further upstream. The summation of all committed rates must be less than or equal to 100 percent.
Peak Burst Size (ms)	The interval in milliseconds for averaging the peak offered rate.
Committed Burst Size (ms)	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 menu selects a boundary for measuring the latency of packets in the modem. By default counts are kept for the number of packets whose latency are 0 to 10 ms, 10 to 20 ms, 20 to 40 ms, etc. Changing boundary 5 to 70 ms, for example, would cause counts covering the ranges 40 ms to 70 ms and 70 ms to 1000 ms instead of the usual 40 ms to 100 ms and 100 ms to 1000 ms. This allows more details to be reported on the statistics page for a particular latency range (that is, 40 ms to 70 ms). Possible responses are: Boundary 1:0 ms Boundary 2:10 ms Boundary 3:20 ms Boundary 4:40 ms Boundary 5:100 ms Boundary 6:1000 ms Boundary 7:3000 ms
Latency Threshold (ms)	The new value for the latency boundary selected in the menu.
IP Fragmentation Configuration	
IP Fragmentation Enable	Factory Default = DISABLED If this box is checked, IP Fragmentation will be Enabled. If Enabled and if EF packets are being sent, then lower priority packets that are bigger than the fragment size are: 1) Fragmented in the modem, if the "do not fragment" bit is set to 0 in the IP header, or 2) Discarded because the "do not fragment" bit is set to 1. In addition, and ICMP message is returned to the sender, indicating that the packets is too big.

	Fragmentation stops when no EF packets have been seen for the last few seconds.
IP Fragment Size	This is the IP Fragment Size. Possible responses are: 100, 148, 244, 292, 340, 388, or 436

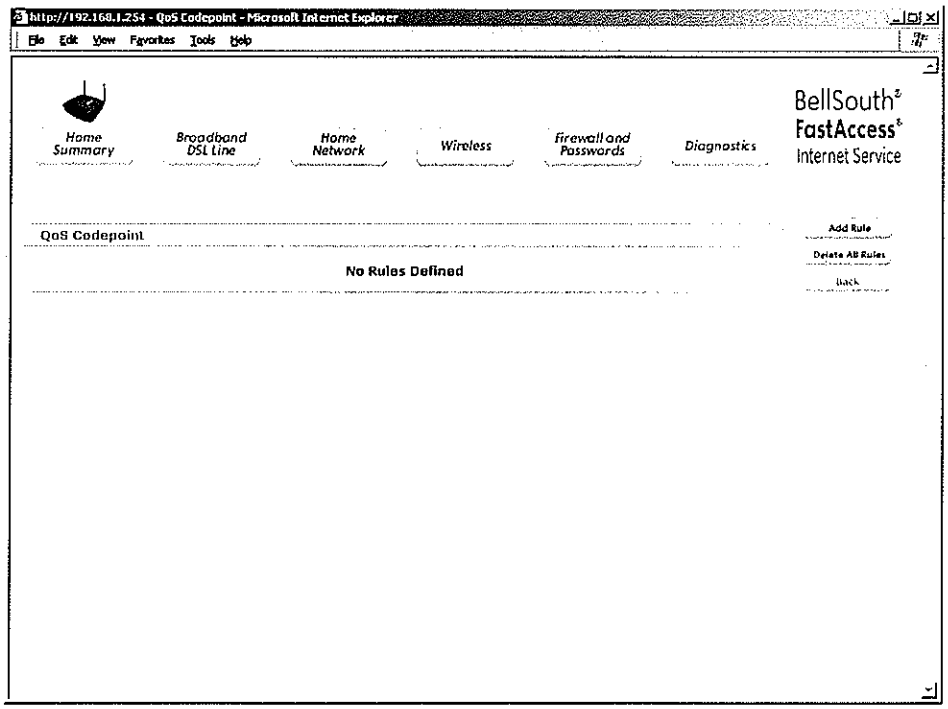
If you made changes to the **QoS Configuration** page and clicked on **save,** the following pop-up screen will be displayed. Click on **OK.** This will save your new QoS settings.



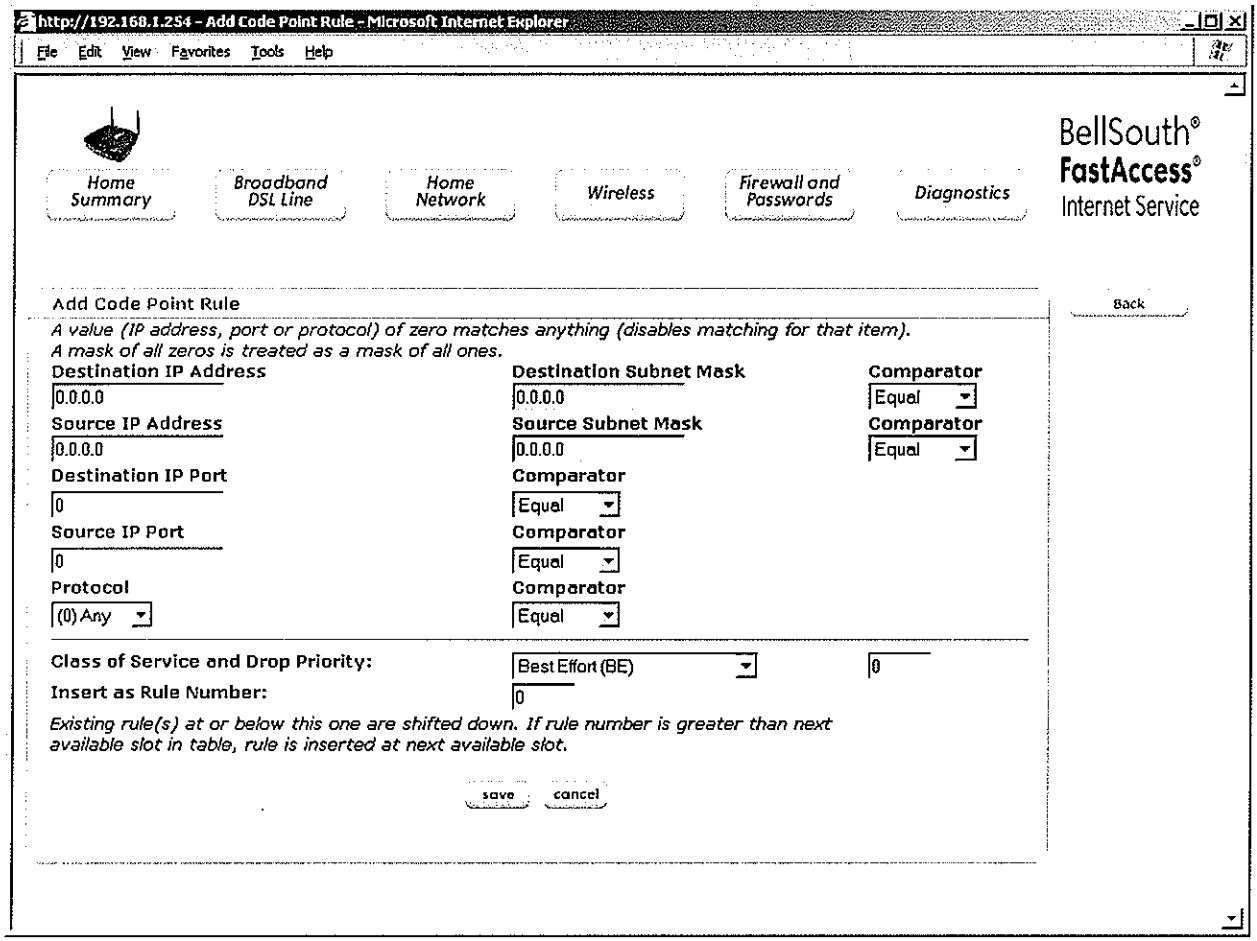
11.4.1 Advanced

If you click the **Advanced** button in the **QoS Configuration** page, the following page will be displayed. This page enables you to add rules to the QoS Codepoint. Click on **add rule.**

NOTE: You may add up to 40 QoS codepoint rules.



If you clicked **add rule,** the following page will be displayed.

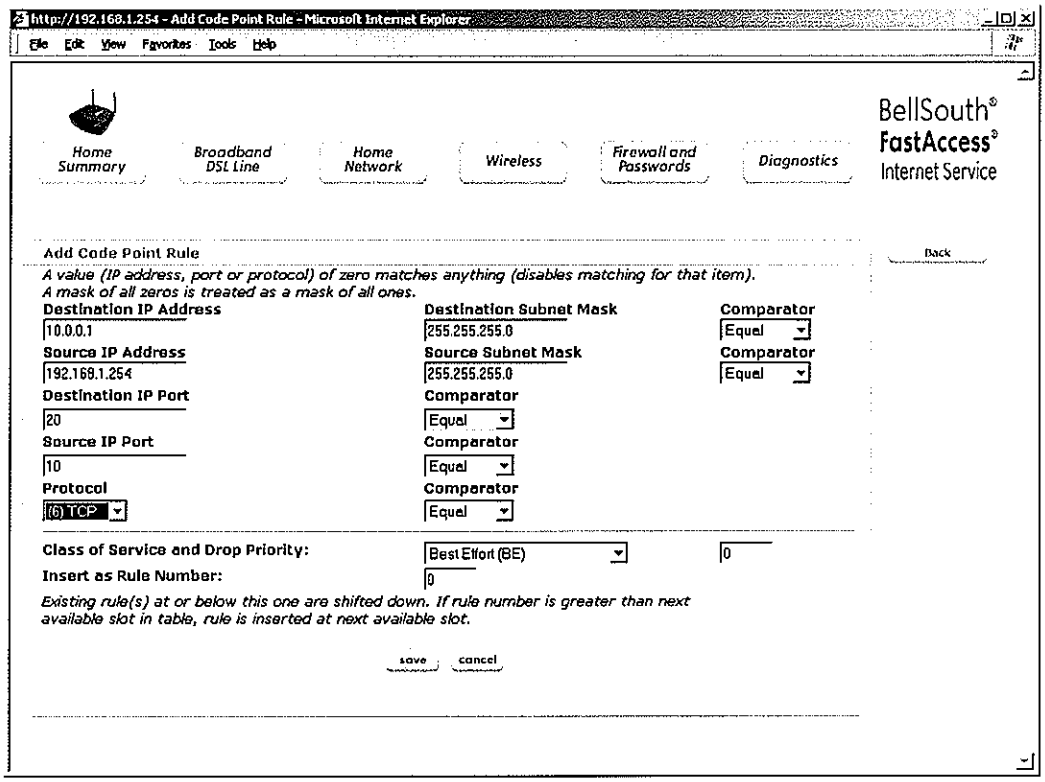


Add Code Point Rule	
Destination IP Address	The destination IP Address. The value 0 means that this data item is not used for matching purposes.
Source IP Address	The source IP Address. The value 0 means that this data item is not used for matching purposes.
Destination IP Port	The destination IP Port. The value 0 means that this data item is not used for matching purposes.
Source IP Port	The source IP Port. The value 0 means that this data item is not used for matching purposes.
Protocol	The IP Protocol. The value 0 means that this data item is not used for matching purposes.
Destination Subnet Mask	The mask for the destination IP Address.
Source Subnet Mask	The mask for the source IP Address.
Comparator	This determines whether the rule will match a packet whose data equals the value specified or will match a packets whose data does not equal the value specified. Possible responses are: Equal Not Equal
Class of Service and Drop Priority	The new class of service and drop priority. The minimum drop priority for EF is 6. The minimum drop priority for the AF classes is 2.

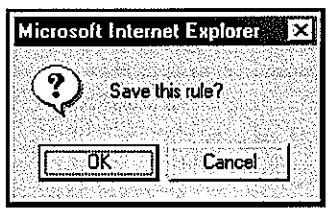
Insert as Rule Number	The rule number that you assign to the rule (0,1,2,3, etc.) Note: Existing rule(s) at or below this one are shifted down. If the rule number is greater than the next available slot in the table, the rule is inserted in the next available slot.

NOTE: A default rule where all data items have values of 0 will match any packet. Since rules are applied in order and the process stops with the first match, any default rule should be the last rule on the list.

Enter the appropriate values in the fields provided, and then click **save** to save the settings. If you click **cancel,** this page will be reset to the previously saved settings.

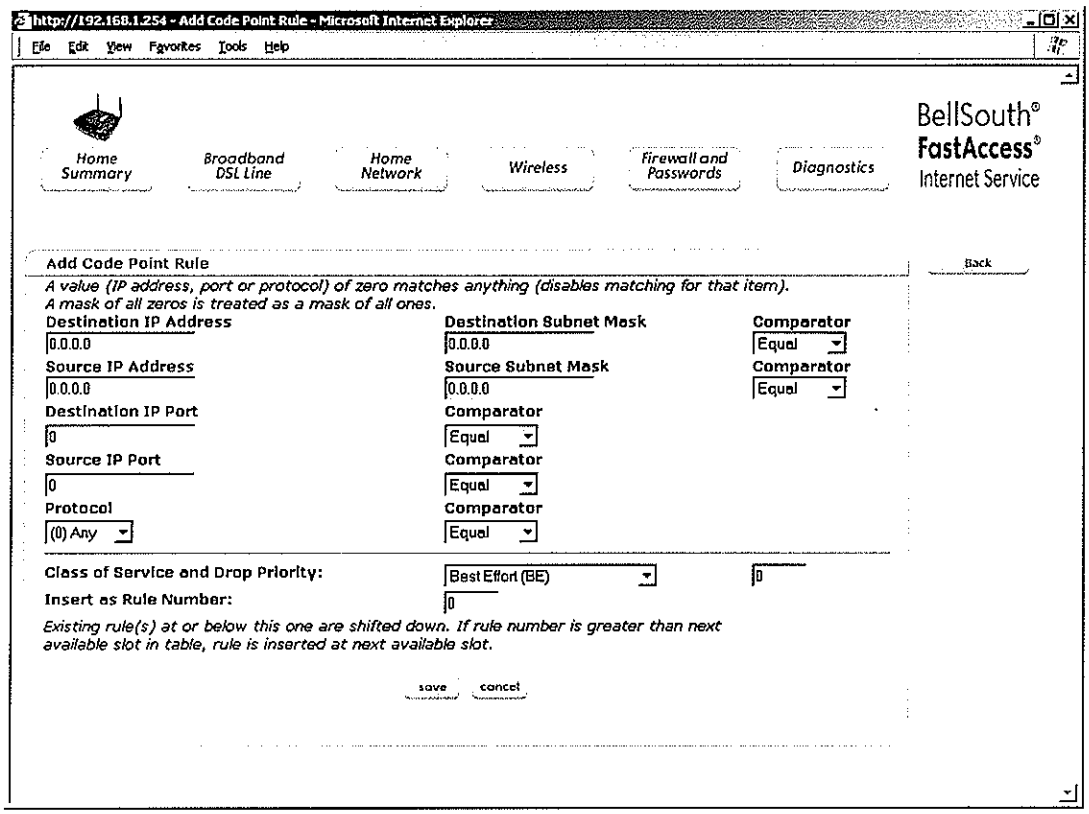


If you changed any settings and clicked on **save** in the preceding **Add Code Point Rule** page, the following pop-up screen will be displayed. Click **OK** to continue.

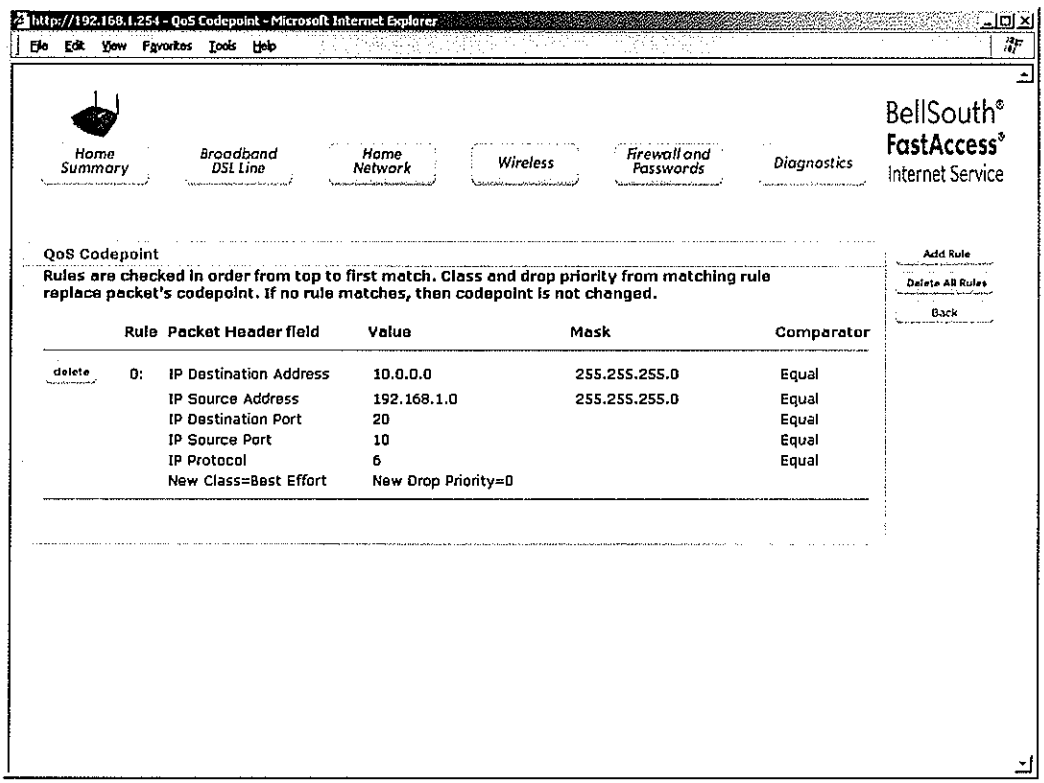


If you clicked **OK** in the preceding pop-up screen, the following page will be displayed. Click the **Back** button to view the saved rule in the **QoS Codepoint** page.

NOTE: After you have clicked **OK** in the preceding pop-up (to save a rule that you have added), the **Add Code Point Rule** page will be displayed with values reset to zero. If you want, you may now add another rule and click **save** to save the rule. To display the saved rules, click on **Back** in the **Add Code Point Rule** page.

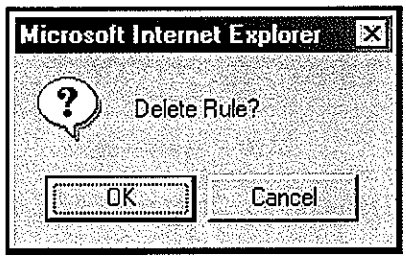


If you clicked the **Back** in the **Add Code Point Rule** page, the following **QoS Codepoint** page will be displayed. You may (1) click the **delete** button adjacent to the rule that you wish to delete, (2) click on **Add Rule** to add a rule, or (3) click on **Delete All Rules** to delete all rules in the **QoS Codepoint** page.

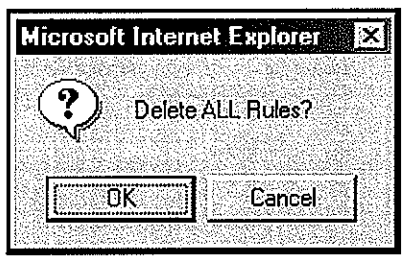


QoS Codepoint	
Rules are checked in order from top to first match. Class and drop priority from matching rule replace packet's Diffserv codepoint. If no rule matches, then codepoint is not changed.	
Rule	The rule number that you assigned to the rule (0,1,2,3, etc.)
Pkt Header field	The data item(s) used for matching by this rule.
Value	The value of the data item to match.
Mask	The subnet mask used for comparing IP Addresses.
Comparator	This determines whether the rule will match a packet whose data equals the value specified or will match a packets whose data does not equal the value specified. Possible responses are: Equal Not Equal

If you clicked on a **delete** button in the **QoS Codepoint page,** the following pop-up screen will be displayed. Click **OK** to delete the selected rule.

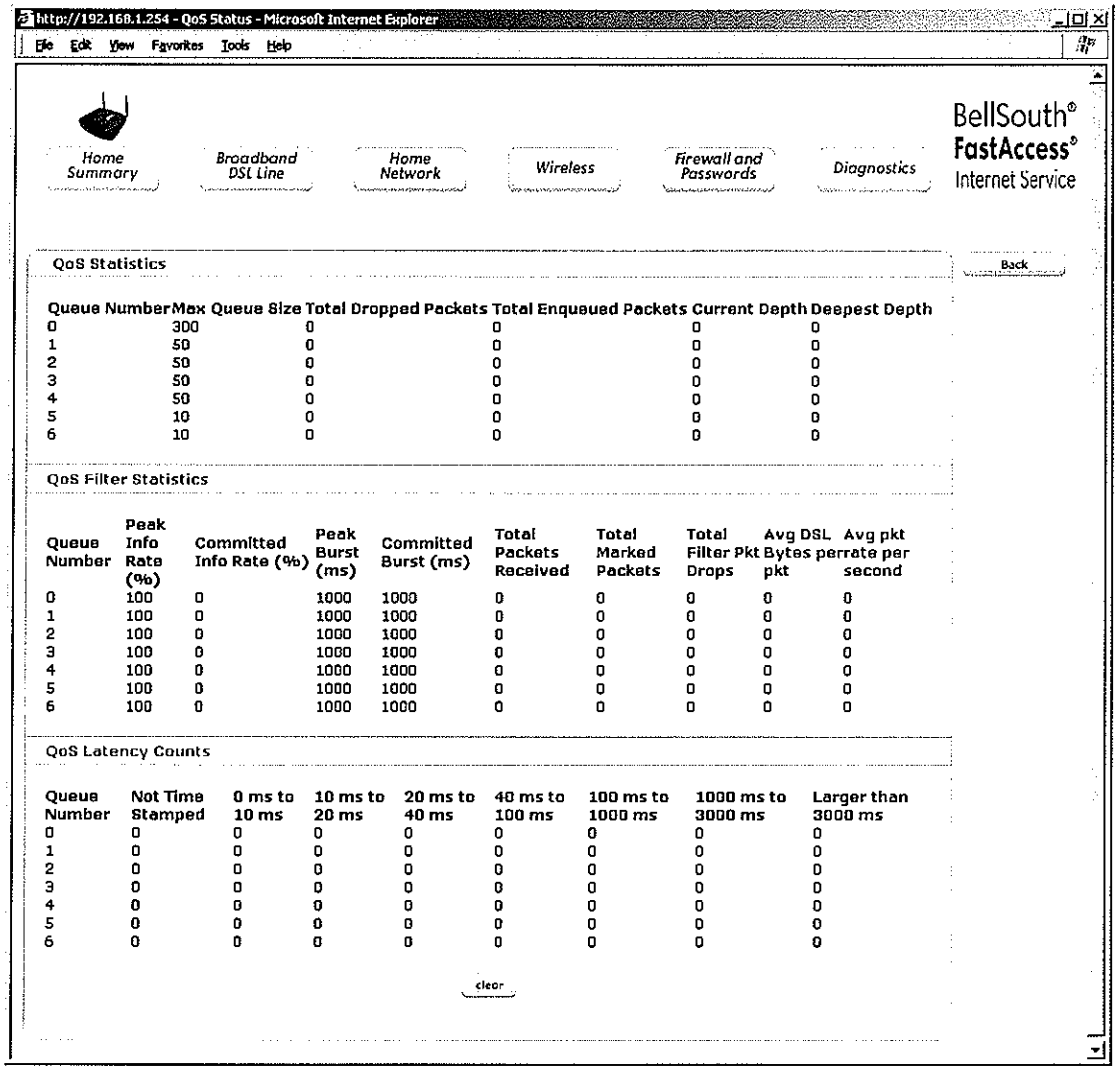


If you clicked on the **Delete All Rules** button, the following pop-up screen will be displayed. Click **OK** to delete all rules in the **QoS Codepoint** page.



11.4.2 Statistics

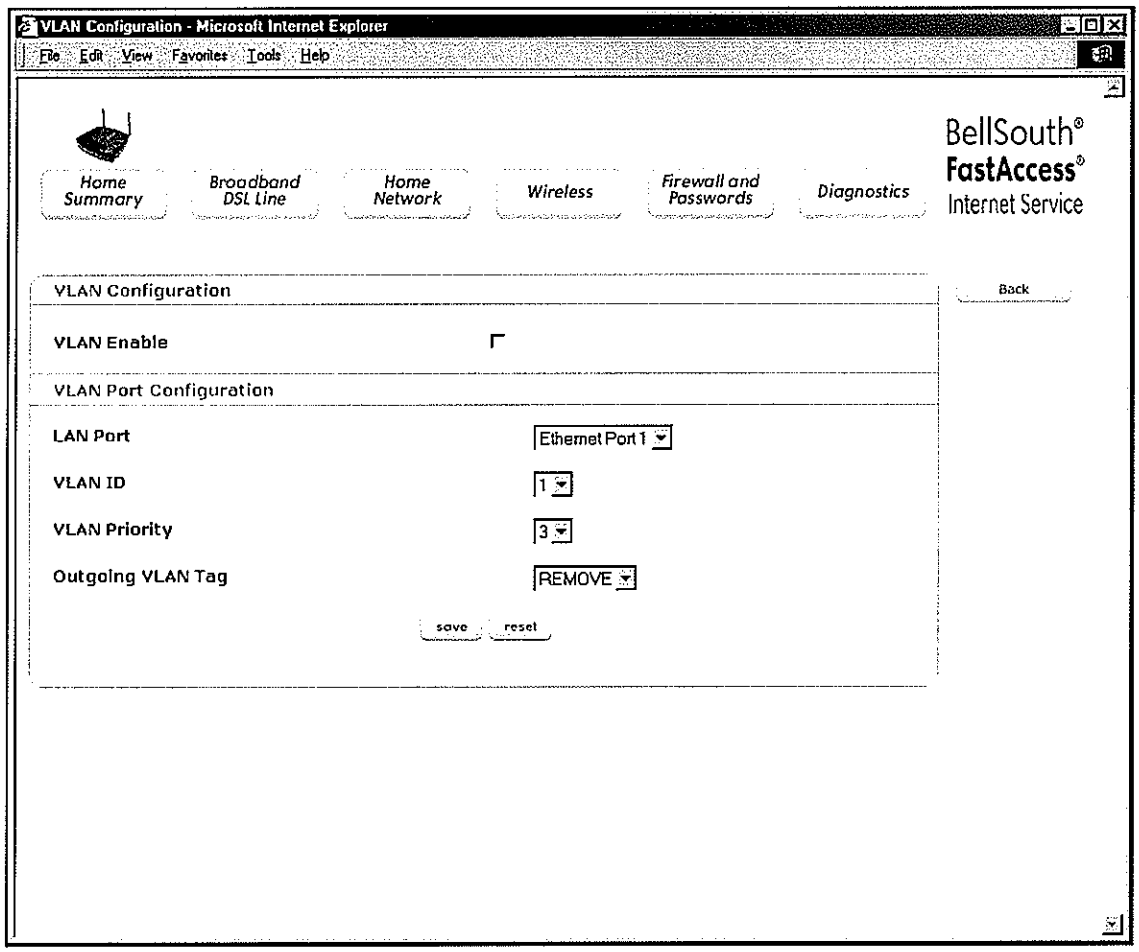
To view the QoS Statistics, click the **Statistics** button in the **QoS Configuration** page. To clear the statistics, click on **clear**. Click the **Back** button to return to the **QoS Configuration** page.



11.5 VLAN

If you click the **VLAN** button in the **Home Network** page, the following page will be displayed. If you change any settings on this page, you must click **save** to allow the settings to take effect. Click **reset** if you want to reset this page to the previously saved VLAN settings.

NOTE: If VersaLink is configured for **ETHERNET PORT 1** mode, the VLAN function will not be available. You must configure VersaLink for **DSLATM** mode to use this function. Refer to section 10.4 for details. The VLAN menu option will not be available if you are in Bridge Ethernet mode.



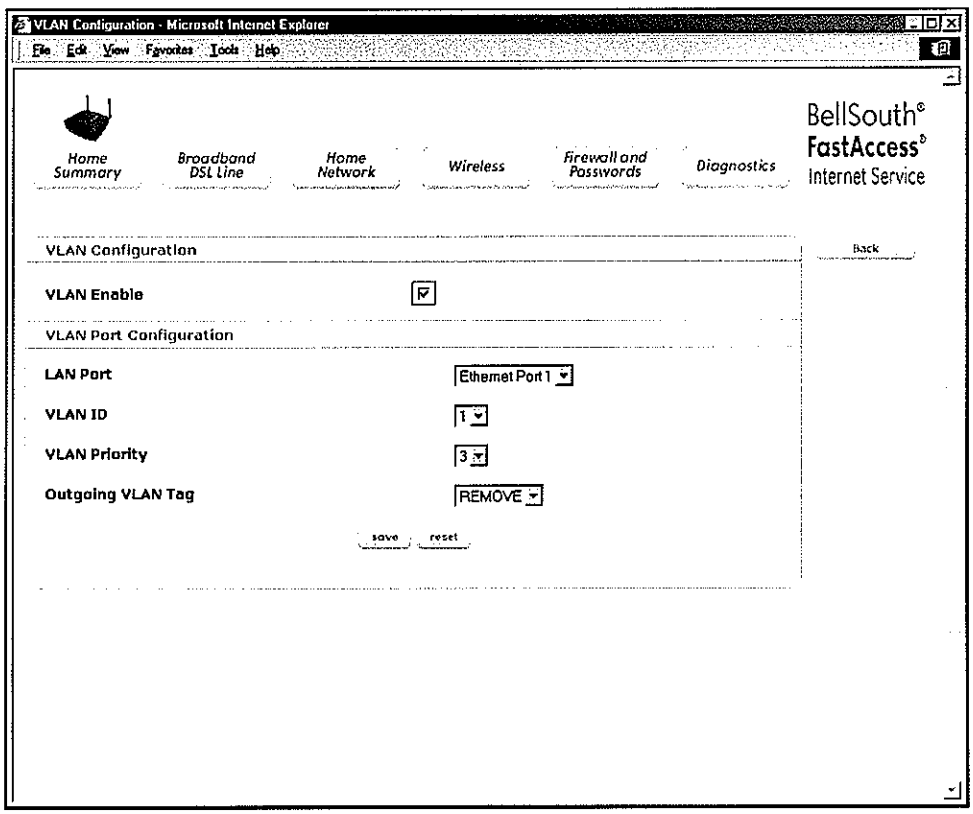
VLAN Configuration	
VLAN Enable	Factory Default = DISABLED If this box is check, VLAN will be Enabled. This will allow VLAN tagging to occur according to the data port's configuration.
VLAN Port Configuration	
LAN Port	This allows you to select the LAN port that you wish to configure. Possible responses are: Ethernet Port 1 Ethernet Port 2 Ethernet Port 3

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

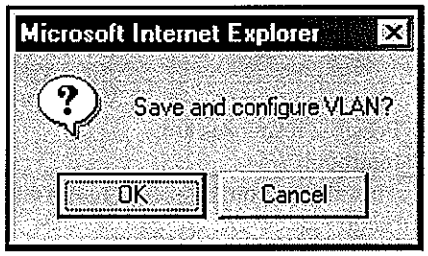
NOTE: For VLAN to function properly, the VLAN ID must be set to a value other than '1' in the following **VLAN Configuration** page and in the **VC 1 Configuration** page when you are using the Bridge Ethernet (VLAN Bridge mode) protocol. Refer to section 10.4.3 for details on configuring the **VC 1 Configuration** page.

To enable VLAN, click on the box adjacent to the **VLAN Enable** field (a check mark will appear in the box). Next, click **save** to save the settings.

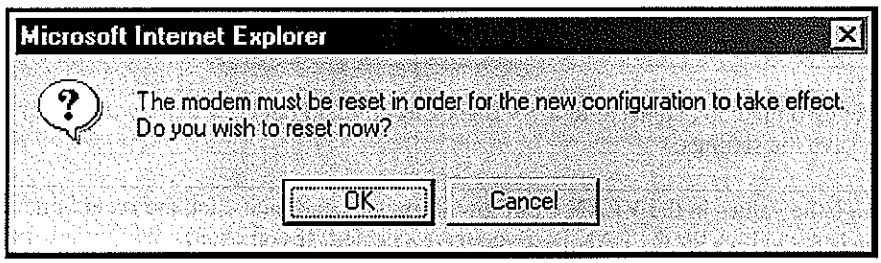
NOTE: If you change the values in the **VLAN Configuration** page and then click the **reset** button, the page will display the previously set values for the LAN Port you have selected. If you change the settings in this page, you must click **save** to save the new settings.



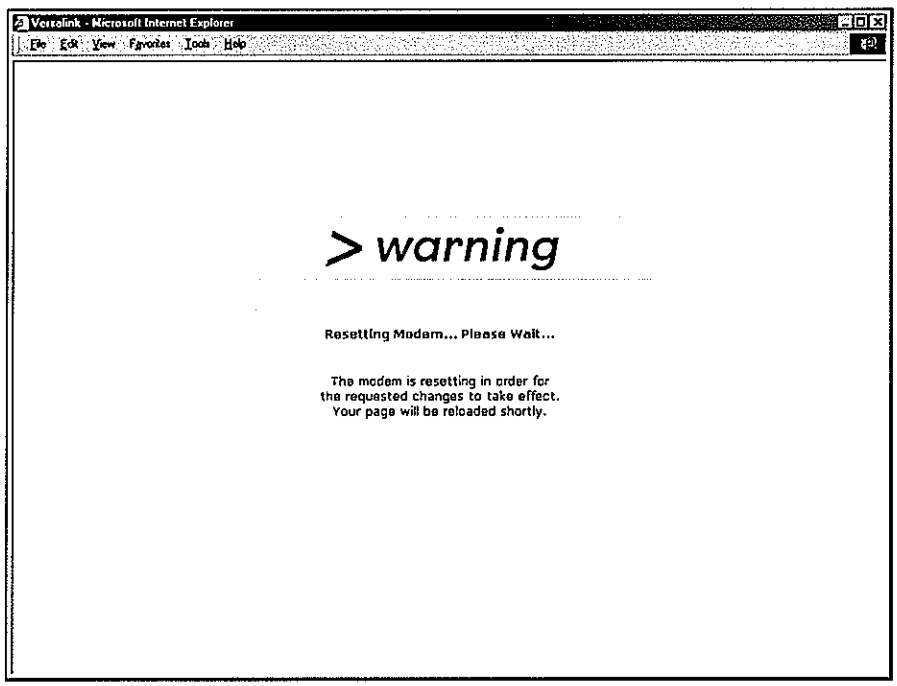
If you click on **save**, the following pop-up screen will appear. Click **OK** in the pop-up screen to allow the new settings to take effect.



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

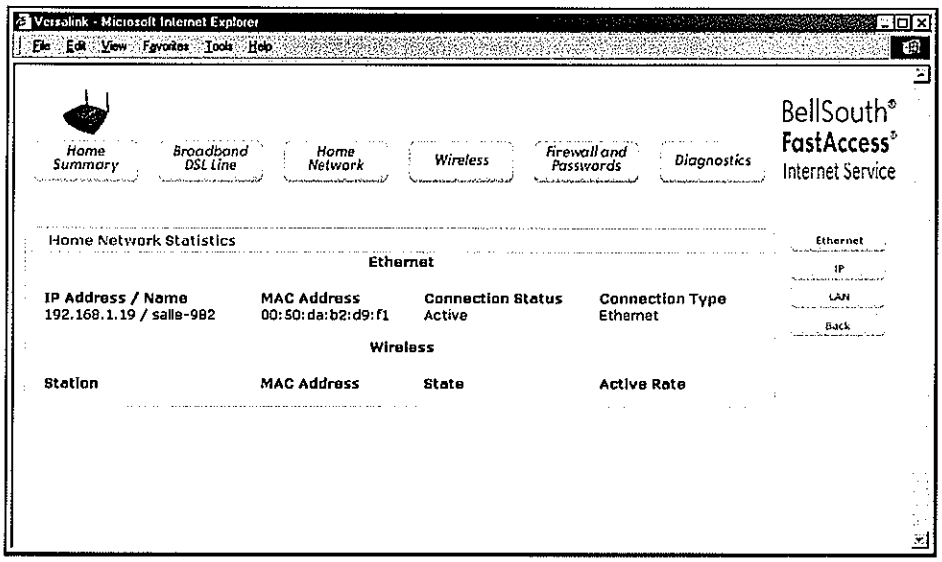


If you clicked **OK** the modem will be reset. After a brief delay, the **Home Summary** page will be displayed.



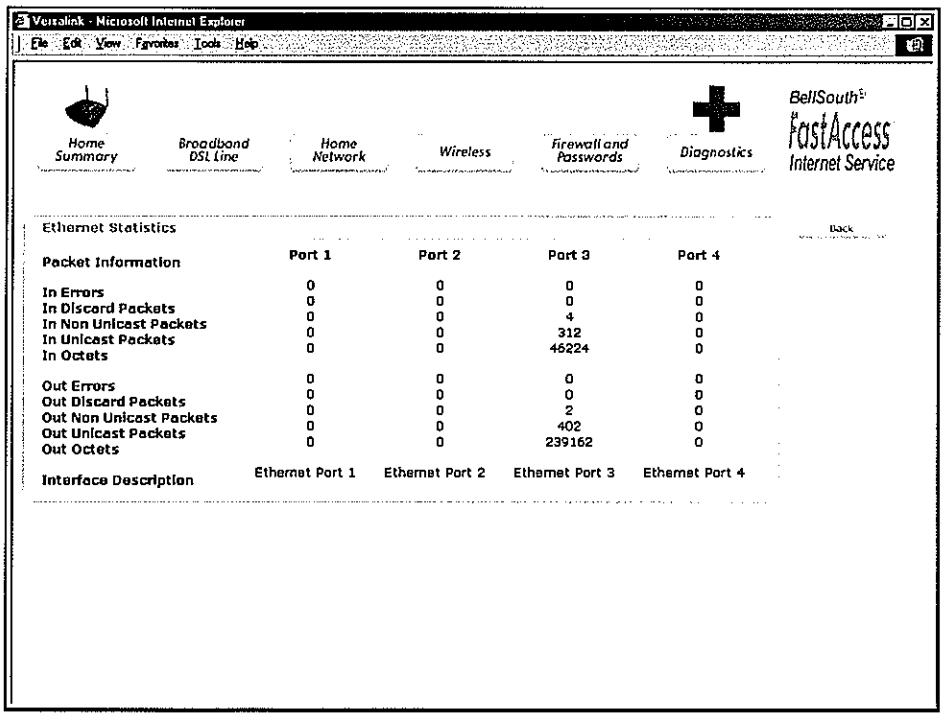
11.6 Statistics

If you click the **Statistics** button in the **Home Network** page, the following page will be displayed. This page enables you to view the Ethernet, IP and LAN statistics of your modem. After you have viewed the statistics, click the **Back** button to return to the **Home Network Statistics** page.



11.6.1 Ethernet Statistics

If you click **Ethernet** in the **Home Network Statistics** page, the following page will be displayed.



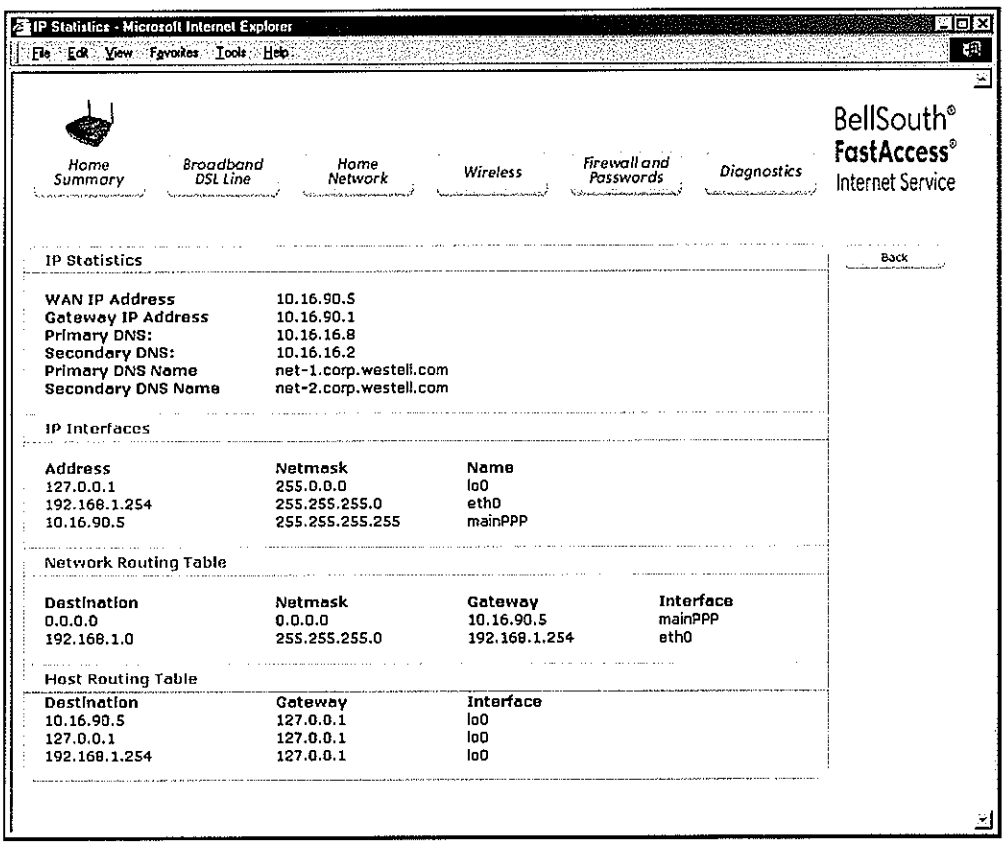
Ethernet Statistics	
In Errors	The number of error packets received on the ATM port.
In Discard Packets	The number of discarded packets received.
In Non Unicast Packets	The number of non-Unicast packets received on the ATM port.
In Unicast Packets	The number of Unicast packets received on the ATM port.
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.
Interface Descriptions	The name of the Ethernet interface.

11.6.2 IP Statistics

If you click **IP** in the **Home Network Statistics** page, the following page will be displayed.

IP Interfaces displays information on all IP interfaces. **Network Routing Table** displays information on all network routes. **Host Routing Table** displays information on all local network routes.

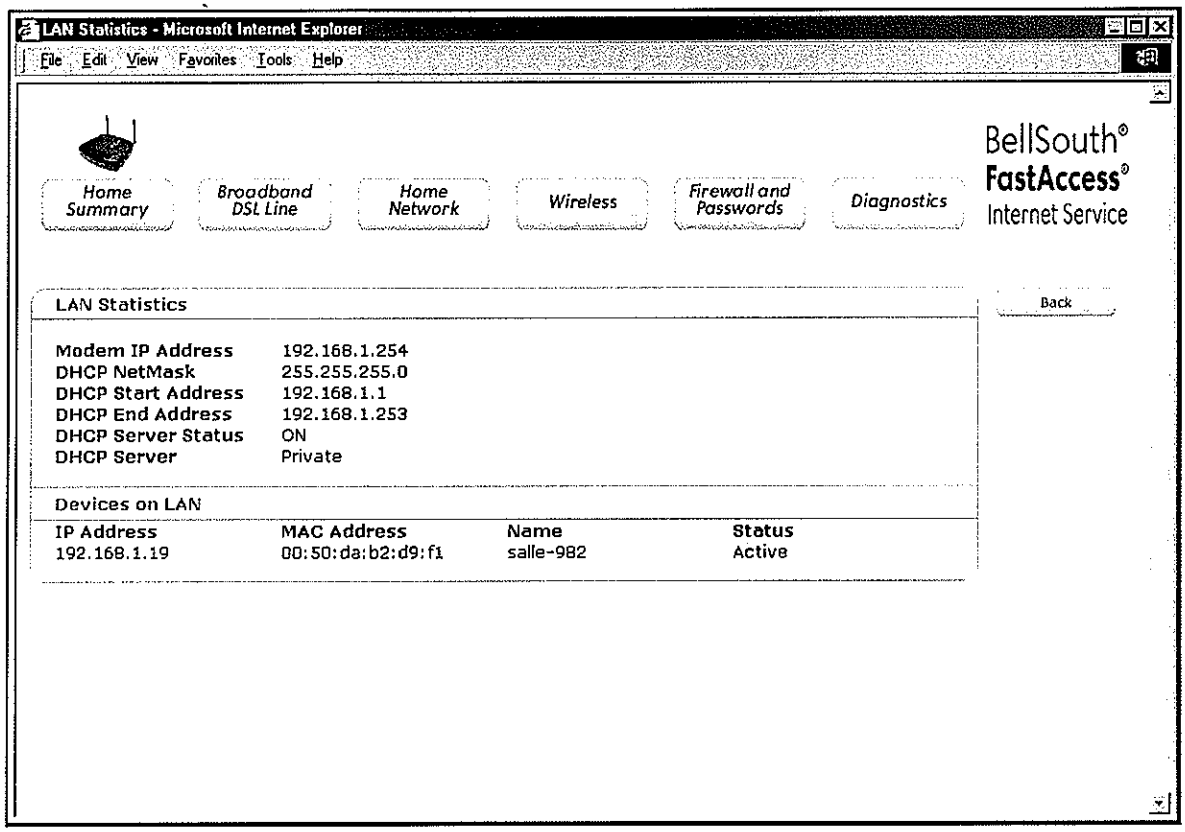
NOTE: The WAN IP Address will display "Down," and the IP Statistics will be unavailable if VersaLink is in **ETHERNET PORT 1** mode.



IP Statistics	
WAN IP Address	Displays the WAN IP address that your modem is on
Gateway IP Address	Displays the modem's gateway IP address
Primary DNS	Displays the primary DNS address
Secondary DNS	Displays the secondary DNS address
Primary DNS Name	Name of primary DNS server
Secondary DNS Name	Name of secondary DNS server
IP Interfaces	
The list of active interfaces on the Modem and their IP and Netmask addresses.	
Address	The IP interface address.
Netmask	The IP interface netmask address.
Name	The IP interface name. lo0 is the loopback interface. eth0, eth1, eth2, or eth3 is the local LAN interface. mainPPP is the WAN protocol interface.
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.
Gateway	Indicates were to send the packet if it matches this route.
Interface	Indicates were to send the packet if it matches this route.
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.
Gateway	Indicates were to send the packet if it matches this route.
Interface	Indicates were to send the packet if it matches this route.

11.6.3 LAN Statistics

If you click **LAN** in the **Home Network Statistics** page, the following page will be displayed.

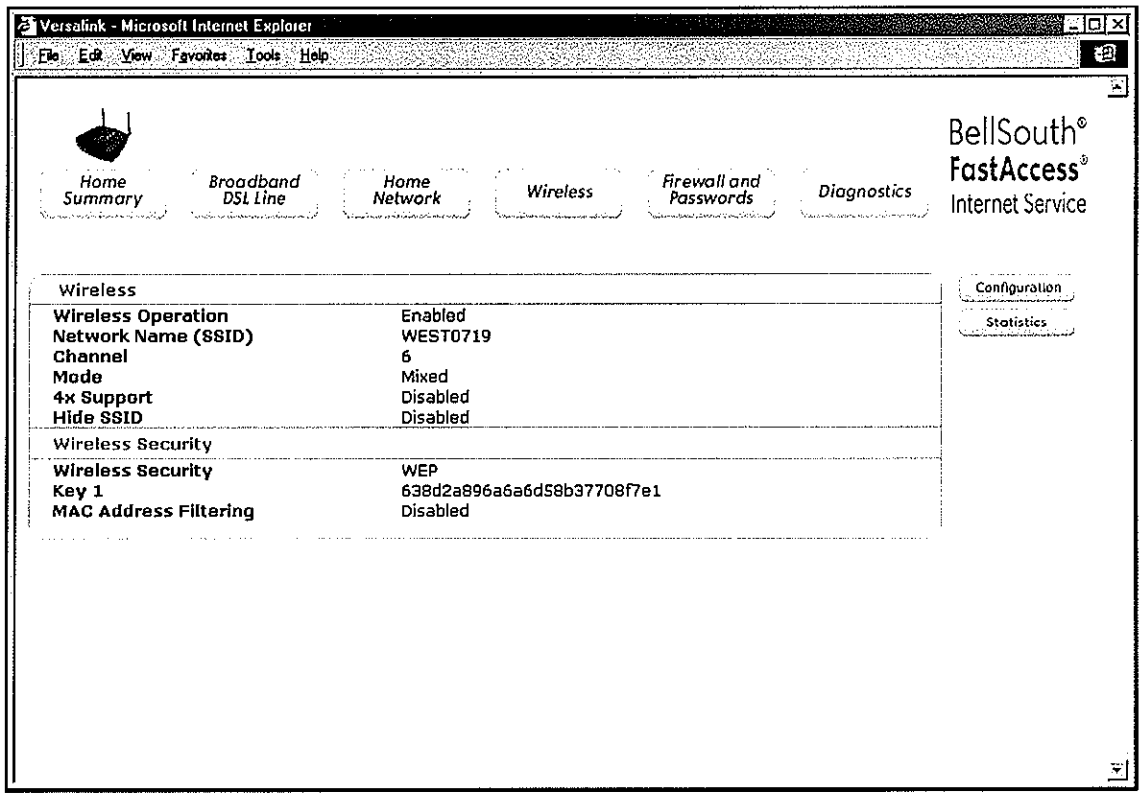


LAN Statistics	
Modem IP Address	Displays the Dual Connect Modem's IP address
DHCP NetMask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address	Displays the starting DHCP Address. Dynamic Host Configuration Protocol automatically assigns IP addresses to devices added to our LAN (Local Area Network).
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 of the DHCP server Possible responses are: **ON**=DHCP server is enabled **OFF**=DHCP server is disabled
DHCP Server	Displays the status of the DHCP server Possible responses are: **Private** = DHCP server is enabled **OFF** = DHCP server is disabled
Devices on LAN	
Displays information about the devices on the LAN	

12. WIRELESS

If you click on **Wireless** at the main menu, the following page will be displayed. This page enables you to set up the wireless network settings of your modem. To configure the wireless settings for VersaLink, click on the **Configuration** button at the right of the page.

IMPORTANT: If you are connecting to the modem via a wireless network adapter, the service set ID (SSID) must be the same for both the Westell modem and your PC's wireless network adapter. The default Network Name (SSID) for the modem is the serial number of the unit located below the bar code on the bottom of the unit and also on the Westell shipping carton. (The SSID displayed in the following page is WEST0719; however, your SSID might differ from the SSID displayed in this page.) To communicate with the modem, the PC's wireless network adapter must be configured with the SSID and pre-defined WEP Key 1 before you begin the modem's Customer Information setup and configuration procedures. Locate and run the utility software provided with your PC's Wireless network adapter and enter the SSID value. Later, for privacy, you should change the **Network Name (SSID)** value in the **Wireless** page to your desired value.

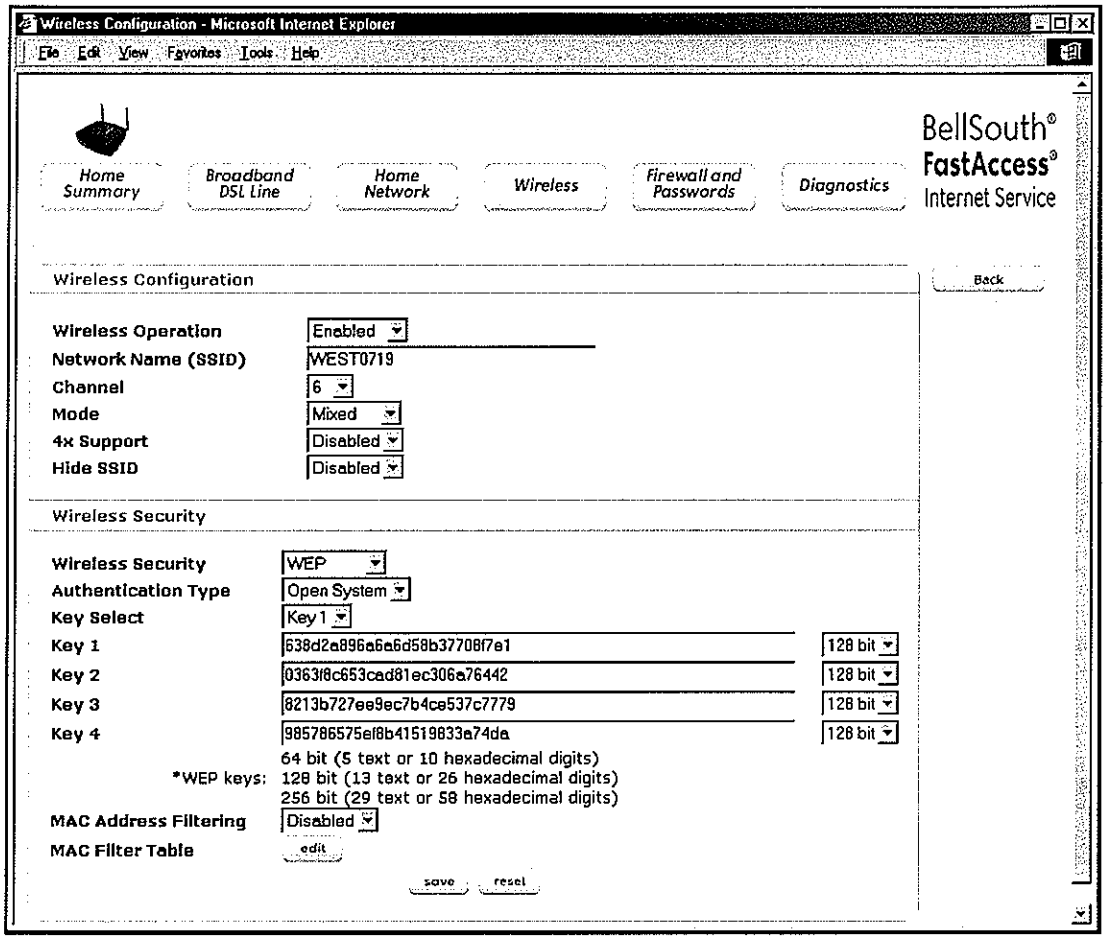


Wireless	
Wireless Operation	Factory Default = Enable Displays the current setting of the modem's wireless operation.
Network Name (SSID)	This string, (32 characters or less) is the name associated with the modem. To connect to the modem, the SSID on a station card must match the SSID on the modem. (Note: If the SSID on a modem is hidden, at the station card you must manually type the SSID of the modem to which you are trying to connect.)
Channel	Factory Default = 6 The modem transmits and receives data on this channel. Station cards do not have to

	be set to the same channel as the AP; the station cards scan all channels and look for the modem with the correct SSID.
Mode	Factory Default = Mixed This setting allows station to communicate with the modem. Possible responses: Mixed: Station using 802.11b or 802.11g cards can communicate with the modem using both 11b and 11g rates. 11b only: Stations using 802.11b or 802.11g cards can communicate with the modem using only 11b rates. 11g only: Only stations using 802.11g cards can communicate with the modem.
4x Support	Factory Default = Disable If enabled, 4X support provides additional algorithms for increased throughput with station cards that support 4x.
Hide SSID	Factory Default = Disable If Enabled, the modem will not broadcast the SSID. Stations must configure the SSID to match the Network Name (SSID) in order to connect to the modem.
Wireless Security	
Wireless Security	Factory Default=WEP Possible Responses: Disabled: No security is used. WPA-PSK: WPA encryption methods are used to encrypt and secure the connection and the data being sent to and from the modem. WEP: WEP encryption used to secure the data being sent to and from the modem; when WEP is enabled, the risk of someone nearby accessing the modem is minimized.
Key n (where n is 1 - 4 for WEP and is blank for WPA-PSK)	Factory Default = Key 1 This information will only be displayed if Security is Enabled. This is the key that is being used for the security mode selected above.
MAC Address Filtering	Factory Default = Disable If Enabled, only the stations in the MAC Filter Table can connect to the modem.

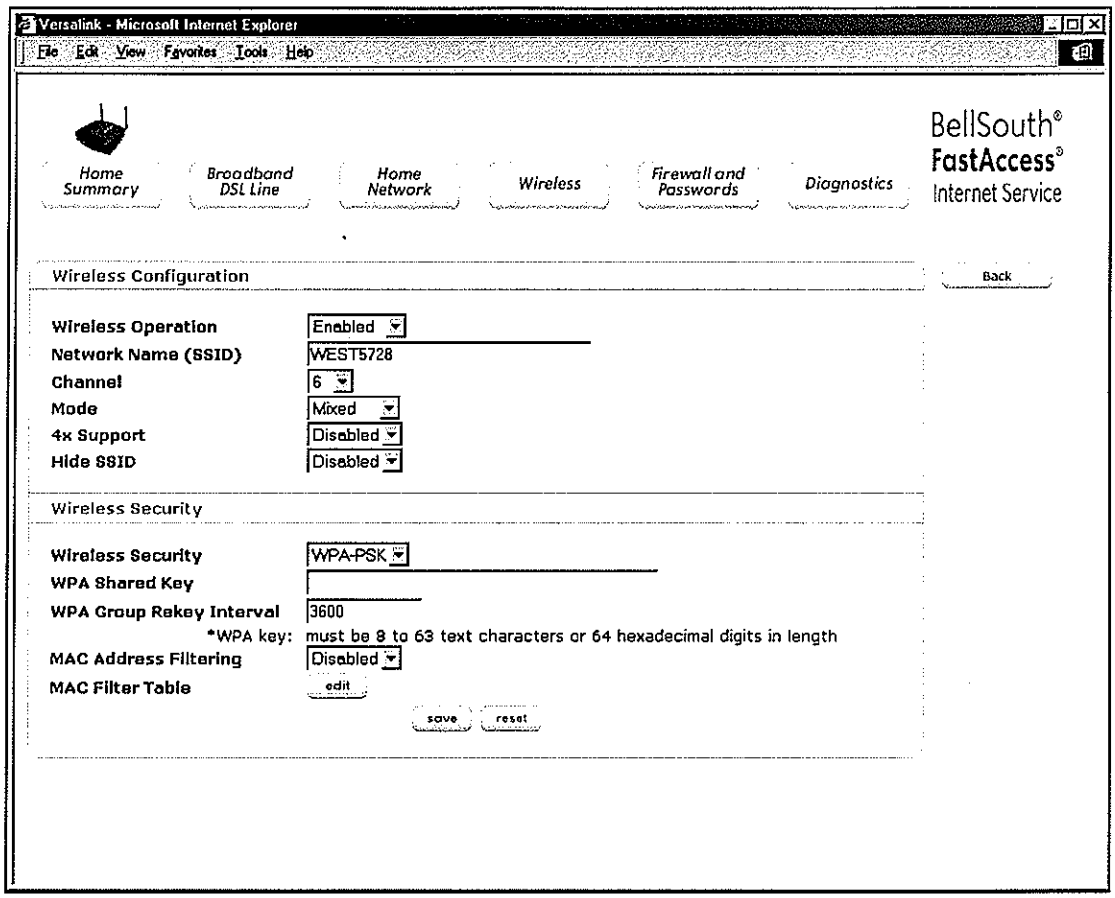
12.1 Configuration

If you click the **Configuration** button at the **Wireless** page, the following page will be displayed. Enter the desired values in the fields provided, and then click **save** to allow the settings to take effect. To edit the **MAC Filter Table**, click the **edit** button. To reset this page to the previously saved settings, click **reset.**



Wireless Configuration	
Wireless Operation	Factory Default = Enabled. Displays the current setting of the modem's wireless operation.
Network Name (SSID)	This string, (32 characters or less) is the name associated with the modem. To connect to the modem, the SSID on a station card must match the SSID on the modem. (Note: If the SSID on a modem is hidden, at the station card you must manually type the SSID of the modem to which you are trying to connect.)
Channel	Factory Default = 6 The modem transmits and receives data on this channel. Station cards no dot have to be set to the same channel as the modem; the station cards scan all channels and look for the modem with the correct SSID.

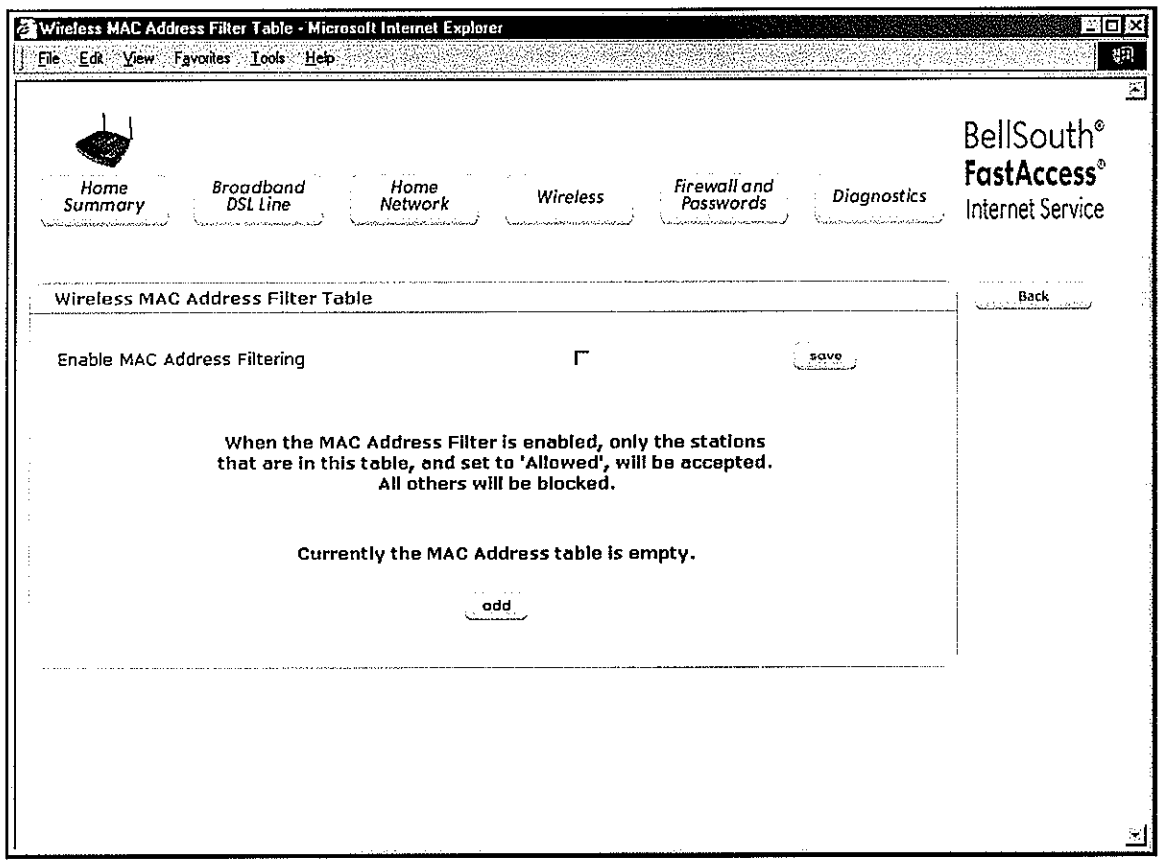
Mode	Factory Default = Mixed This setting allows station to communicate with the modem. Possible responses are: Mixed: Station using 802.11b or 802.11g cards can communicate with the modem using both 11b and 11g rates. 11b only: Stations using 802.11b or 802.11g cards can communicate with the modem using only 11b rates. 11g only: Only stations using 802.11g cards can communicate with the modem.
4x Support	Factory Default = Disable If enabled, 4X support provides additional algorithms for increased throughput with station cards that support 4x.
Hide SSID	Factory Default = Disable If Enabled, the modem will not broadcast the SSID. Stations must configure the SSID to match the Network Name (SSID) in order to connect to the modem.
Wireless Security (if WEP is used)	
Wireless Security	Factory Default=WEP Possible Responses: Disabled: No security is used. WPA-PSK: WPA encryption methods are used to encrypt and secure the connection and the data being sent to and from the modem. WEP: WEP encryption used to secure the data being sent to and from the modem; when WEP is enabled, the risk of someone nearby accessing the modem is minimized.
Authentication Type	Factory Default = Open System Possible responses: Open System: Open System authentication is the default selection. WEP encryption is not used for association. Shared Key: WEP encryption is used for the association process and only stations having the correct key can connect to the modem.
Key Select	Factory Default = 1 Select Key 1 to Key 4 as the WEP key to be used. The key position must be the same in both the modem and the station.
Key n (where n is 1 - 4 for WEP and is blank for WPA-PSK)	The WEP key is treated as either text or hexadecimal (hex) characters. The number of characters is based on the key size selected. The key size 64 bit is either 5 text or 10 hex characters, 128 bit is either 13 text or 26 hex characters, and 256 bit is either 29 text or 58 hex characters. Hexadecimal characters are 0-9 and A-F (or a-f). This key must be the same in both the modem and the station. Some station cards use a "Pass Phrase." This is not the same as "text" and should not be used.
MAC Address Filtering	Factory Default = Disabled If Enabled, only the stations in the MAC Filter table can connect to the modem.
MAC Filter Table	This table enables you to add, edit or delete MAC addresses of stations that are allowed to communicate with the modem.



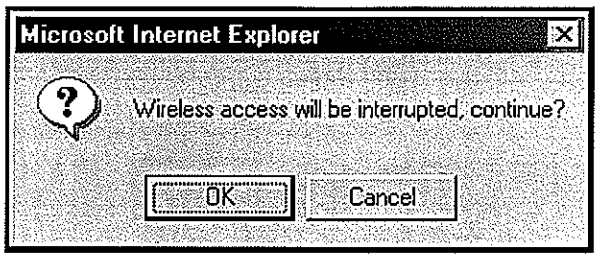
Wireless Configuration	
Wireless Operation	Factory Default = Enabled. Displays the current setting of the modem's wireless operation.
Network Name (SSID)	This string, (32 characters or less) is the name associated with the modem. To connect to the modem, the SSID on a station card must match the SSID on the modem. (Note: If the SSID on a modem is hidden, at the station card you must manually type the SSID of the modem to which you are trying to connect.)
Channel	Factory Default = 6 The modem transmits and receives data on this channel. Station cards no dot have to be set to the same channel as the modem; the station cards scan all channels and look for the modem with the correct SSID.
Mode	Factory Default = Mixed This setting allows station to communicate with the modem. Possible responses are: Mixed: Station using 802.11b or 802.11g cards can communicate with the modem using both 11b and 11g rates. 11b only: Stations using 802.11b or 802.11g cards can communicate with the modem using only 11b rates. 11g only: Only stations using 802.11g cards can communicate with the modem.
4x Support	Factory Default = Disable If enabled, 4X support provides additional algorithms for increased throughput with station cards that support 4x.
Hide SSID	Factory Default = Disable If Enabled, the modem will not broadcast the SSID. Stations must configure the SSID to

	match the Network Name (SSID) in order to connect to the modem.
Wireless Security (if WPA-PSK is used)	
Wireless Security	Factory Default=WEP Possible Responses: Disabled: No security is used. WPA-PSK: WPA encryption methods are used to encrypt and secure the connection and the data being sent to and from the modem. WEP: WEP encryption used to secure the data being sent to and from the modem; when WEP is enabled, the risk of someone nearby accessing the modem is minimized.
WPA Shared Key	This string (8 to 63 characters of 64 hex characters) is the key used for encrypting packets being sent to and from the modem. This key must be the same in both the modem and the station.
WPA Group Rekey Interval	Factory Default = 3600 The number of seconds between rekeying the WPA group key. A value of 0 means that rekeying is disabled. The Shared Key is the initial key and new keys are created and used, based on that key, at each Rekey Interval.

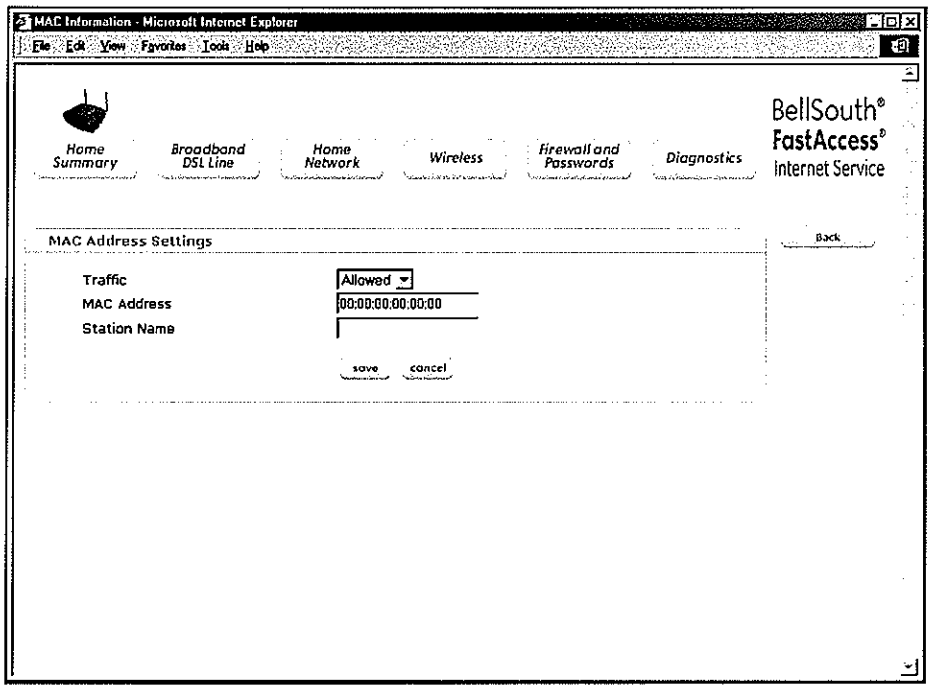
If you clicked **edit,** the following page will be displayed. Click the **add** button to add stations to the MAC Address table, and then click **save** to save the settings. To add more entries, click the **add** button. When you have finished adding entries, click the box adjacent **Enable MAC Address Filtering** (a check mark will appear in the box). Next, click **save** to save the settings.



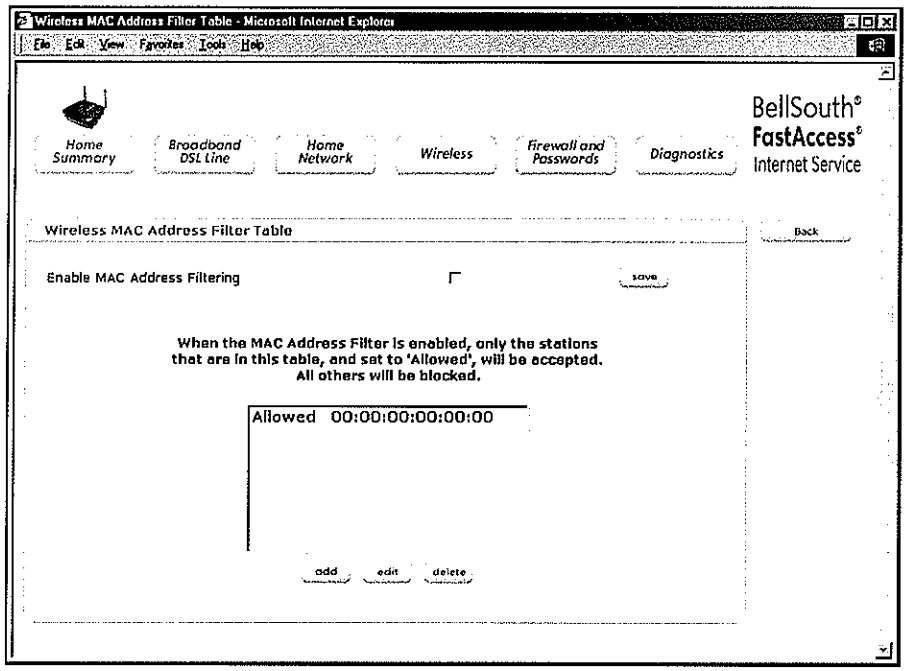
If you clicked **save** in the **Wireless Configuration** page, the following pop-up will be displayed. Click **OK** to continue.



If you clicked the **add** button in the **Wireless MAC Address Filter Table**, the following page will be displayed. After you have entered the desired MAC Address settings, click **save** to save your settings.

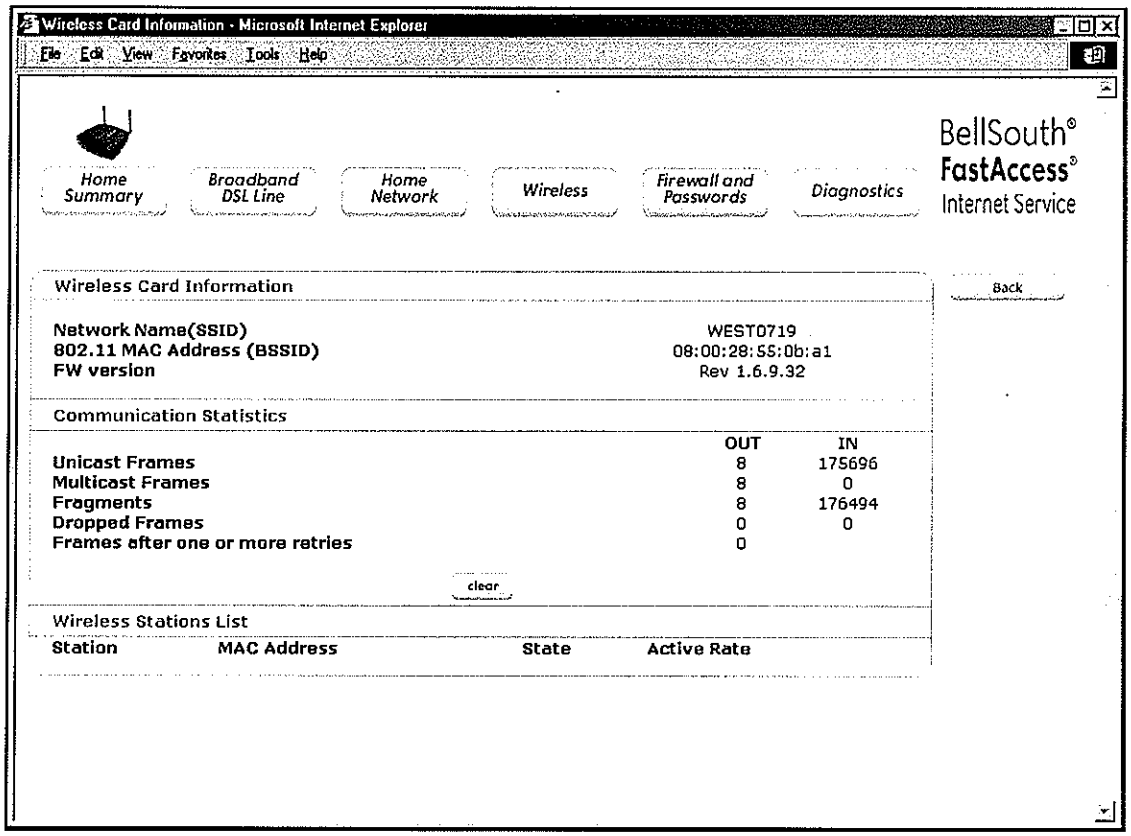


If you clicked **save**, the following page will be displayed. This page enables you to add, edit or delete stations at the MAC Address Filter table. After you have made the desired changes to this page, click the **save** button to allow the changes to take effect.



12.2 Statistics

If you click the **Statistics** button at the **Wireless** page, the following page will be displayed. This page provides information about your modem's wireless connection. To clear the statistics in this page, click on **clear.**

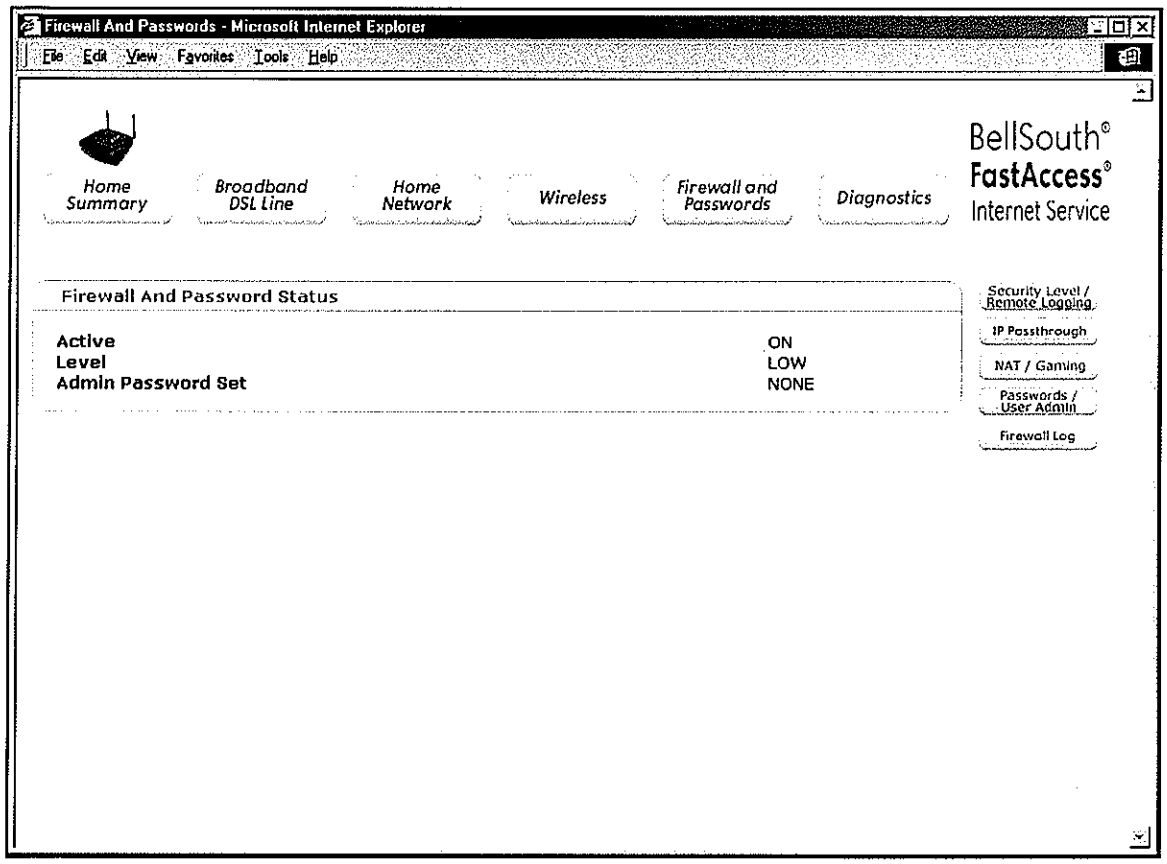


Wireless Card Information	
Network Name (SSID)	This string, (32 characters or less) is the name associated with the Access Point (AP). To connect to the AP, the Service Set ID (SSID) on a Station card must match the SSID on the AP.
802.11 MAC Address (BSSID)	This is the Media Access Controller address of the AP. It is used as the Basic Service Set Identifier (BSSID).
FW Version	This is the Network Interface Card Identifier. It uniquely identifies the hardware platform of the AP. This is used with other information to determine if the inserted card can be used as an AP, and if so, the version of AP firmware to be used. Not all makes of wireless station cards can be used as an AP.
Communication Statistics	
NOTE: Data preceded by **OUT** pertain to transmissions from 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-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-Frames after one or more retries	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
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-Dropped Frames	The number of frames that were not received by VersaLink due to the short or long retry limit being reached because no acknowledgement or CTS was received.
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 VersaLink.
Active Rate	The current transmit and receive rate.

13. FIREWALL AND PASSWORDS

If you click on **Firewall and Passwords** at the main menu, the following page will be displayed. This page enables you to set up your firewall and password settings. To configure the settings, click on the desired submenu option at the right of the page. After you have completed a submenu configuration, click the **Back** button to return to the **Firewall and Passwords Status** page.



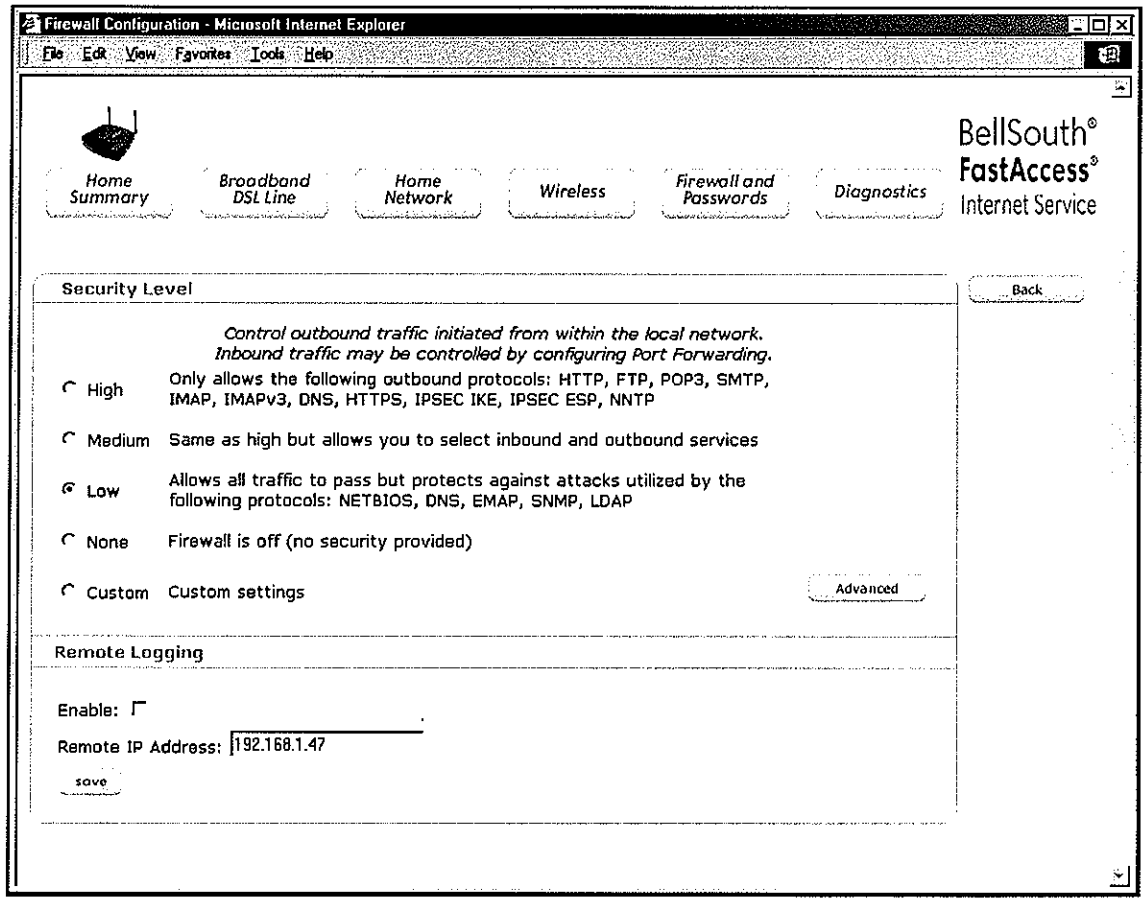
Firewall and Password Status	
Active	Factory Default = ON If OFF is displayed, firewall security has not been activated.
Level	Factory Default = Low The security level of your firewall. Possible responses are: High = High security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. All other traffic is prohibited. Medium = Like High security, Medium security only allows basic Internet functionality by default. However, Medium security allows customization through NAT configuration so that you can enable the traffic that you want to pass. Low = The Low security setting will allow all traffic except for known attacks. With Low security, VersaLink is visible to other computers on the Internet.

	None = Firewall security is not activated. 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.
Admin Password Set	Factory Default = NONE The password used in the administrator's login.

13.1 Security Level/Remote Logging

If you click **Security Level/Remote Logging** in the **Firewall and Password Status** page, the following page will be displayed. If you change any settings in this page, you must click **save** to allow the settings to take effect.

NOTE: Westell recommends that you do not change the settings in this page. If you need to reset the modem to factory default settings, push the **reset** button on the rear of the modem. The **Security Level/Remote Logging** menu option will not be available if you are in **Bridge Ethernet** mode.



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

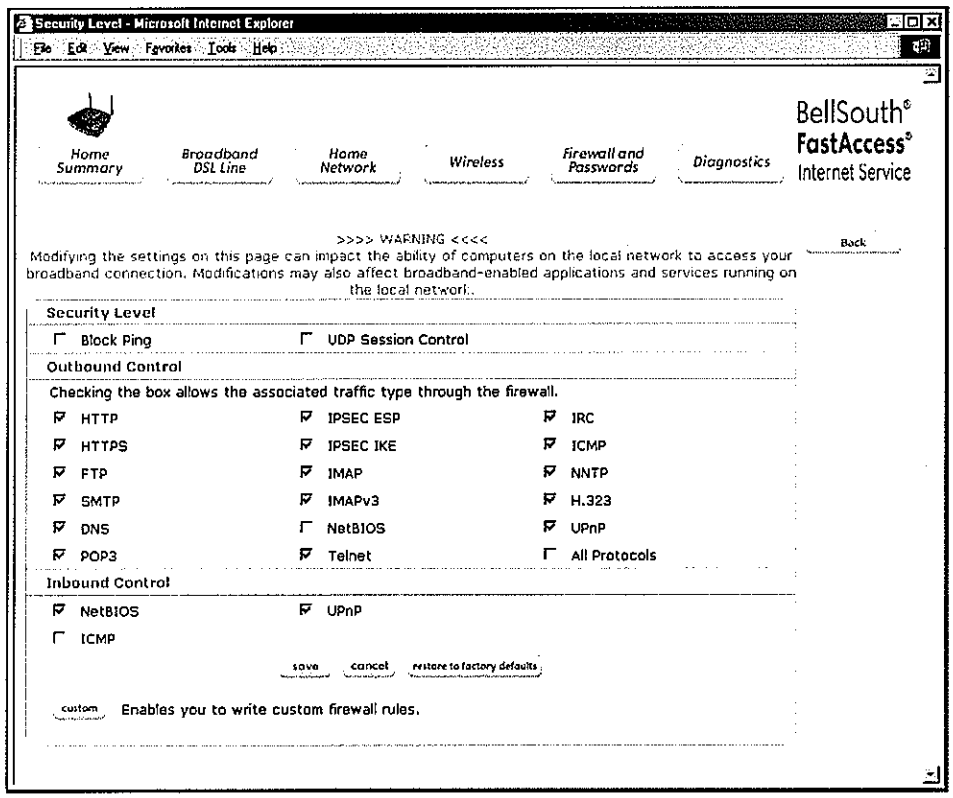
	If enabled, VersaLink will send firewall logs to a syslog server.
Remote IP Address	The IP address of the syslog server machine to which the diagnostics logs to be sent.

If you have selected "High" or "None" at the **Security Level** page, the following pop-up screen will be displayed if you click the **Advanced** button. Click **OK** in the pop-up screen to return to the **Security Level** page.

Note: If you selected "High" or "None" at the **Security Level** page, you will not have access to the advanced firewall settings or the **Firewall Rules** page. The advanced firewall settings can be accessed only when the firewall is set to Medium, Low, or Custom.

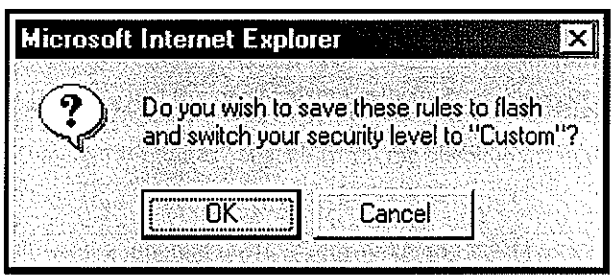
If you click **Advanced** in the **Security Level** page (and the security level is set to Medium, Low, or Custom), the following page will be displayed. Entered the desired setting in this page, and then click **save** to allow the settings to take effect. To restore this page to the factory default settings, click **restore to defaults.** Click **cancel** to cancel any changes that you have made to this page.

WARNING: Modifying the setting on this page can impact the ability of computers on the local network to access your broadband connection. Modifications may also affect broadband-enabled applications and services running on the local network.

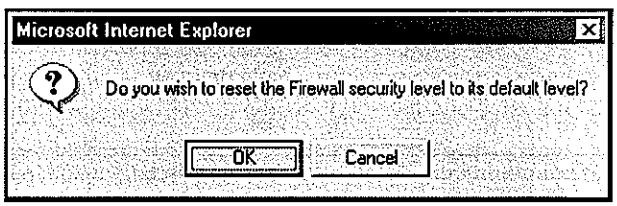


Security Level	
Block Ping	Factory Default = Disabled When Enabled (box is checked), the Block Ping function shall block any incoming ping to the LAN IP address.
UDP Session Control	Factory Default = Disbled When Enabled, the UDP Session Control function shall strictly match the UDP ports and addresses on inbound UDP traffic. When this function is Disabled (box is not checked), any Internet device could talk to the port until the transmission times out.
Outbound Control	
The Outbound Control section shows the outbound traffic types that can be controlled from this page. When a certain outbound protocol is checked, the firewall will allow the corresponding traffic type to pass from the LAN to the firewall on the modem to the Internet. Similarly, when a certain outbound protocol is unchecked, the firewall will stop the corresponding traffic type from passing from the LAN to the firewall on the modem to the Internet. All Protocols = This checkbox provides an easy mechanism for the user to check or uncheck all the traffic types shown in the Outbound Control section. (That is, when the user checks the "All Protocols" checkbox, all the checkboxes in the outbound control section of the page will be checked.)	
Inbound Control	
The Inbound Control section shows the inbound traffic (from WAN to LAN) types that can be controlled from this page. When a certain inbound protocol is checked, the firewall will allow the corresponding traffic type to pass from the Internet to the firewall on the modem to the LAN. Similarly, when a certain inbound protocol is unchecked, the firewall will stop the corresponding traffic type from passing from the Internet to the firewall on the modem to the LAN. Save Button: Clicking this button saves the settings on this page to the modem. When these settings are saved the Firewall's security level will be switched to "Custom". Cancel Button: Clicking this button will cancel all changes made on this page and reloads the page. Restore to Defaults: Clicking this button will set the firewall level to the default level, "LOW."	
Custom	
The "Custom" button will open a page that displays the current inbound/outbound rules in their text form. From this page the user can modify (add/delete/edit) the rules according to their needs. Back Button: Clicking this button will take user back to the Firewall main page.	

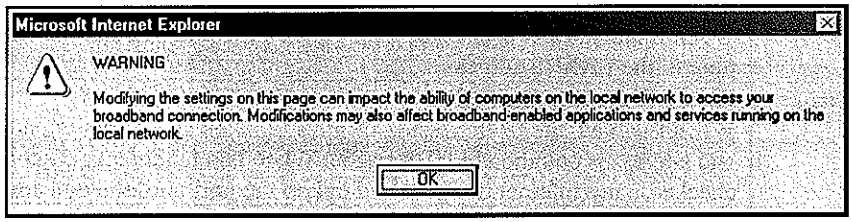
If you clicked **save,** the following pop-up screen will be displayed. Click **OK** in the pop-up screen.



If you clicked **restore to defaults,** the following pop-up screen will be displayed. Click **OK** to reset this page to the factory default settings.

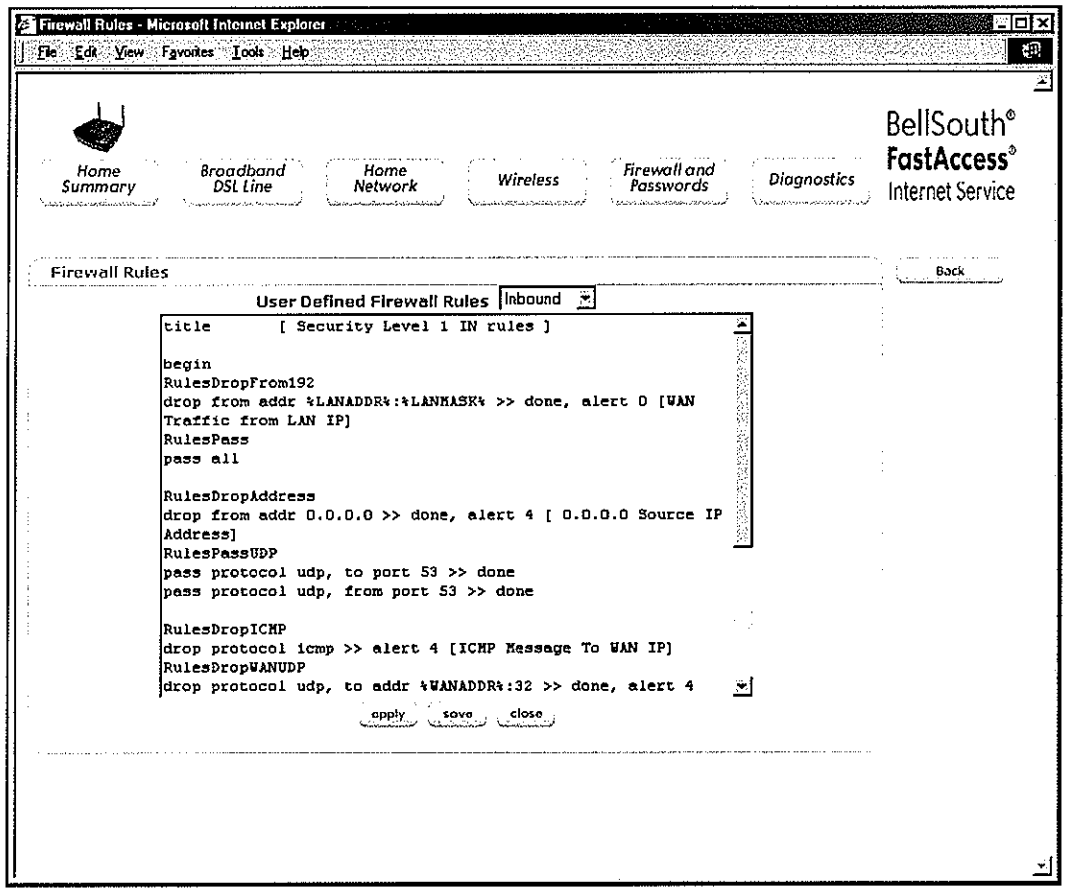


If you clicked **custom**, the following pop-up screen will be displayed. To proceed, click **OK** in the pop-up screen.

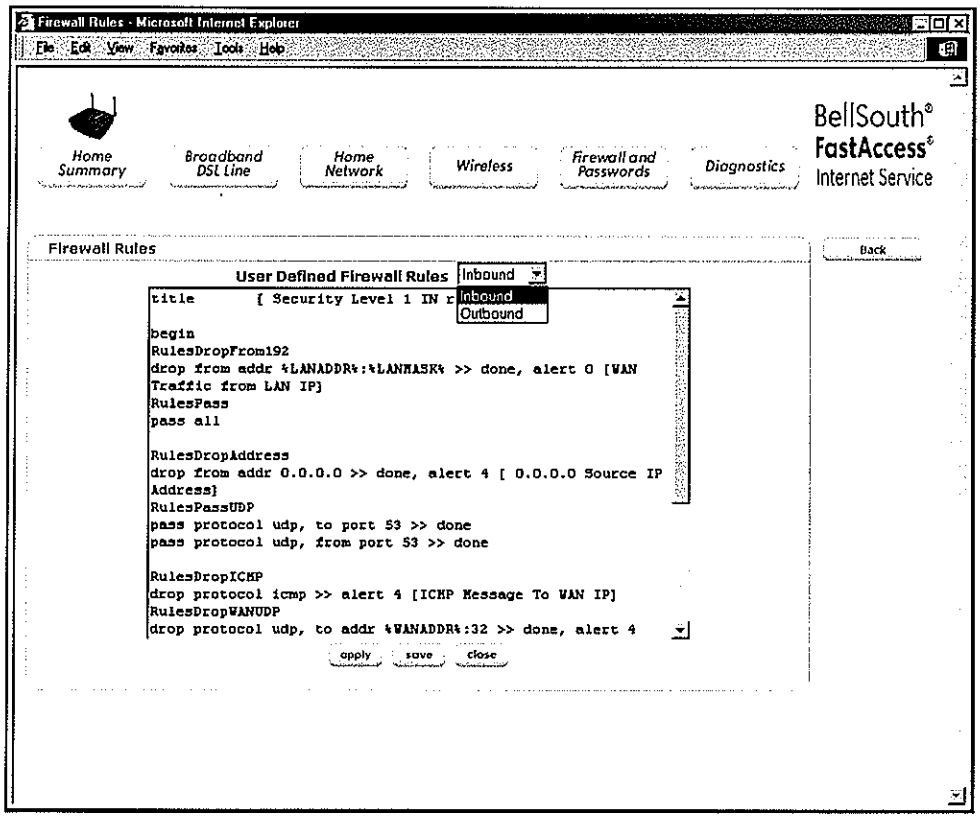


If you clicked **OK** in the preceding pop-up screen, the following **Firewall Rules** page will be displayed. The **User Defined Firewall Rules** drop-down arrow enables you to change the security parameters on your Inbound and Outbound Firewall rules.

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

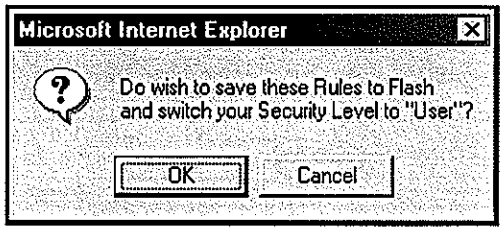


If you select **Inbound**, this will restrict inbound traffic from the WAN to the LAN. Selecting **Outbound** will restrict outbound traffic from the LAN to the WAN. Select a setting and then click **Apply** to apply the new settings.



If you clicked **apply** in the **User Defined Firewall Rules** page, the following screen will be displayed. Click **OK** to continue.

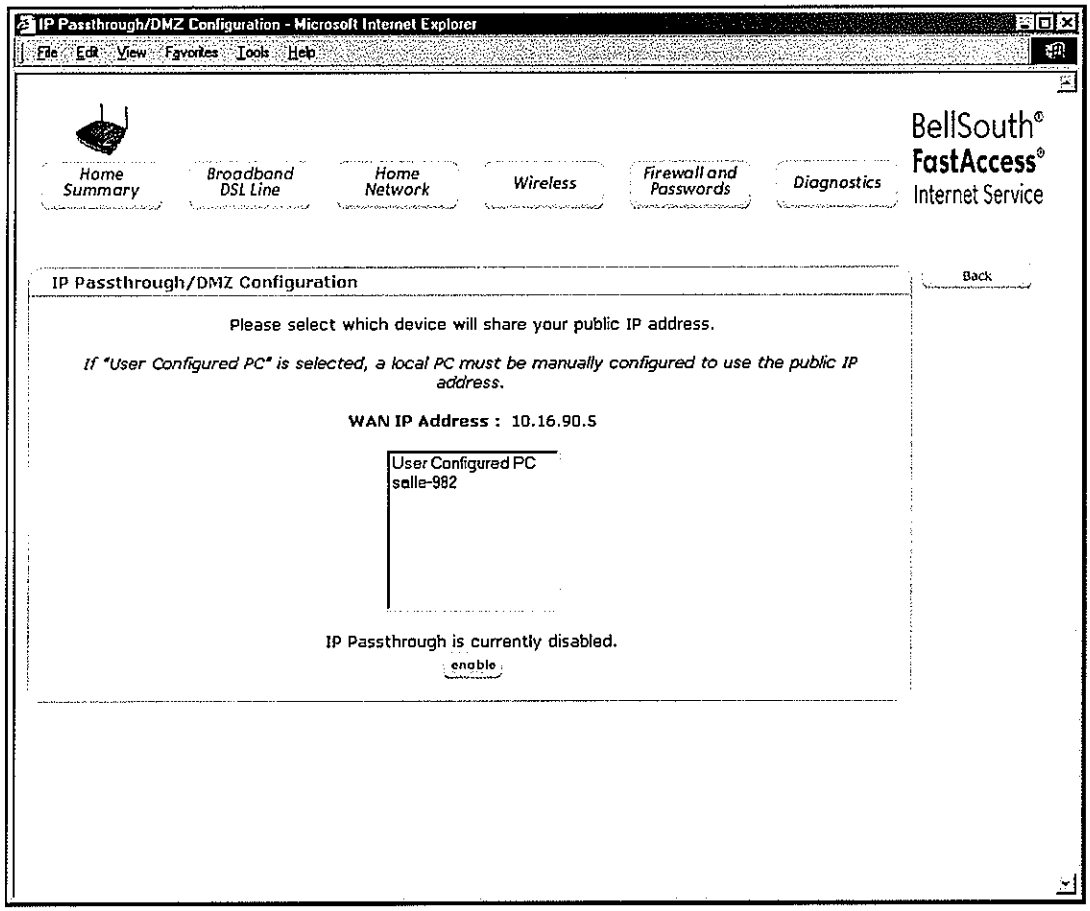
If you clicked **save** in the preceding **Firewall Rules** page, the following screen will be displayed. Click **OK** to save these firewall rules to flash and switch your security level to "User"?



13.2 IP Passthrough/DMZ – Single IP Address Passthrough

If you click the **IP Passthrough** button in the **Firewall and Password Status** page, the following **IP Passthrough/DMZ Configuration** page will be displayed. This page enables you to select the device on your LAN that will share your single static IP address. Refer 11.2 to section for instructions on configuring **IP Passthrough/DMZ.**

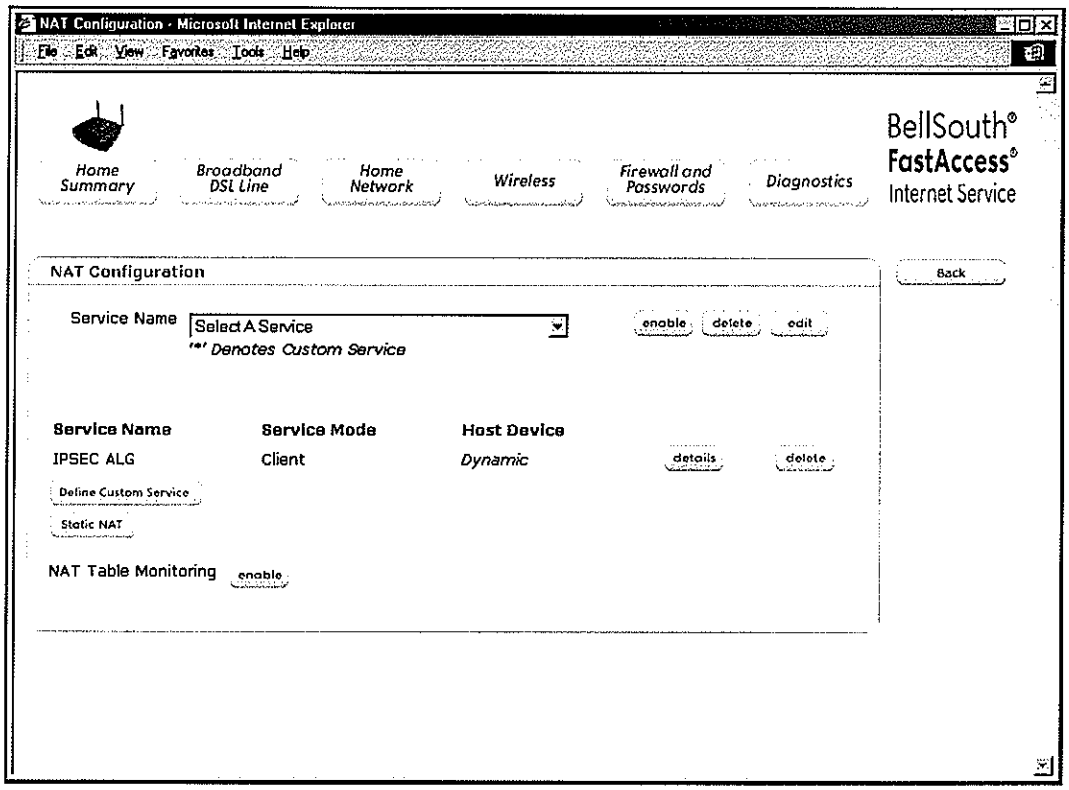
NOTE: The IP Passthrough/DMZ menu option will not be available if you are in Bridge Ethernet mode.



13.3 NAT/GAMING

If you click the **NAT/Gaming** button in the **Firewall and Passwords Status** page, the following **NAT Configuration** page will be displayed. The **NAT Configuration** page enables you to set up NAT services for your modem. Refer to section 11.3 for instructions on configuring the modem's NAT/Gaming functions.

NOTE: The NAT/Gaming menu option will not be available if you are in Bridge Ethernet mode.

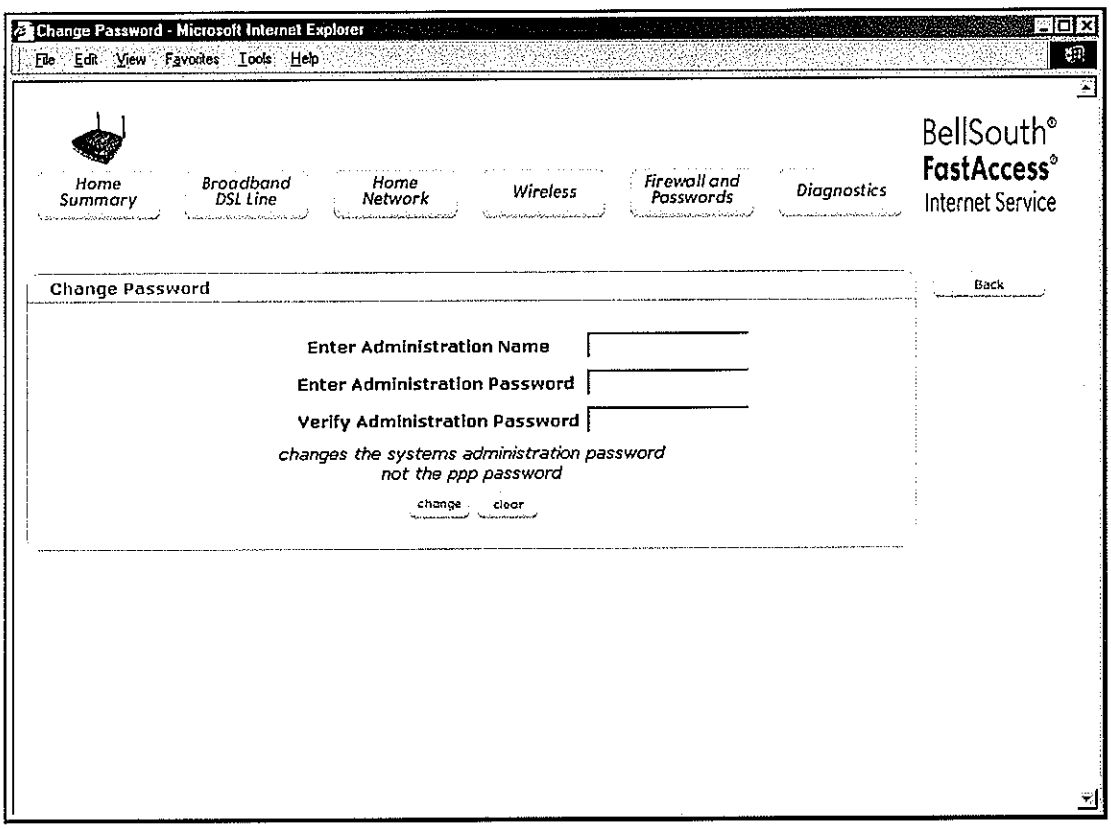


NAT Configuration	
Service Name	A drop-down menu of NAT (Network Address Translation) services that you can select from when you are ready to configure your modem for NAT service.
NAT Table Monitoring	Factory Default = Disabled If Enabled, this feature will monitor traffic on the ports.

13.4 Password/User Admin

If you click the **Password/User Admin** button in the **Firewall and Passwords Status** page, the following Password page will be displayed. After you enter your data into the appropriate settings, click on **change** to change the administration name and password. Click **clear** to clear the values in this page.

NOTE: This page will enable you change only the administration Name and Password, not the PPP password. If VersaLink is password protected and you are not an authorized user, you will not be able to change the values. (VersaLink cannot be configured unless the user is logged in.) Contact your network administrator for further instructions.

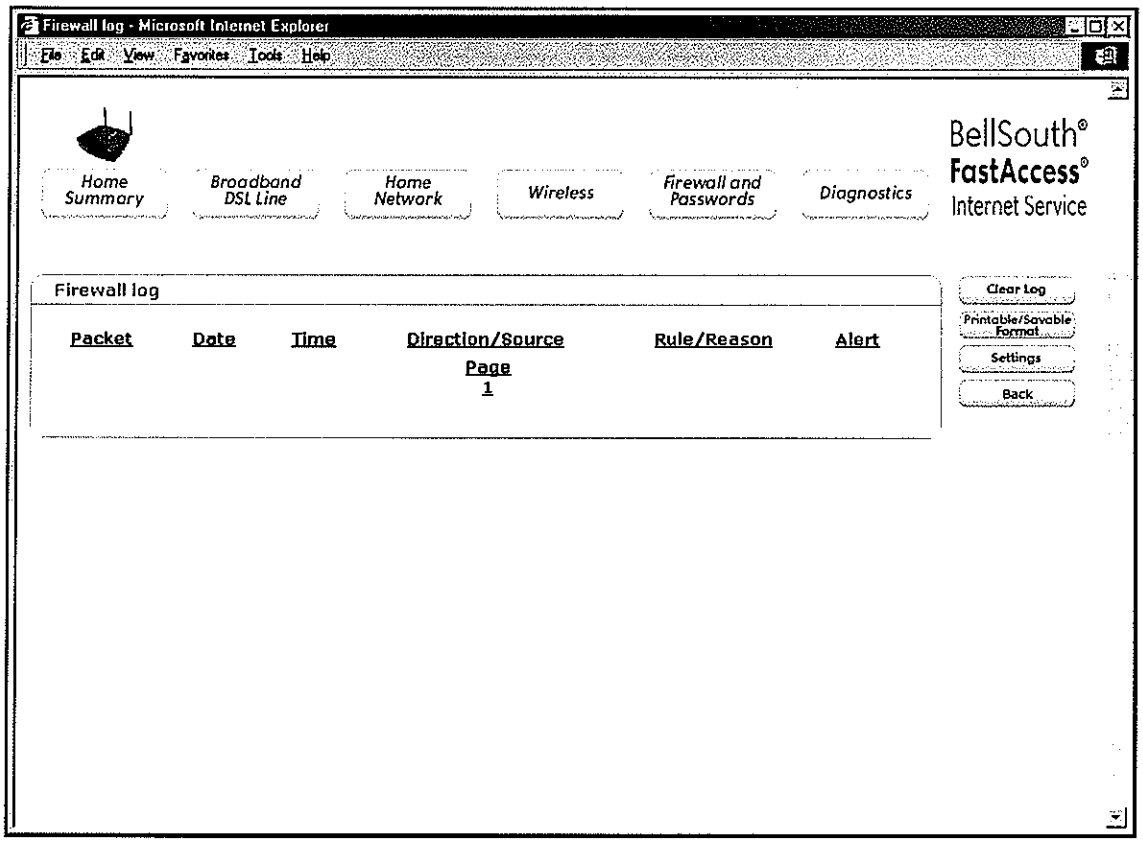


Change Password	
Enter Administrative Name NOTE: This changes the Systems Administrator password not the PPP password.	Type the name of your network administrative.
Enter Administrative Password	Type your network administrator's password.
Verify Administrative Password	Re-type your network administrator's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

13.5 Firewall Log

If you click on **Firewall Log** in the **Firewall and Passwords Status** page, the following page will be displayed. This page alerts you of noteworthy information sent to your modem from the Internet.

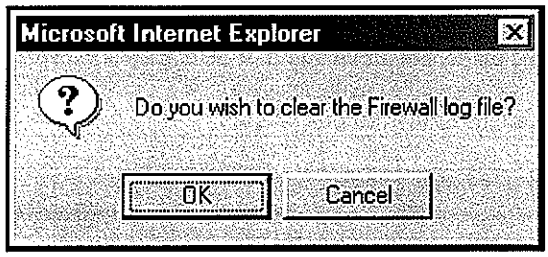
NOTE: One thousand entries can be made, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for new entries as they occur. The Firewall Log menu option will not be available if you are in Bridge Ethernet mode.



Firewall Log	
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.

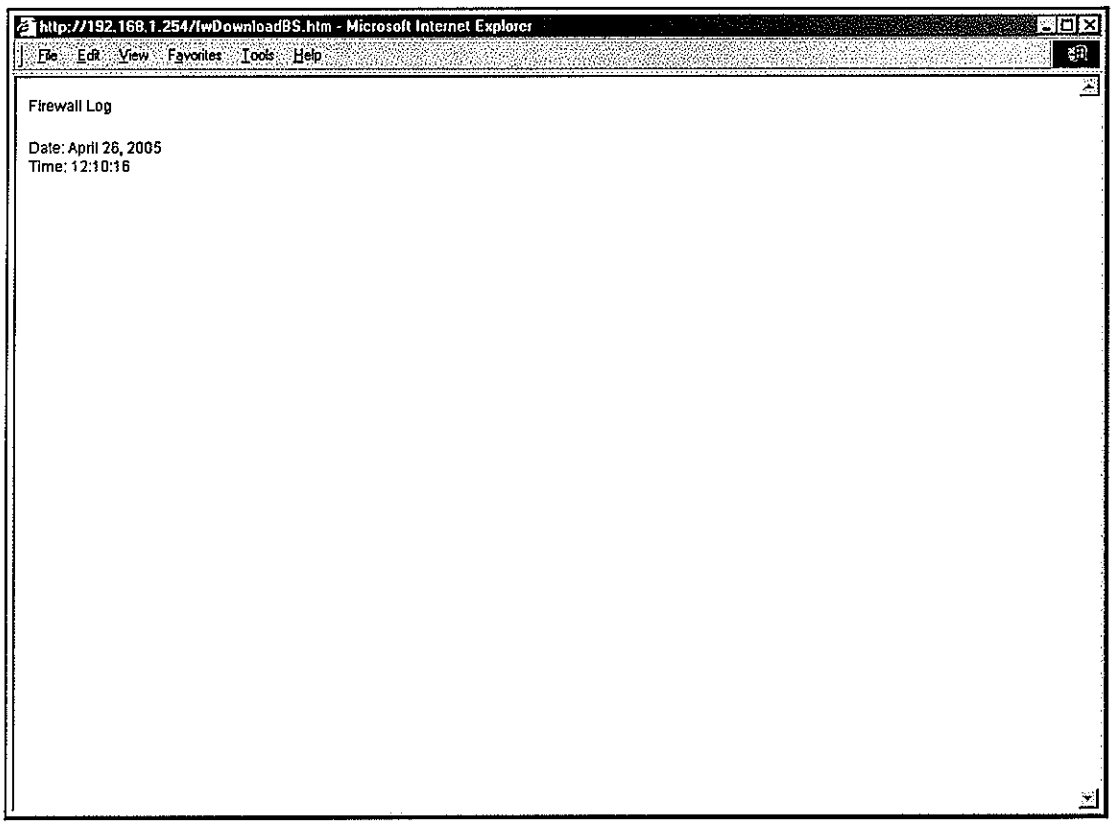
13.5.1 Clear Log

If you click on **Clear Log** in the **Firewall Log** page, the following pop-up screen will be displayed. Click on **OK** to clear the firewall log.



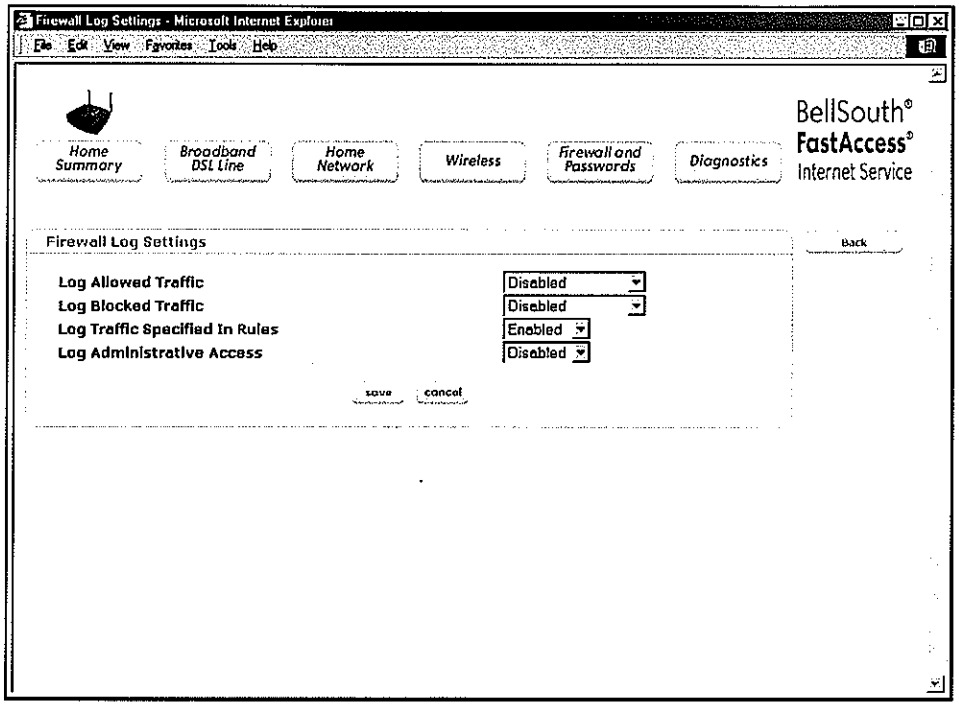
13.5.2 Printable/Savable Format

If you click on **Printable/Savable Format** in the **Firewall Log** page, the following page will be displayed. This option opens a new window that contains a list of all logged packets that can be saved or printed. After printing or saving the log, click your browser's "back" arrow to return to the **Firewall Log** page.



13.5.3 Settings

If you click on **Settings** in the **Firewall Log** page, the following page will be displayed. This page allows you to enable or disable the firewall log settings. Click on **save** to save the settings.

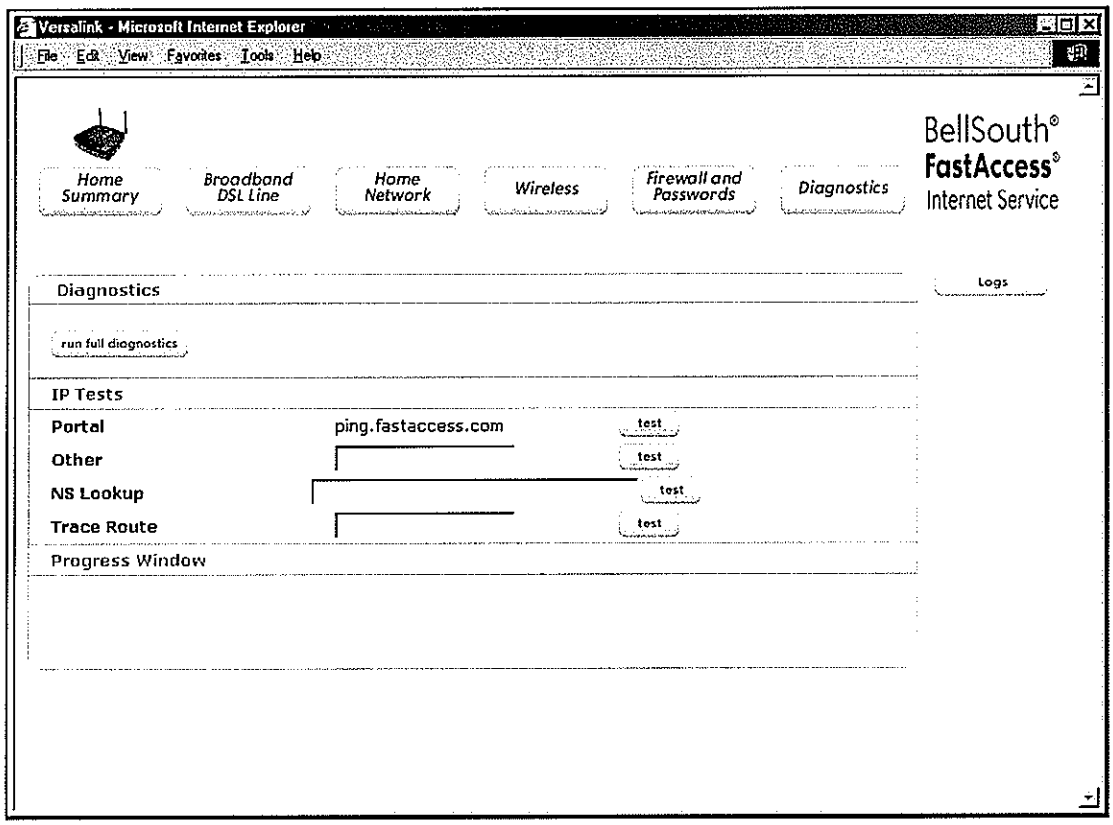


Firewall Log Settings	
Log Allowed Traffic	Factory Default = Disabled This option allows the user to log the traffic through the firewall that is allowed via the firewall setup page. Possible responses are: Disabled Inbound Packets Outbound Packets All Packets
Log Blocked Traffic	Factory Default = Disabled This option allows the user to log the traffic through the firewall that is being blocked via the firewall setup page. Possible Response are: Disabled Inbound Packets Outbound Packets All Packets
Log Traffic Specified in Rules	Factory Default = Enabled When Enabled, this option allows the user to log the traffic through the firewall that is being allowed via the custom rules setup page. If Disabled, this function will not be activated.
Log Administrative Access	Factory Default = Disabled When Enabled, this option allows the user to log the times an administrator has accessed any administrative protected modem pages.

14. DIAGNOSTICS

If you click on **Diagnostics** at the main menu, the following page will be displayed. This page enables you to perform simple diagnostic tests on your modem. To configure the settings, click on the desired submenu button at the right of the page.

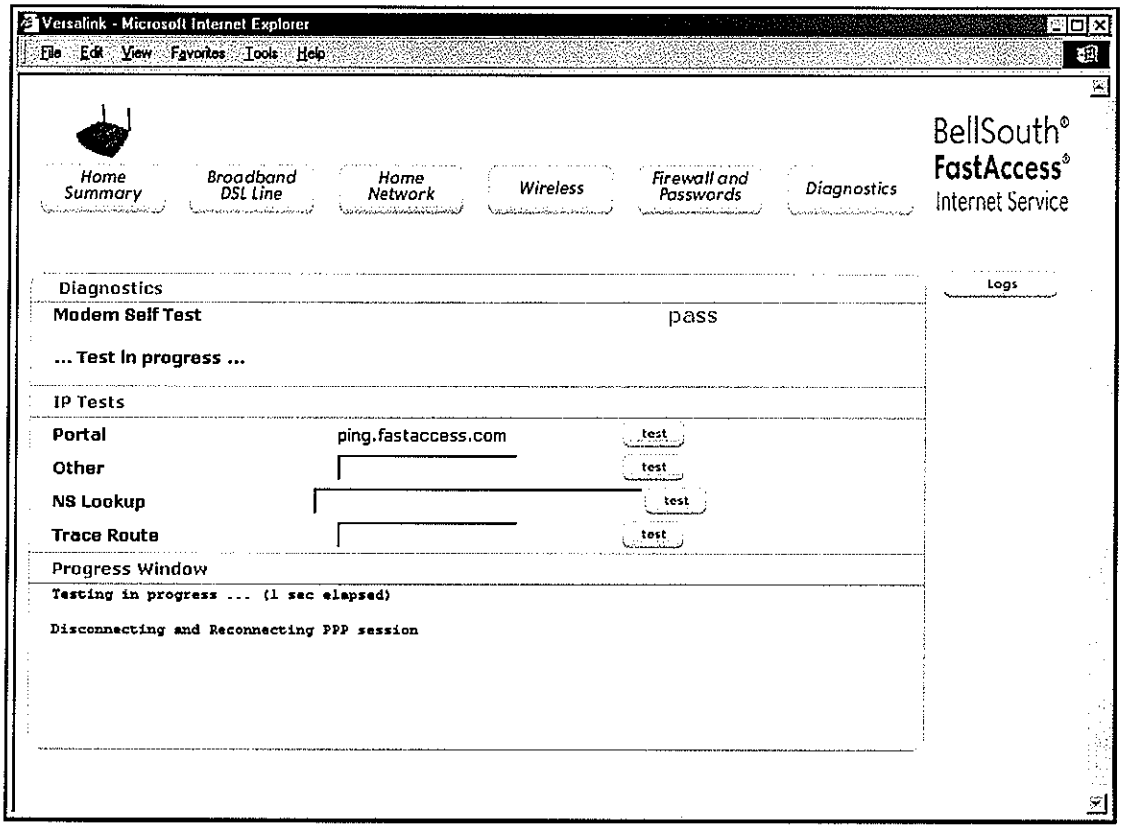
NOTE: The **Diagnostics** menu option will not be available if you are in Bridge Ethernet mode.



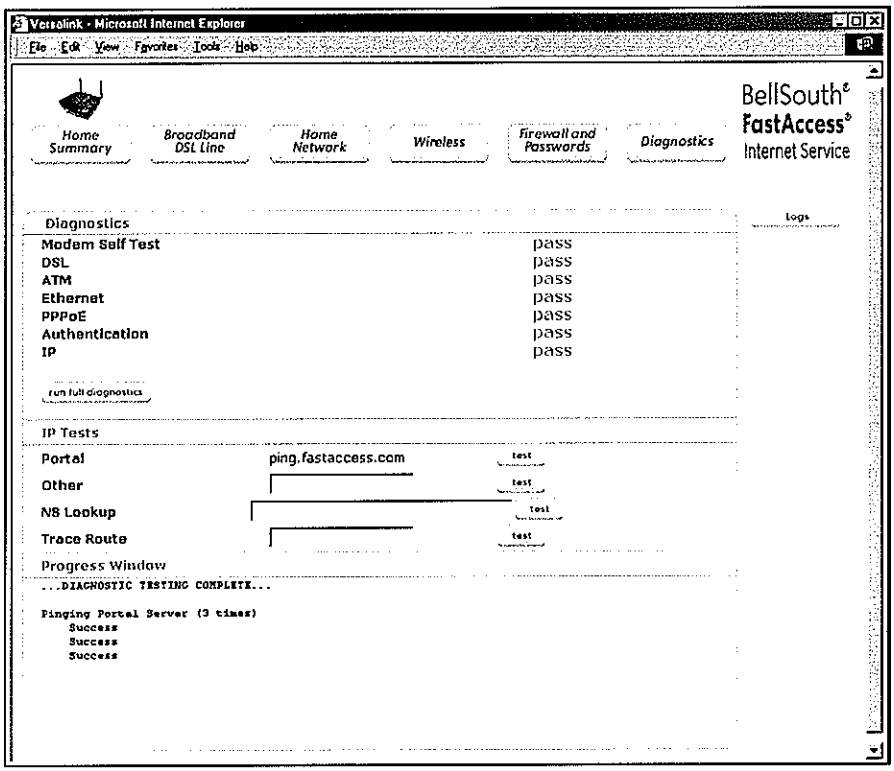
Diagnostics	
run full diagnostics	Enables you to run a full diagnostic test on the modem.
IP Tests	
Portal	Test will ping www.fastaccess.com portal
Other	Test will allow you to ping a specific URL or IP address of your choice
NS Lookup	Default NS Lookup = www.yahoo.com Test is a Name Server Lookup.
Trace Route	Test will determine the route taken to destination for the URL of your choice, and will show where the packet is stopped on the network.
Progress Window	
Progress Window	Displays the progress of the test being performed

14.1 Full Diagnostics

If you want to run a full diagnostics test, click on **run full diagnostics**. The following page will be displayed. The **Diagnostics** window will display "...Testing in progress..." until the diagnostics test has completed.



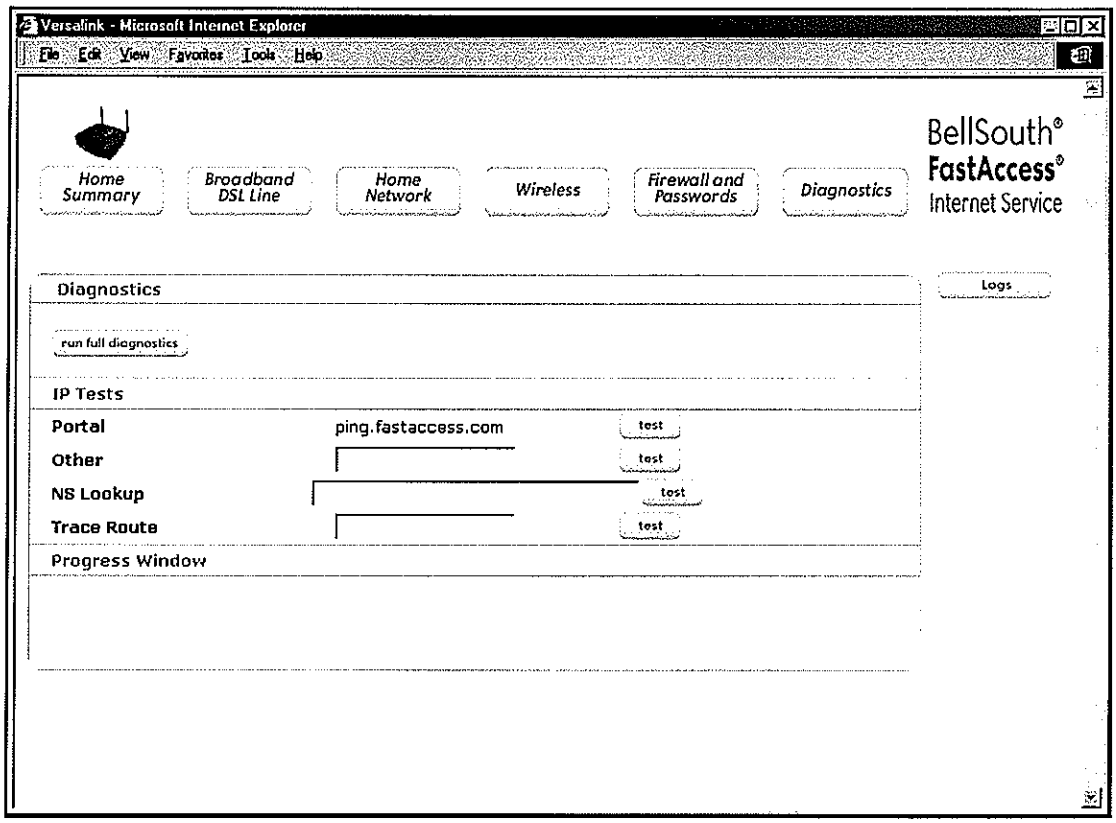
After the diagnostics test has completed, the page will refresh and the test results will be displayed. If there is a failure, the **Diagnostics** field will also display the details of the failed connection.



Diagnostics	
Modem Self Test	pass = Modem passed self test fail = Modem failed self test
DSL	pass = DSL connection established fail = No DSL connection established
ATM	pass = ATM cells have been received over the PVC fail = No ATM cells have been received over the PVC
Ethernet	pass = Ethernet frames have been received fail = No Ethernet frames have been received
PPPoE	pass = PADO has been received fail = No PADO has been received
Authentication	pass = Username/Password has been accepted fail = Username/Password has not been accepted
IP	pass = Ping to www.fastaccess.com was successful fail = Ping to www.fastaccess.com was not successful
IP Tests	
Portal	Test will ping www.fastaccess.com portal
Other	Test will allow you to ping a specific URL or IP address of your choice
NS Lookup	Default NS Lookup = www.yahoo.com Test is a Name Server Lookup.
Trace Route	Test will determine the route taken to destination for the URL of your choice, and will show where the packet is stopped on the network.
Progress Window	
Progress Window	Displays the progress of the test being performed

14.2 IP Tests

To perform an IP test, click the **test** button that is adjacent to the test you wish to run.



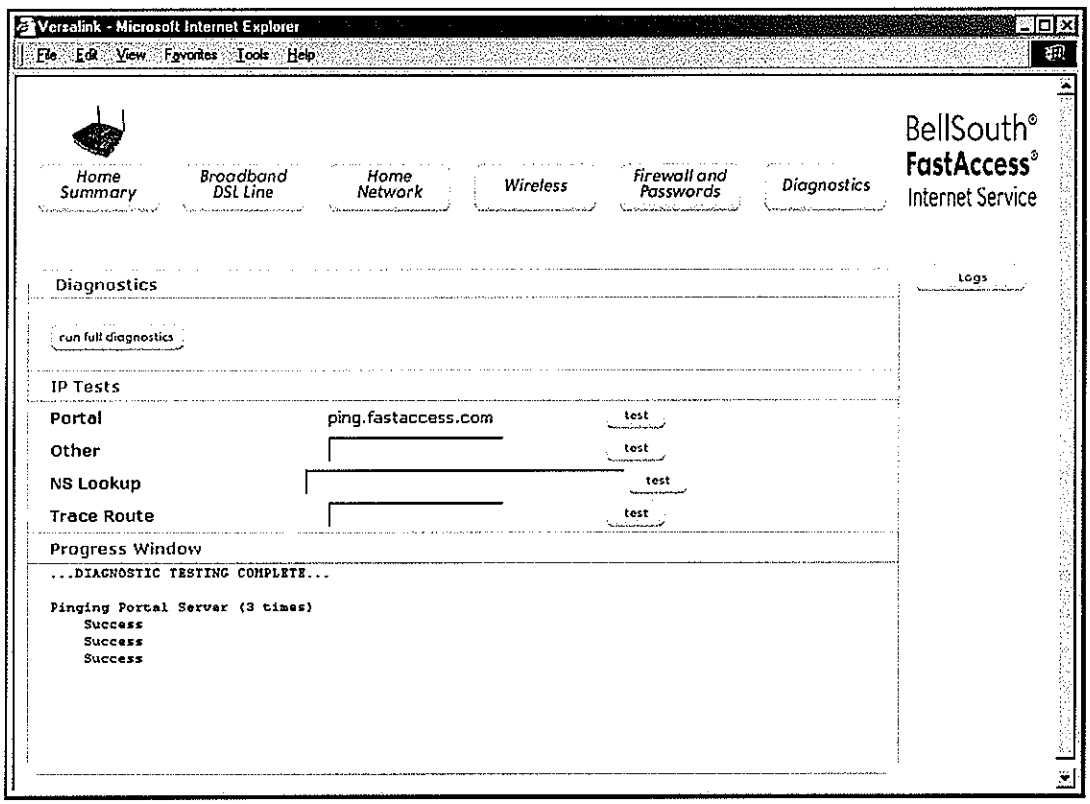
IP Tests	
Portal	Test will ping www.fastaccess.com portal
Other	Test will allow you to ping a specific URL or IP address of your choice
NS Lookup	Default NS Lookup = www.yahoo.com Test is a Name Server Lookup.
Trace Route	Test will determine the route taken to destination for the URL of your choice, and will show where the packet is stopped on the network.
Progress Window	
Progress Window	Displays the progress of the test being performed

14.2.1 Portal Test

The following page displays an example **Portal** test. The progress window will display the progress of the test. If there is a failure, the Diagnostics field will display the following message:

...Diagnostic Testing Complete...

Cannot access the specified URL or Web Address. Please try a different address by using the dialog box marked Other and clicking the test button. If the problem persists, go to the **Home Summary** page and restart the connection via connect/disconnect button in the **Easy Login** page. After the connection restarts, return to the Diagnostics page and try the test again. If the problem persists, contact the BellSouth help desk at 1-888-321-2DSL (2375).



14.2.2 Other

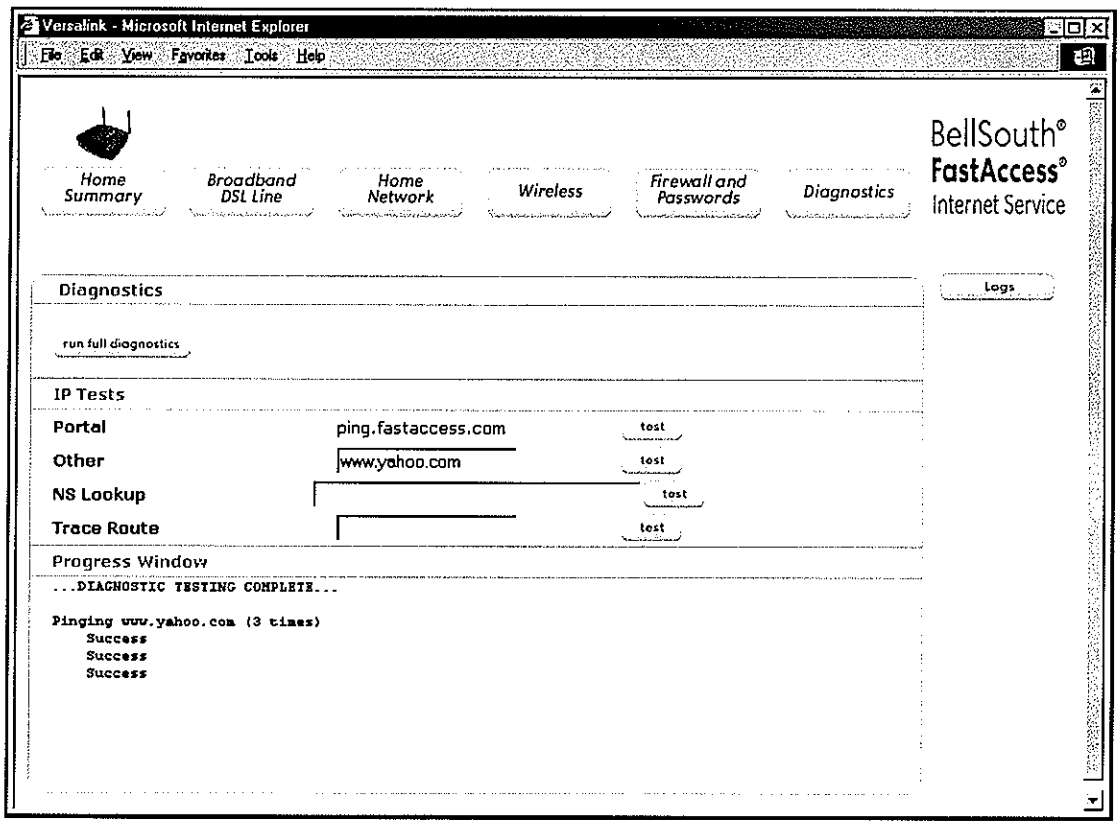
The following page displays an example **Other** test. Note: If the **Other** field is blank when the **test** button is clicked, the progress window will display a message that there is no IP address or URL to test.

If there is a failure, the progress window will display the following message:

...Diagnostic Testing Complete...

Pinging (IP address or URL you entered) (3 times)
DNS Failure

Go to the **Home Summary** page and restart the connection via connect/disconnect button in the **Easy Login** page. After the connection restarts, return to the **Diagnostics** page and try the test again. If the problem persists, contact the BellSouth help desk at 1-888-321-2DSL (2375).



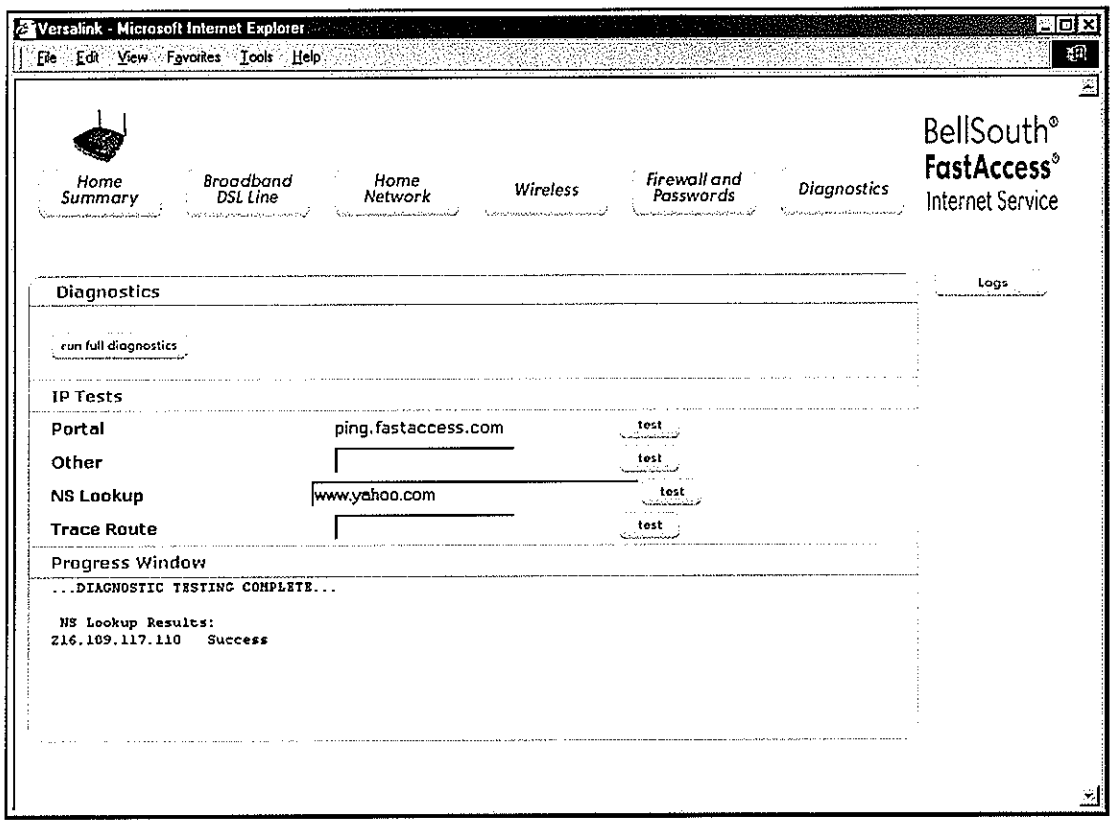
14.2.3 NS Lookup

The following page displays an example **NS Lookup** test. Note: If the **NS Lookup** field is blank when the test button is clicked the progress window will display a message that there is no data, enter host name.

If there is a failure, the progress window will display the following message:

Diagnostic Testing Complete
NS Lookup Results: Host not found

Go to the **Home Summary** page and restart the connection via connect/disconnect button in the **Easy Login** page. After the connection restarts, return to the **Diagnostics** page and try the test again. If the problem persists, contact the BellSouth help desk at 1-888-321-2DSL (2375).

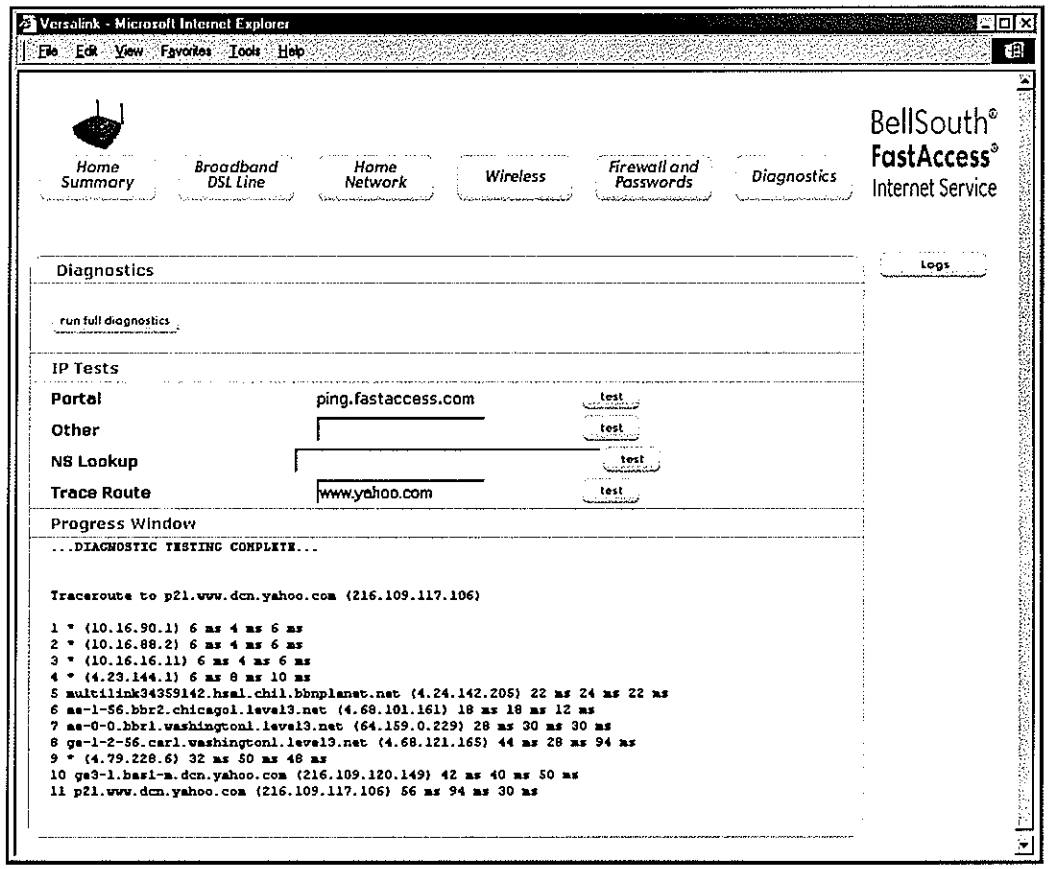


14.2.4 Trace Route

The following page displays an example **Trace Route** test. Note: If the **Trace Route** field is blank when the **test** button is clicked or if there is a failure, the progress window will display only the following message:

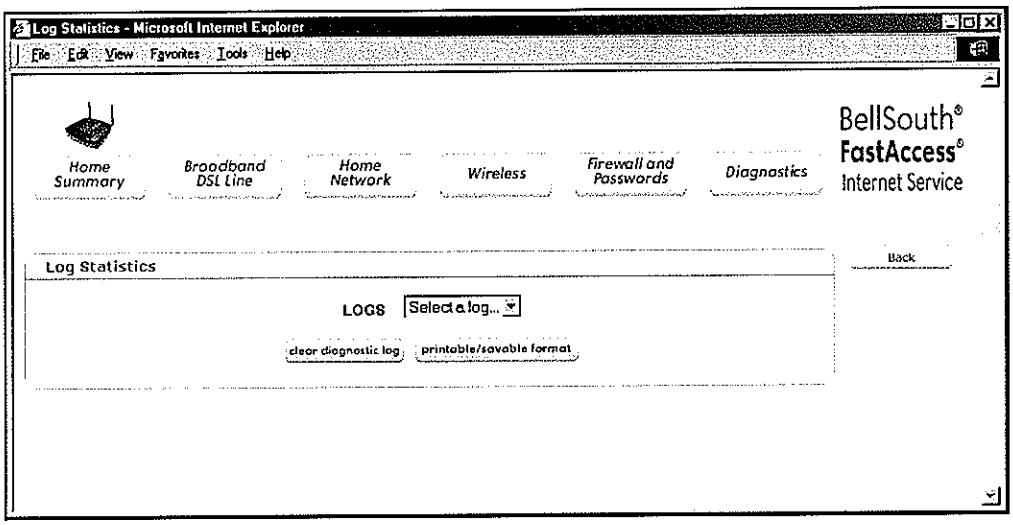
Diagnostic Testing Complete

Go to the **Home Summary** page and restart the connection via connect/disconnect button in the **Easy Login** page. After the connection restarts, return to the **Diagnostics** page and try the test again. If the problem persists, contact the BellSouth help desk at 1-888-321-2DSL (2375).

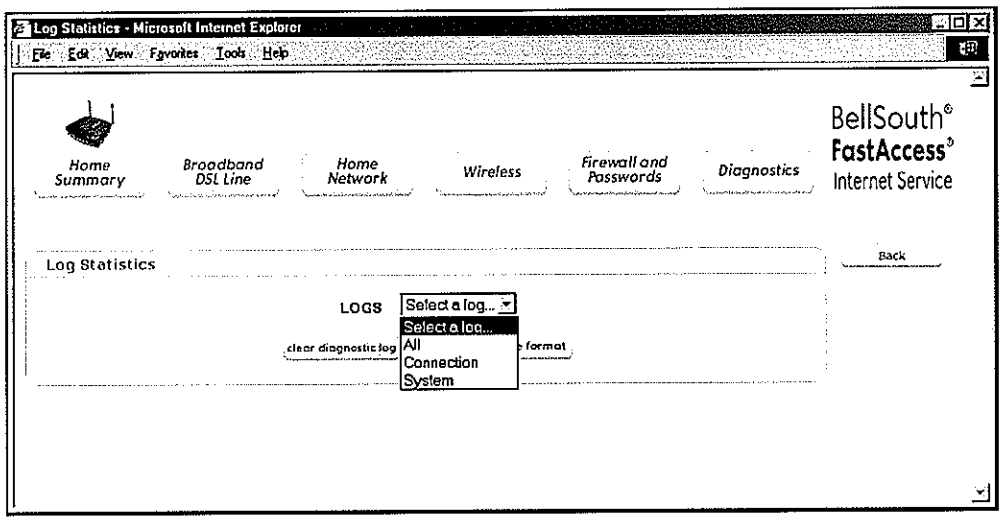


14.3 Logs

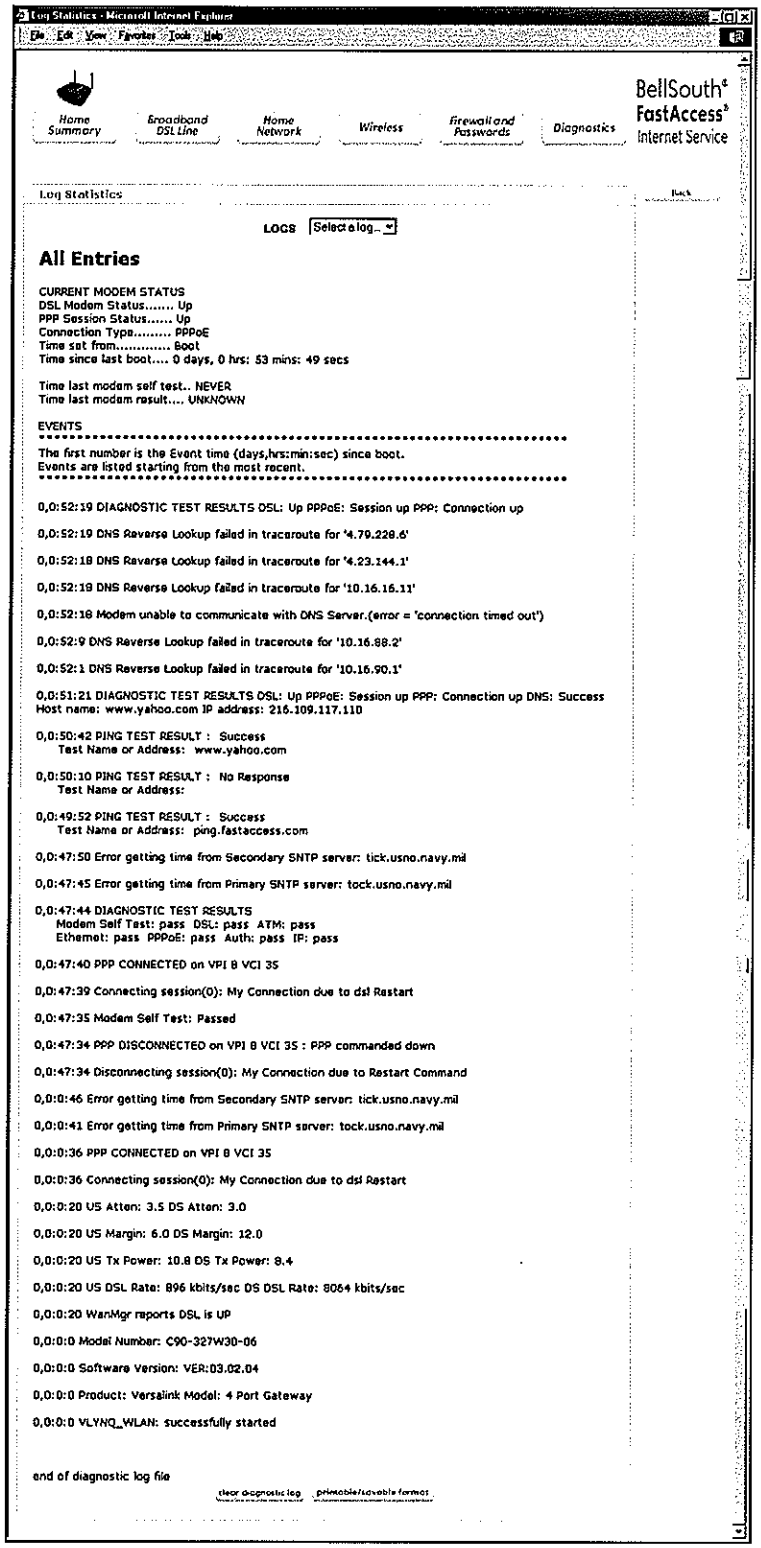
If you click **Logs** in the **Diagnostics** page, the following page will be displayed.



Next, select an option from the **LOGS** drop-down menu.



If you selected **All**, the following page will be displayed. Click **clear** to clear the log statistics, or click **printable/savable format** to print or save the logs file to a location on your PC.



15. NAT SERVICES

For your convenience, the Westell VersaLink Gateway supports protocols for Applications, Games, and VPN-specific programs. Table 5 provides protocol information for the services that are supported by your VersaLink Gateway.

Note: To configure VersaLink for a service or application, follow the steps described in section 11.3 (NAT/Gaming) of this User Guide.

Table 5. Applications/Games/NAT VPN Support

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

Application/Game	Port/Protocol
Fighter Ace II	50000-50100 TCP/UDP
Fighter Ace II for DX play	50000-50100 TCP/UDP, 47624 TCP, 2300-2400 TCP/UDP
FTP	20 TCP, 21 TCP
GameSpy Online	UDP 3783 UDP 6515 TCP 6667 UDP 12203 TCP/UDP 13139UDP 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 ALG	ENABLES ALG
IPSEC ESP	PROTOCOL 50
IPSEC IKE	500 UDP
Ivisit	9943 UDP, 56768 UDP
JKII:JO (Jedi Knight II: Jedi Outcast)	UDP - 28070 (default) UDP- 27000 to 29000
KALI, Doom & Doom II	2213 UDP, 6666 UDP (EACH PC USING KALI MUST USE A DIFFERENT PORT NUMBER STARTING WITH 2213 + 1
KaZaA	1214 TCP/UDP
Limewire	6346 TCP/UDP, 1214 TCP
Medal Of Honor: Allied Assault	TCP 80 UDP 53 UDP 2093 UDP 12201 TCP 12300 UDP 2135 UDP 2139

Application/Game	Port/Protocol
	TCP/UDP 28900
mIRC Chat	6660-6669 TCP
Motorhead Server	16000 TCP/UDP, 16010-16030 TCP/UDP
MSN Game Zone	6667 TCP, 28800-29000 TCP
MSN Game Zone (DX 7 & 8 play)	6667 TCP, 6073 TCP, 28800-29000 TCP, 47624 TCP, 2300-2400 TCP/UDP This service will open up port's for both traffic directions.
MSN Messenger	6891-6900 TCP, 1863 TCP/UDP, 5190 UDP, 6901 TCP/UDP
Napster	6699 TCP
Need for Speed 3, Hot Pursuit	1030 TCP
Need for Speed, Porsche	9442 UDP
Net2Phone	6801 UDP
NNTP	119 TCP/UDP
Operation FlashPoint	47624 UDP, 6073 UDP, 2300-2400 TCP/UDP, 2234 TCP
Outlaws	5310 TCP/UDP
Pal Talk	2090-2091 TCP/UDP, 2095 TCP, 5001 TCP, 8200-8700 TCP/UDP, 1025-2500 UDP
pcAnywhere host	5631 TCP, 5632 UDP, 22 UDP
Phone Free	1034-1035 TCP/UDP, 9900-9901 UDP, 2644 TCP, 8000 TCP
Quake 2	27910 UDP
Quake 3	27660 UDP Each computer playing QuakeIII must use a different port number, starting at 27660 and incrementing by 1. You'll also need to do the following: 1. Right click on the QIII icon 2. Choose "Properties" 3. In the Target field you'll see a line like "C:\Program Files\Quake III Arena\quake3.exe" 4. Add the Quake III net_port command to specify a unique communication port for each system. The complete field should look like this: "C:\Program Files\Quake III Arena\quake3.exe" +set net_port 27660 5. Click OK. 6. Repeat for each system behind the NAT, adding one to the net_port selected (27660,27661,27662)
Quicktime 4/Real Audio	6970-32000 UDP, 554 TCP/UDP
Rainbow Six & Rogue Spear	2346 TCP
RealOne Player	TCP - 554, 7070 to 7071 UDP - 6970 to 7170
Real Audio	6970-7170 UDP
Return To Castle Wolfenstein	Default -27960 TCP/UDP UDP - 27950 to 27980
Roger Wilco	TCP/UDP 3782 UDP 3783 (BaseStation)
ShoutCast Server	8000-8005 TCP
Spinner Radio/Netscape Music	TCP - 554
SSH Secure Shell	22 TCP/UDP
Starcraft	2346 TCP
Starfleet Command	2300-2400 TCP/UDP, 47624 TCP/UDP
SOF/SOFII (Soldier of Fortune / Soldier of Fortune	UDP - 28910 to 28915

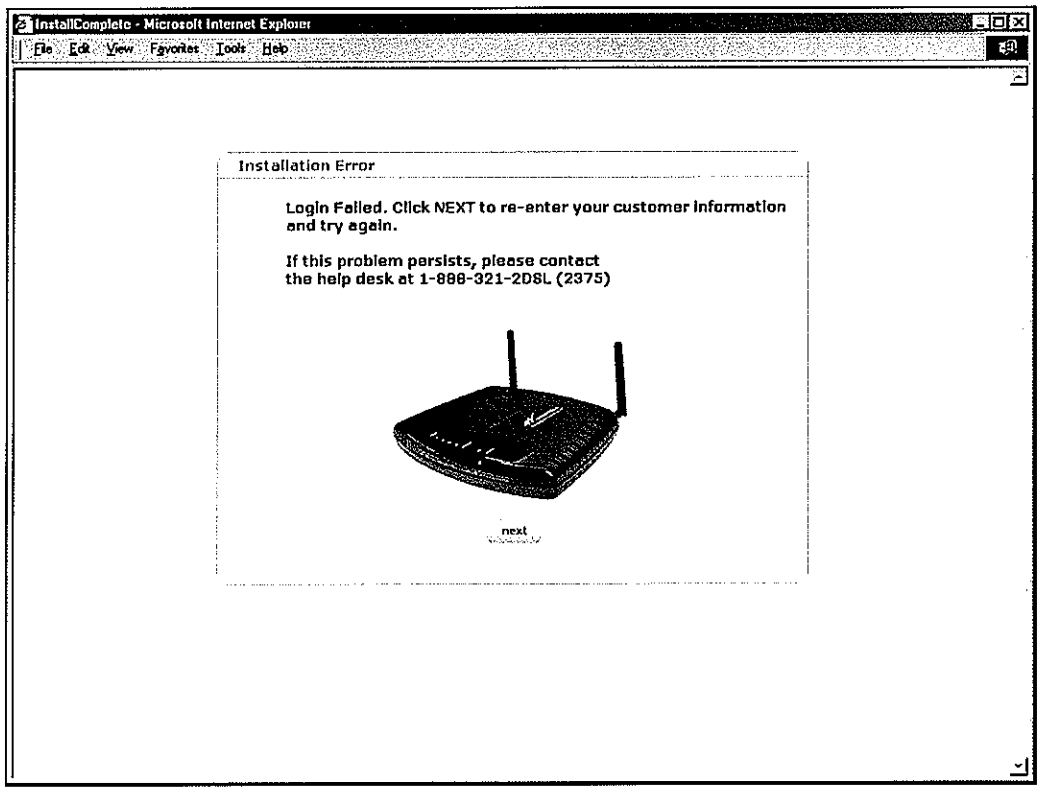
Application/Game	Port/Protocol
II)	
Telnet	23 TCP
Tiberian Sun & Dune 2000	1140-1234, 4000 TCP/UDP
Tribes2	TCP - 15104, 15204, 15206, 6660 to 6699 UDP - 27999 to 28002
Ultima Online	5001-5010 TCP, 7775-7777 TCP, 8800-8900 TCP, 9999 UDP, 7875 UDP
Unreal Tournament server	7777 (default gameplay port) 7778 (server query port 7779,7779+ are allocated dynamically for each helper UdpLink objects, including UdpServerUplin objects. Try starting with 7779-7781 and add ports if needed 27900 server query, if master server uplink is enabled. Home master servers use other ports like 27500 Port 8080 is for UT Server Admin. In the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 and ServerName to the IP assigned to the router from your ISP.
USENET News Service	143 TCP
VNC, Virtual Network Computing	5500 TCP, 5800 TCP, 5900 TCP
Westwood Online, C&C	4000 TCP/UDP, 1140-1234 TCP/UDP
World Wide Web (HTTP)	80 TCP 443 TCP (SSL) 8008 OR 8080 TCP (PROXY)
Yahoo Messenger Chat	5000-5001 TCP
Yahoo Messenger Phone	5055 UDP
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.

16. APPENDIX A: TROUBLESHOOTING CONNECTION FAILURES

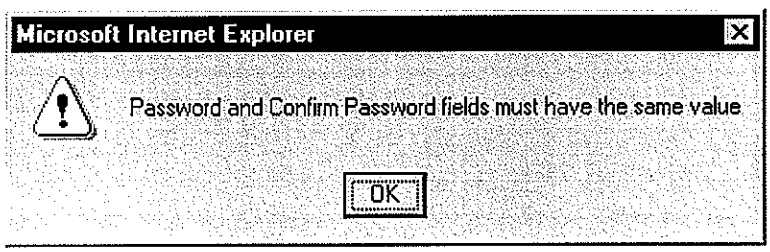
Refer to this section for a detailed explanation on connection failures.

16.1 Login Failed at Customer Information

If you entered your login values (provided by BellSouth) at the **Customer Information** page and your login failed, the following page will appear. Click **next** to return to the **Customer Information** page and re-enter your login values. If this problem persists, contact the BellSouth help desk at 1-888-321-2DSL (2375).

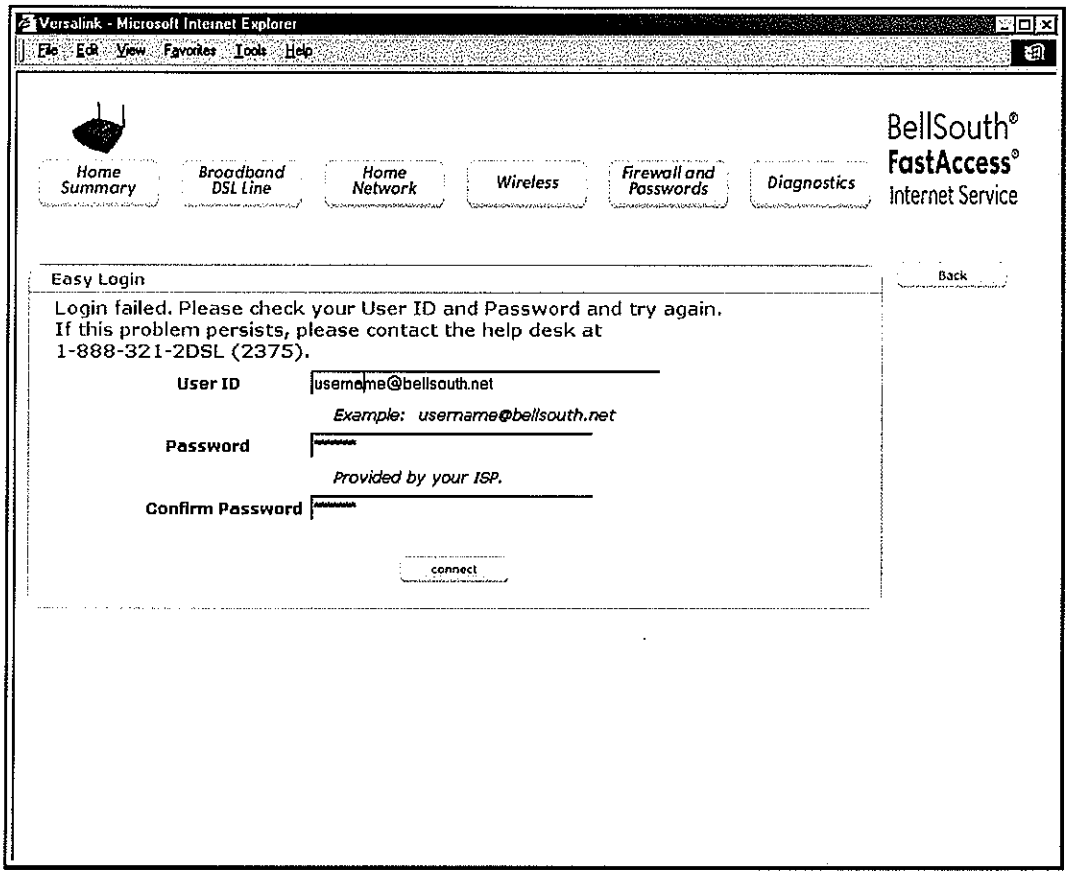


The following pop-up screen will be displayed if the value in your **Confirm Password** field is not identical to the value in your **Password** field. The **Password** and **Confirm Password** fields must contain identical values in order to establish a successful login. If you have retyped the appropriate values in each field and are still unable to establish a connection, contact the BellSouth help desk at 1-888-321-2DSL (2375).

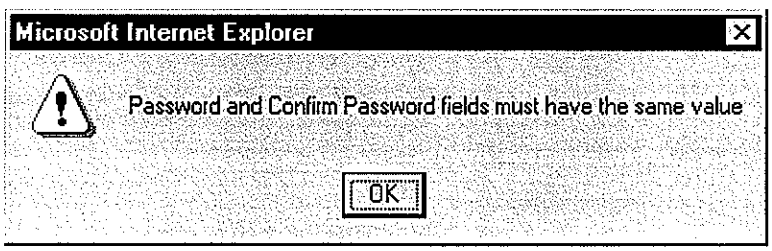


16.2 Login Failed at Easy Login Page

If you entered your login values (provided by BellSouth) at the **Easy Login** page and your login failed, the following page will appear. Retype the appropriate values in the **User ID** and **Password** fields and click on **connect.** If this problem persists, contact the BellSouth help desk at 1-888-321-2DSL (2375).



The following pop-up screen will be displayed if the value in your **Confirm Password** field is not identical to the value in your **Password** field. The **Password** and **Confirm Password** fields must contain identical values in order to establish a successful login. If you have retyped the appropriate values in each field and are still unable to establish a connection, contact the BellSouth help desk at 1-888-321-2DSL (2375).

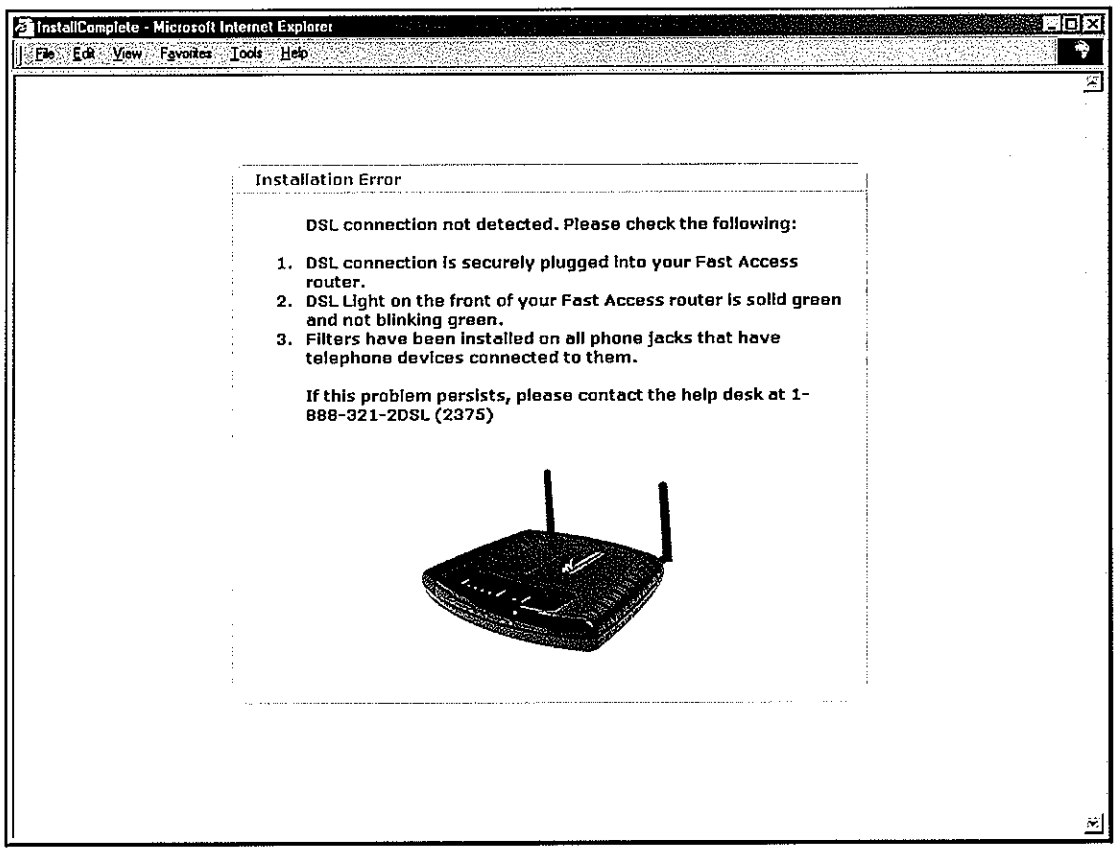


16.3 DSL Connection is Down

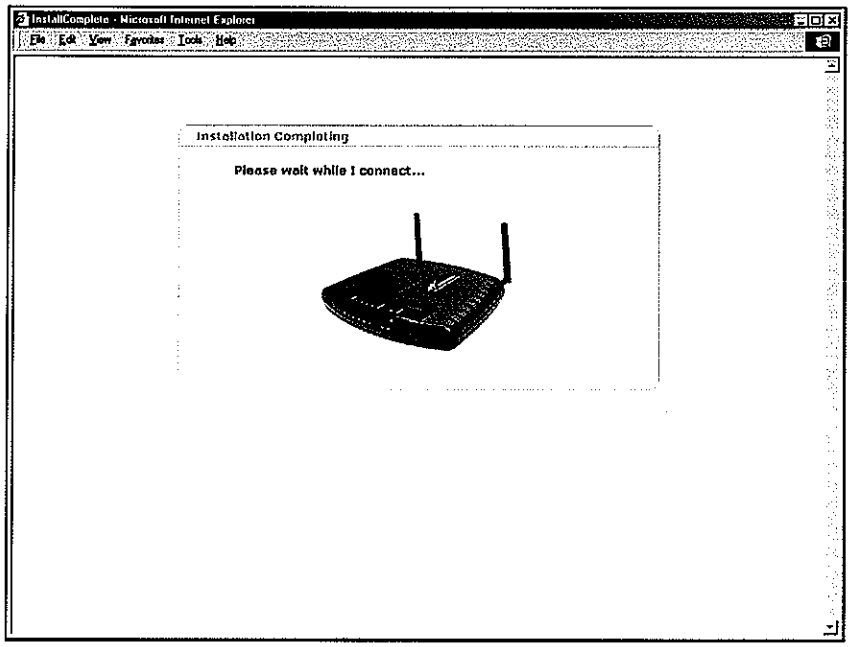
If your DSL connection is down when you log into the **Customer Information** page, the following page will appear.

- Check that the phone line is securely connected to your FastAccess modem.
- Check that the DSL LED on the front of your FastAccess modem is solid green and is not blinking.
- Check that filters have been installed on all phone jacks that have telephone devices connected to them.

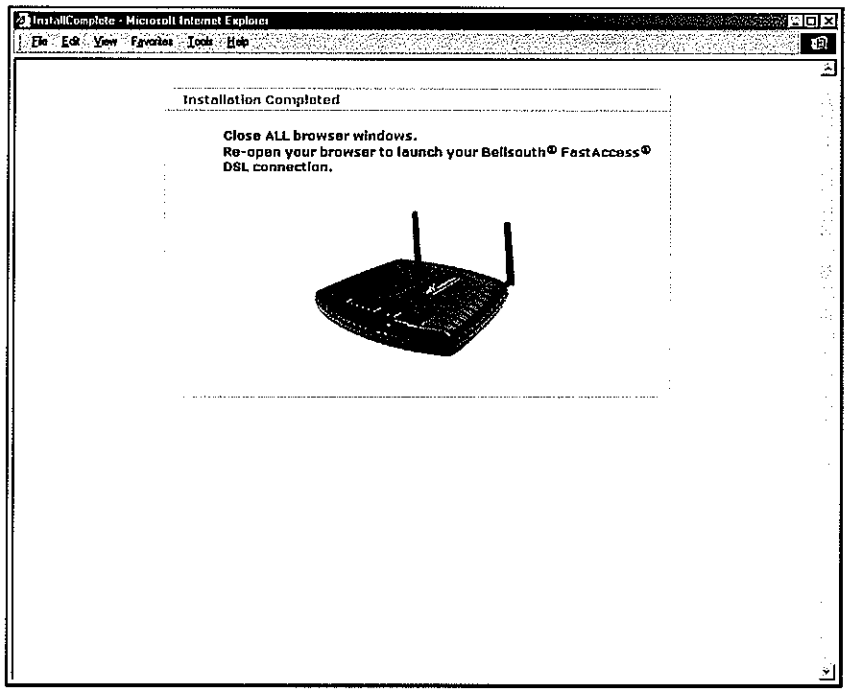
If this problem persists, contact the BellSouth help desk at 1-888-321-2DSL (2375).



Once a DSL connection is detected, please wait a brief moment while the modem connects to the ISP's equipment. After the modem has connected, the **DSL** LED will light solid green and the DSL sync will be Up.



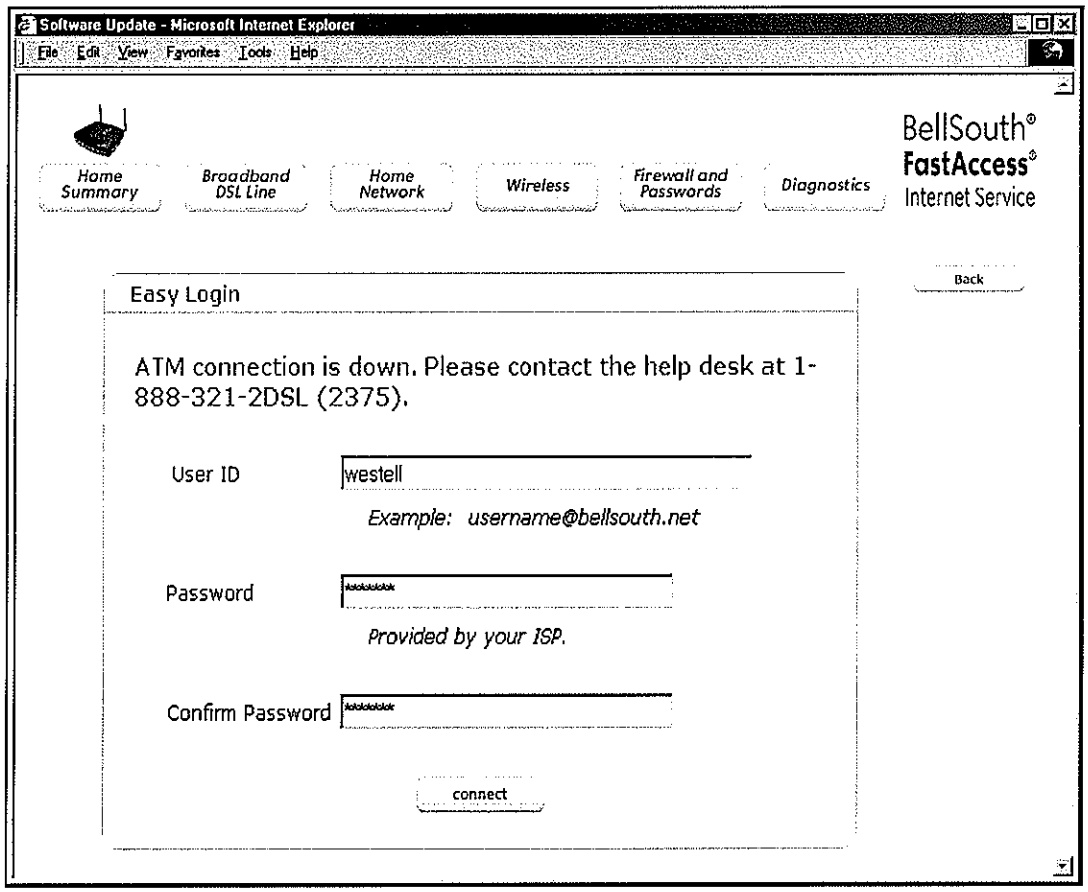
Close all browser windows, and then re-open your browser to launch your BellSouth® FastAccess® DSL connection.



When you are ready to access the modem's web pages, type **http://launchmodem** in the browser's address bar and press "Enter" on your keyboard. The **Home Summary** page will be displayed.

16.4 ATM Connection is Down

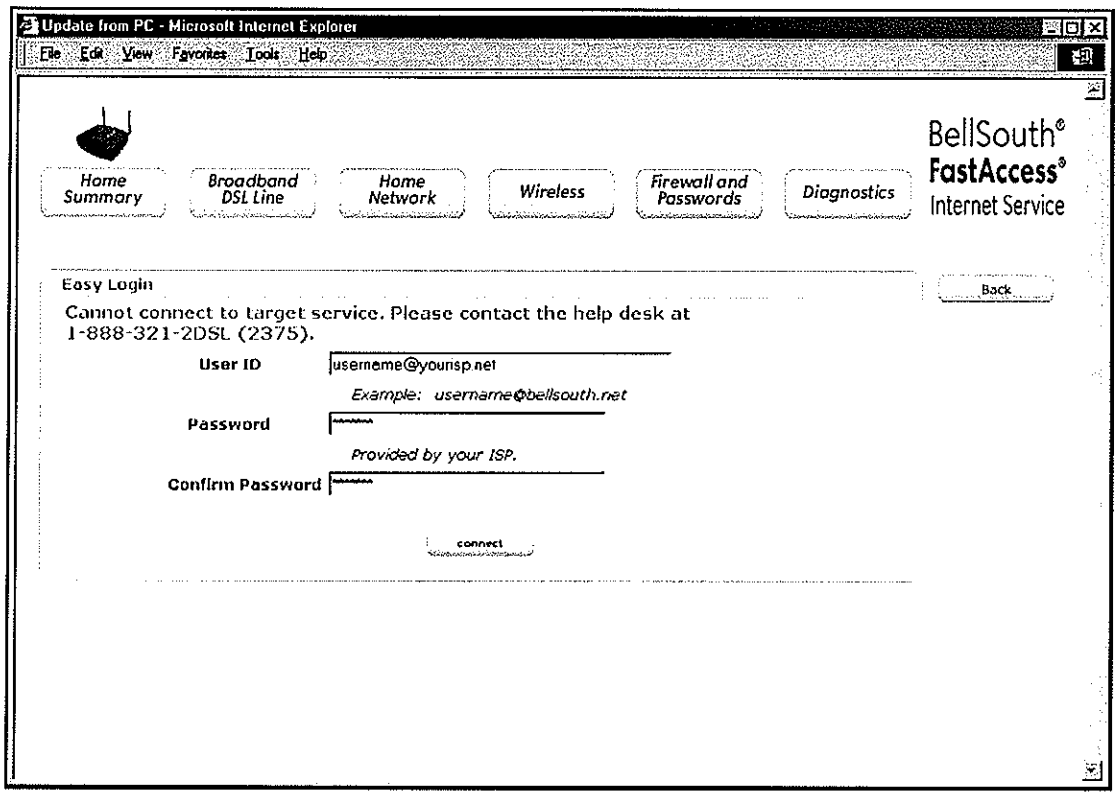
If the ATM connection is down when you log into the **Customer Information** page, the following page will appear. Contact the BellSouth help desk at 1-888-321-2DSL (2375).



16.5 Cannot Connect to Target Internet Service Provider

If you cannot connect to your target Internet service provider, the following page will appear. Contact the BellSouth help desk at 1-888-321-2DSL (2375).

NOTE: If you attempt to connect to the Internet and your connection fails, the **Internet** LED will light red and then return to the off state.

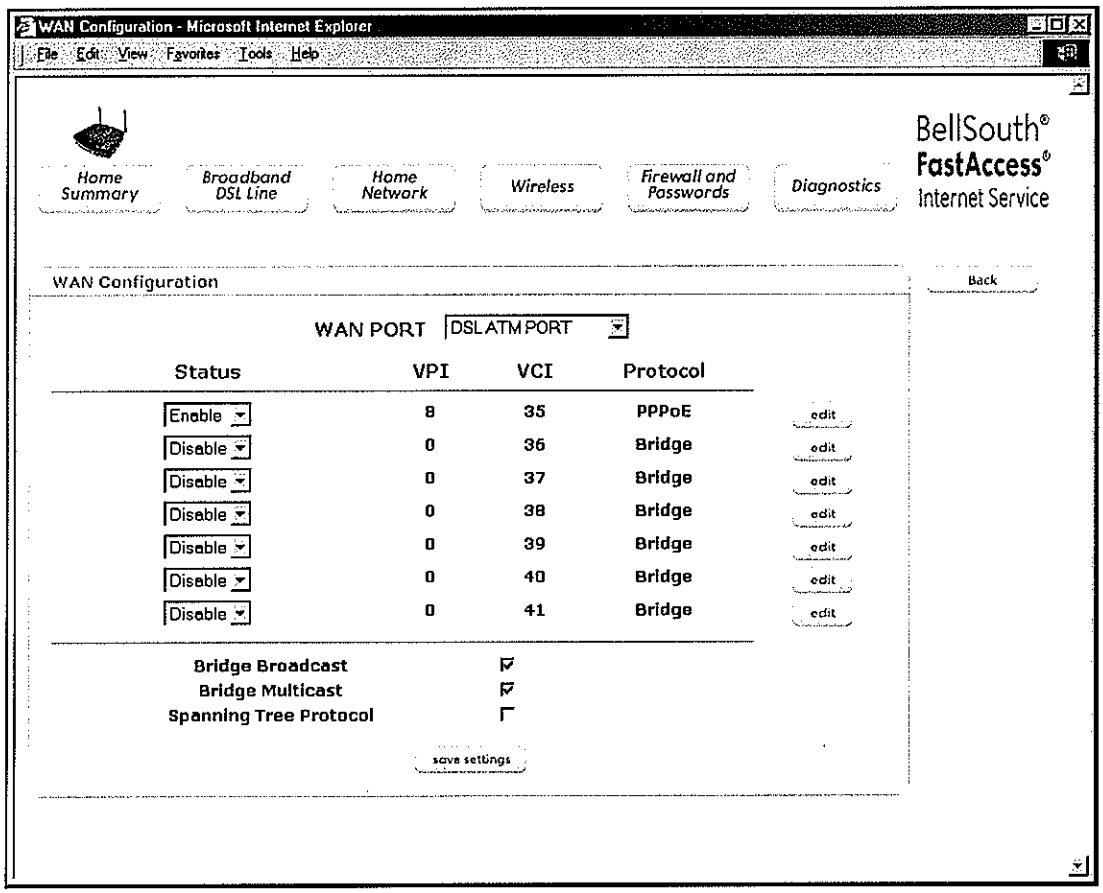


Once your connection succeeds, the **Internet** LED will light solid green, and at the **Home Summary** page the **Internet Login** field will display **Up.**

17. APPENDIX B: CONFIGURING THE WAN PORT

This section explains the configuration details for VersaLink's WAN PORT feature. To access this feature, click Broadband DSL Line as the main menu, and then click the WAN button. The following page will be displayed. At the **WAN PORT** drop-down menu, select either **DSLATM PORT** or **ETHERNET PORT 1** for your WAN setting.

NOTE: If you use VersaLink's **DSLATM PORT** mode, you will enable VersaLink's DSL transceiver. This will disable the WAN Ethernet interface (labeled **Ethernet 1**) on the rear panel of VersaLink and allow the WAN interface to use the DSL port instead. Conversely, if you use VersaLink's uplink mode, **ETHERNET PORT 1**, you will disable VersaLink's DSL transceiver. This will disable the DSL port (on the rear panel of VersaLink) and allow the WAN interface to use the **Ethernet 1** port.

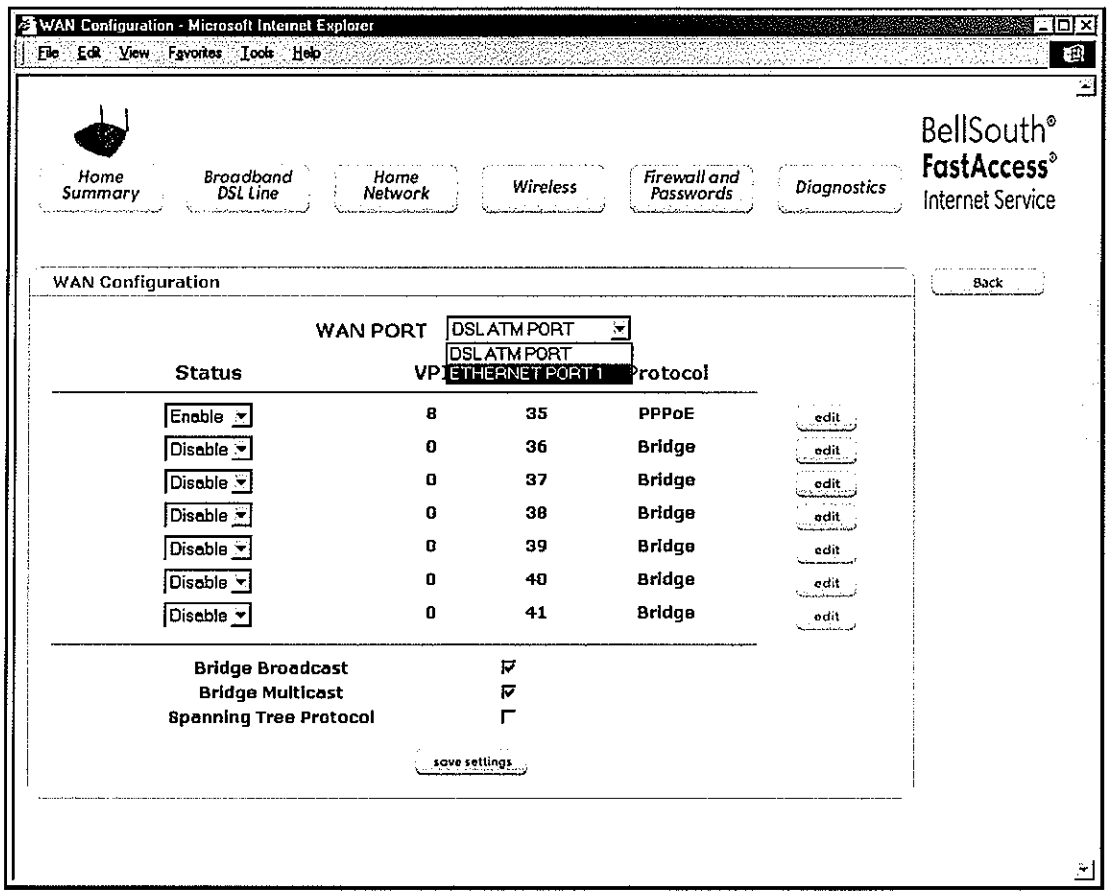


17.1 Disabling DSLATM PORT – Enabling ETHERNET PORT 1

If VersaLink is in **DSLATM PORT** mode and you want to configure VersaLink for **ETHERNET PORT 1** mode, follow the instructions provided in this section. By using the **ETHERNET PORT 1**, you will disable VersaLink's DSL transceiver. This will disable the DSL Port and allow the WAN interface to use the WAN Ethernet Port (Ethernet 1) on the rear of the modem.

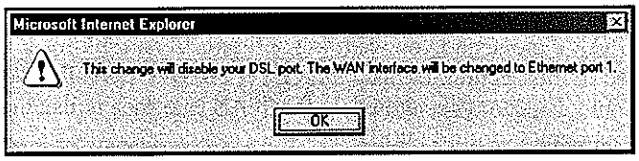
NOTE: The uplink feature (Ethernet 1) is optional. If **ETHERNET PORT 1** is disabled, VersaLink will use DSL and Wireless only, and the Ethernet 1 port can be used in addition to ports E2, E3, and E4 for LAN access. When using **DSLATM PORT**, you may connect to any of the three Ethernet (E2, E3, or E4) jacks on the rear panel of VersaLink as they serve as an Ethernet switch. Ethernet 1 port is used as a WAN transport connection when installing VersaLink without DSL. When using Ethernet 1 port instead of the DSL port, Ethernet LAN connection is limited to ports E2, E3, and E4. The uplink feature (ETHERNET PORT 1) is optional, and if it is not enabled in the .ini file, VersaLink will use DSL and Wireless only.

To use **ETHERNET PORT 1**, click the **WAN** button in the **Broadband DSL Line** page, the following page will be displayed. Next, select **ETHERNET PORT 1** from the **WAN PORT** drop-down menu.

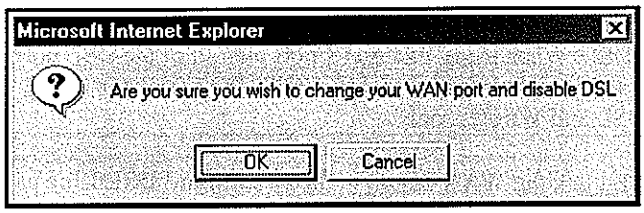


NOTE: If you experience any problems, please reset VersaLink via the external hardware reset button or via the procedure defined in the **Reset Modem** menu in section 9.5 (Reset Modem). The actual information displayed in this page may vary, depending on network connection established.

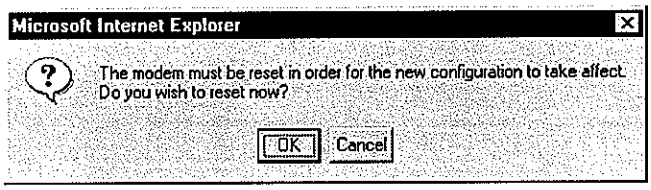
If you selected **ETHERNET PORT 1** from the **WAN PORT** drop-down menu, the following screen will be displayed. Click **OK.**



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



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



If you clicked on **OK** in the preceding screen, the following screen will be displayed. VersaLink will be reset and the new configuration will take effect. After a brief delay, the **Home Summary** page will be displayed.

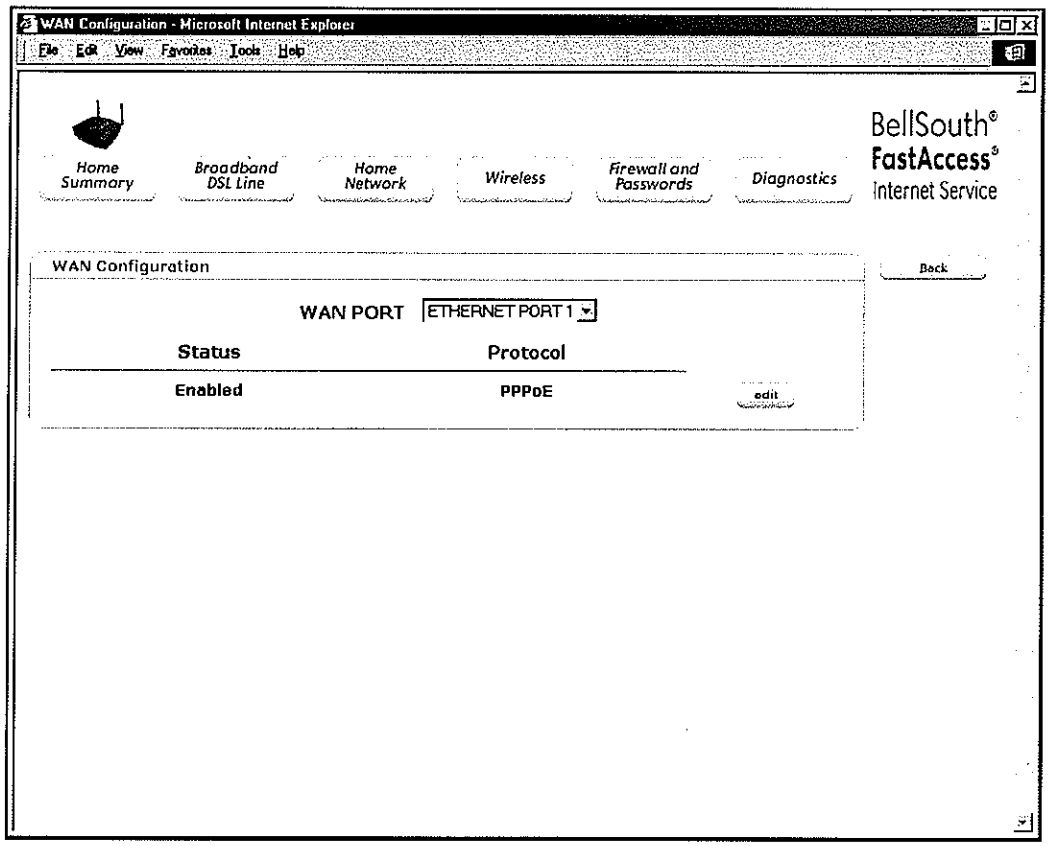
NOTE: After VersaLink has been reset, the **DSL** LED will be OFF. This is because the DSL transceiver has now been disabled. However, the Power, Ethernet, Wireless and Internet LEDs will remain lit.

17.2 Enabling DSLATM PORT – Disabling ETHERNET PORT 1

If VersaLink is in **ETHERNET PORT 1** mode and you want to configure VersaLink for **DSLATM PORT** mode, follow the instructions provided in this section. By using the **DSLATM PORT**, you will enable VersaLink's DSL transceiver. This will disable the WAN Ethernet port and allow the WAN interface to use the DSL port on the rear of the modem. To enable the **DSLATM PORT**, click on **Broadband DSL Line** at the main menu, and then click the **WAN** button.

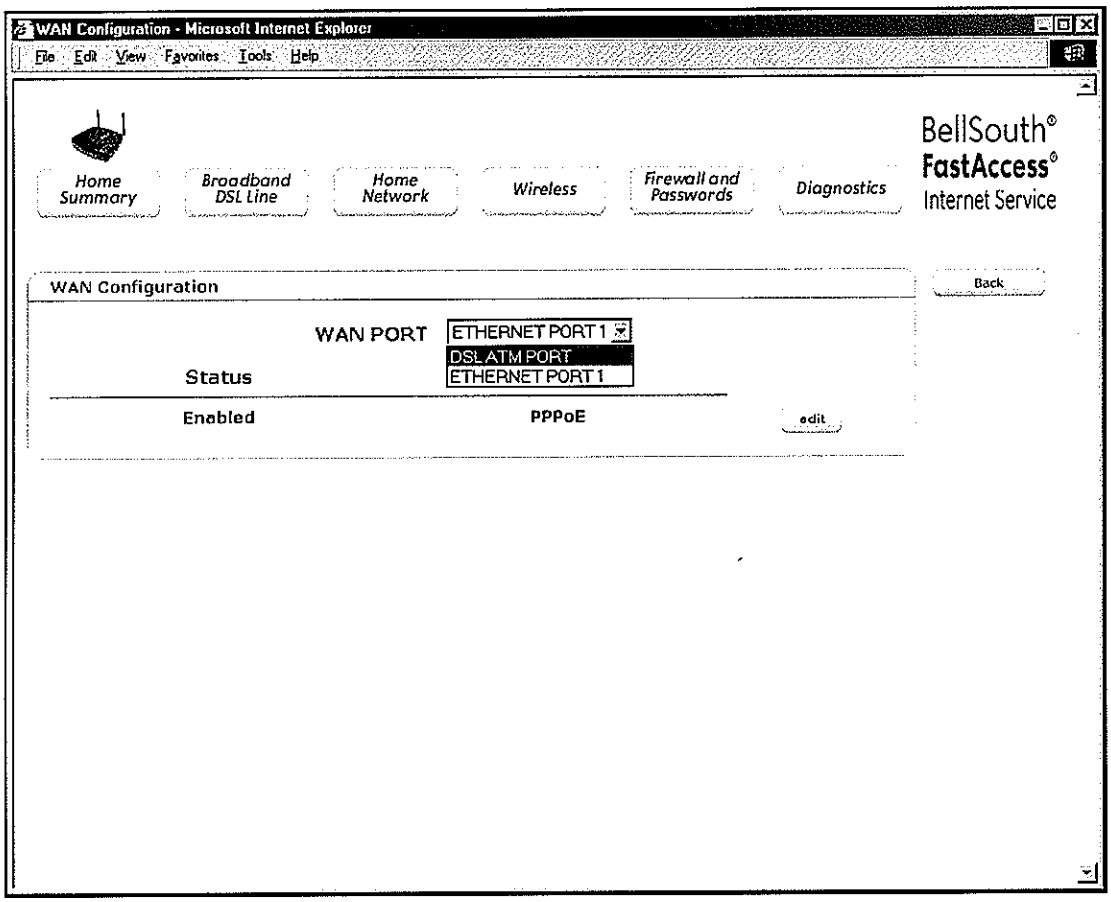
NOTE: The uplink feature (Ethernet 1) is optional. If **ETHERNET PORT 1** is disabled, VersaLink will use DSL and Wireless only, and the Ethernet 1 port can be used in addition to ports E2, E3, and E4 for LAN access. When using DSLATM port, you may connect to any of the three Ethernet (E2, E3, or E4) jacks on the rear panel of VersaLink as they serve as an Ethernet switch. Ethernet 1 port is used as a WAN transport connection when installing VersaLink without DSL. When using Ethernet 1 port instead of the DSL port, Ethernet LAN connection is limited to ports E2, E3, and E4. The uplink feature (ETHERNET PORT 1) is optional, and if it is not enabled in the .ini file, VersaLink will use DSL and Wireless only.

To use **DSLATM PORT**, click the **WAN** button in the **Broadband DSL Line** page, the following page will be displayed.

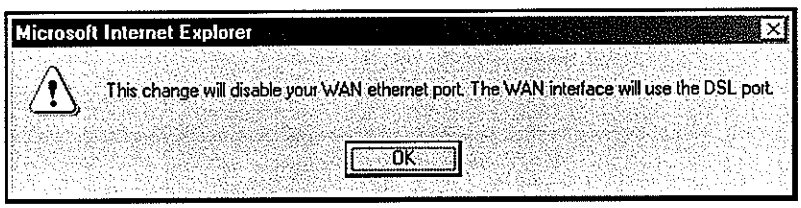


NOTE: If you experience any problems, please reset VersaLink via the external hardware reset button or via the procedure defined in the **Reset Modem** menu in section 9.5 (Reset Modem). The actual information displayed in this page may vary, depending on network connection established.

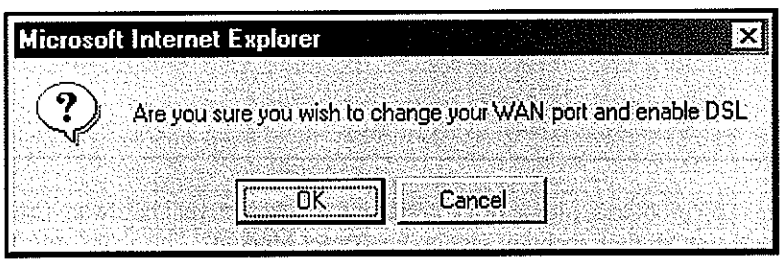
Next, select **DSLATM PORT** from the **WAN PORT** drop-down menu.



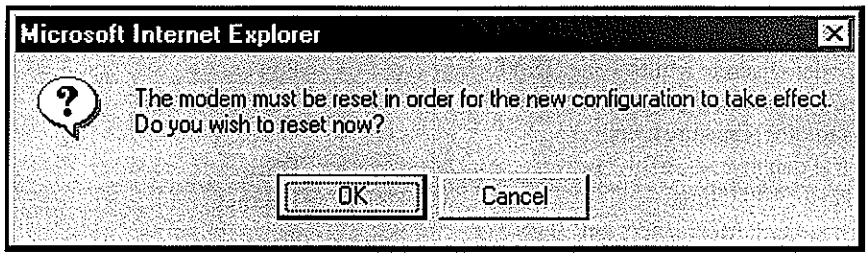
If you selected **DSLATM PORT**, the following pop-up screen will be displayed. Click **OK.**



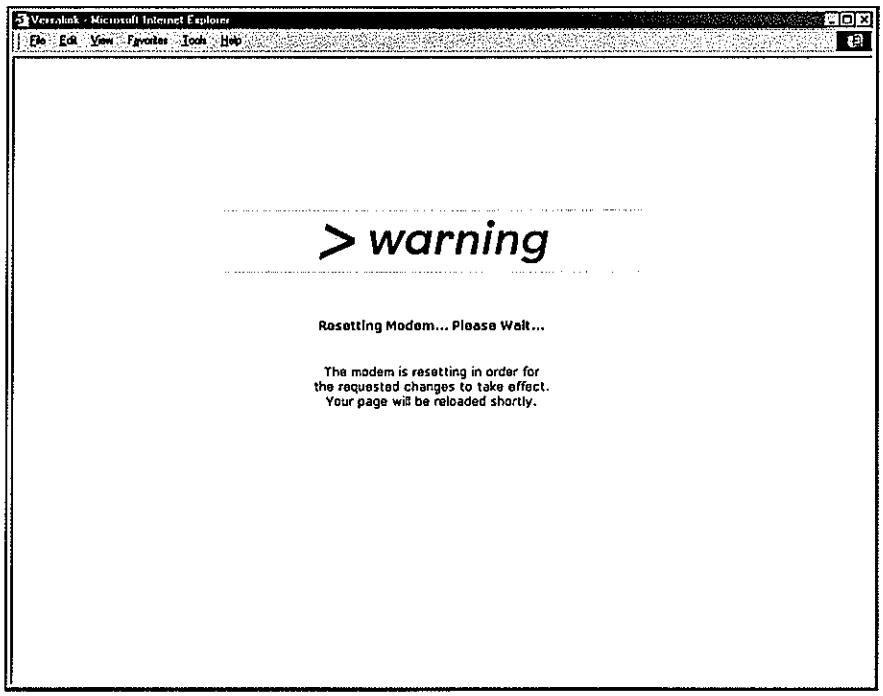
If you clicked **OK** in the pop-up screen, the following pop-up screen will be displayed. Click **OK.**



If you clicked **OK,** the following pop-up screen will be displayed. VersaLink must now be reset to allow the new configuration to take effect. Click on **OK.**



After you click **OK** in the preceding screen, the following screen will be displayed and the modem will be reset. After a brief delay, the **Home Summary** page will be displayed. Confirm that the **DSL** and **Internet Login** fields display **Up.** (Depending on your connection type, you may need to go to the **Easy Login** page and click the connect button to establish a PPP session. After you establish a PPP session, the **Internet Login** field should display Up.)



18. PRODUCT SPECIFICATIONS

DSL

- 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: -40 dBm/Hz
- DSL Impedance: 100 Ohms
- DSL Performance: Performance: per G.992.1, ANSI T1.413.

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 Class PC or above, Macintosh
- Microsoft Windows (98 SE, 2000, ME, NT 4.0, or XP), Linux, or MAC OS X 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
- 10/100 Base-T Network Interface Card (NIC)

System Requirements for Wireless

- Pentium® or equivalent and above class machines
- Microsoft® Windows® (98 ME, 2000, 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/g+ PC adapter

LEDs

- Power
- E1, E2, E3, E4
- Wireless
- DSL
- Internet

Connectors

- DSL/LINE: 6-pin modular jack RJ-11
- Ethernet: 8-pin RJ-45 modular jack
- Power connector: 12V DC
- Wireless IEEE 802.11b/g SMA connector and antenna

Environmental

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

Power Supply/Consumption

- 120 VAC to 12V DC wall-mount power supply
- Less than 4 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

19. 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 SOFTWARE 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 CD 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 CD 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 CD 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 CD appears, you may return the SOFTWARE CD 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.

20. PUBLICATION INFORMATION

Westell® Versa Link™ Gateway (Model 327W)
User Guide Part no. 030-300452 Rev. A

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