Prestige 653HWI Series

ADSL Security Gateway with IEEE802.11g and ISDN Backup

Compact Guide

Version 3.40
October 2003

ZyXEL
Unleash Networking Power

Table of Contents

1 Introducing the Prestige

The Prestige 653 HWI series consists of two models:

- Wireless Ready, with neither wireless card nor external antennas

- Wireless Built-in, complete with internal wireless LAN card and two external antennas

The Prestige is the ideal all-in-one device for small networks connecting to the Internet via ADSL. Key features of the Prestige include firewall, VPN, wireless LAN, NAT, remote management, UPnP and built-in ISDN Backup. See your *User's Guide* for more details on all Prestige features.

You should have an Internet account already set up and have been given most of the following information.

INTERNET ACCOUNT INFORMATION		
Your device's WAN IP Address (if given): _____		
DNS Server IP Address (if given): Primary _____, Secondary _____		
Virtual Path Identifier (**VPI**): _____		
Virtual Channel Identifier (**VCI**): _____		
Multiplexing (VC-based or LLC-based):	☐ **VC**	☐ **LLC**
Encapsulation:		
○ **RFC 1483**		
○ **ENET ENCAP**	Ethernet Encapsulation Gateway IP Address: _____	
○ **PPPoA**	User Name: _____	Password: _____
○ **PPPoE**	Service Name: _____	
	User Name: _____	Password: _____

2 Hardware

2.1 Rear Panel Connections
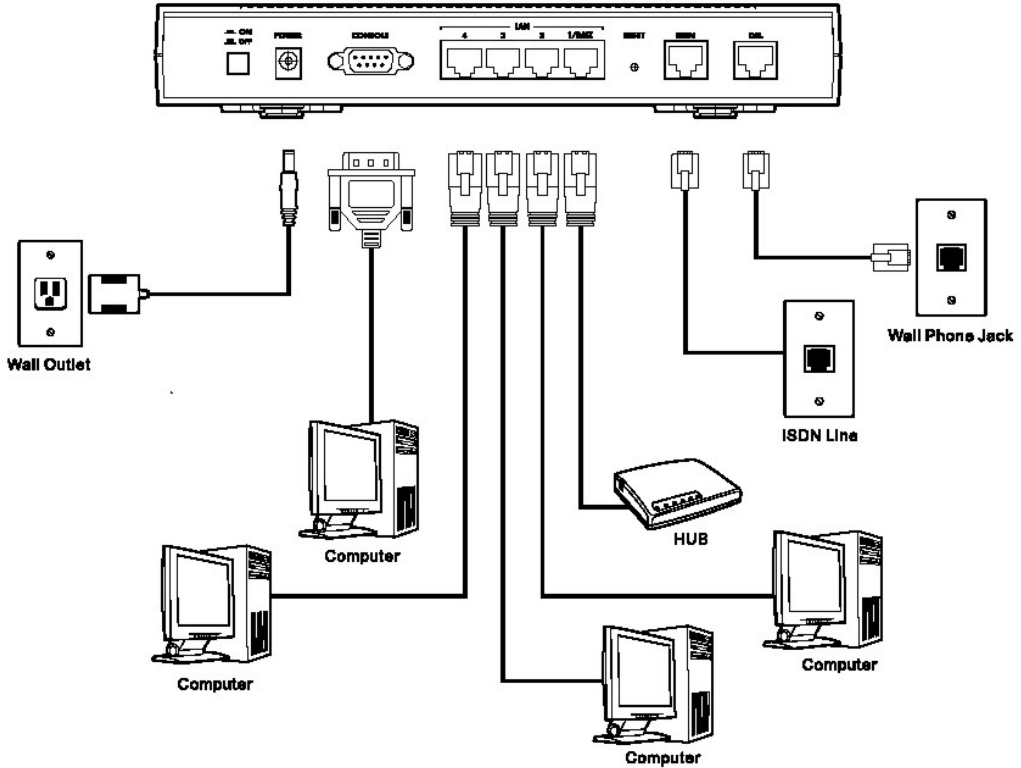
Figure 1 Prestige Hardware Connections

Table 1 Prestige Rear Panel Description

LABEL	DESCRIPTION
DSL	Connect to a telephone jack using the included phone wire.
LAN 1/DMZ-4	Connect to a computer/external hub using an Ethernet cable. Connect the DMZ port to servers that you want visible to the outside world.

Table 1 Prestige Rear Panel Description

LABEL	DESCRIPTION
POWER	Connect to a power source using the power adaptor for your region (see your *User's Guide*). After you've made the connections, connect the power adaptor to a power supply and push in the power button to turn on the Prestige. The **PWR** LED turns on. The **SYS** LED blinks while performing system testing and then turns steady on if the testing is successful. A **LAN** LED turns on if a LAN port is properly connected.
CONSOLE	Only connect this port if you want to configure the Prestige using the SMT via console port; see your *User's Guide* for details. Connect the 9-pin male end of the console cable to the console port of the Prestige and the other end to a serial port (COM1, COM2 or other COM port) on your computer. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 9600 bps port speed.
ISDN	RJ-45 interface for Basic Rate Interface (BRI) based on Euro ISDN standard S/T Interface The ISDN port is used for an auxiliary dial-up WAN connection. The ISDN port can also be used for remote management.
RESET	You only need to use this button if you've forgotten the Prestige's password. It returns the Prestige to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc.; see your *User's Guide* for details).

> **Connecting the DSL, LAN and ISDN cables to the wrong ports can damage your Prestige.**

2.2 Inserting a Card Bus Wireless LAN Card

If your Prestige has built-in wireless capabilities then skip this section. If your Prestige is Wireless Ready, then follow the steps below to install a wireless LAN card.

Step 1. Turn off the Prestige.

> **Never insert or remove a wireless LAN card when the Prestige is turned on.**

Step 2. Locate the slot labeled **Wireless LAN** on the Prestige.

Step 3. With its pin connector facing the slot and the LED side facing upwards, slide the wireless LAN card into the slot.

Figure 2 Prestige Top Panel

Never force, bend or twist the wireless LAN card into the slot.

Step 4.   Turn on the Prestige. The **WLAN** LED should turn on.

2.3 The Top Panel LEDs

Figure 3 Prestige Top Panel

Refer to the following table for LED descriptions.

Table 2 Top Panel LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Prestige is receiving power.
		Off	The Prestige is not receiving power.
SYS	Green	On	The Prestige is functioning properly.
		Blinking	The Prestige is restarting.
		Off	The system is not ready or has malfunctioned.
	Red	On	Power to the Prestige is too low.
LAN 1/DMZ-4	Green	On	The Prestige has a successful 10Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
		Off	The Prestige does not have 10Mb Ethernet connection.
	Orange	On	The Prestige has a successful 100Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
		Off	The Prestige does not have 100Mb Ethernet connection.
WLAN	Green	On	The Wireless link is ready.
		Off	The Wireless link is not ready or has failed.
		Blinking	The Prestige is sending/receiving data through the WLAN.
DSL	Green	On	The Prestige is linked successfully to a DSLAM.
		Blinking	The Prestige is initializing the DSL line.
		Off	The DSL link is down.
ACT	Green	Blinking	The Prestige is sending/receiving data.
ISDN	Green	Blinking	The Prestige is sending/receiving data via ISDN
B1/B2	Green	On	The ISDN B1 or B2 channel is in use
		Off	Both ISDN channels are idle
	Orange	On	The ISDN B1 and B2 channels are in use
		Off	Both ISDN channels are idle

3 Setting Up Your Computer's IP Address

Skip this section if your computer is already set up to accept a dynamic IP address. This is the default for most new computers.

The Prestige is already set up to assign your computer an IP address. Use this section to set up your computer to receive an IP address or assign it a static IP address in the 192.168.1.2 to 192.168.1.254 range with a subnet mask of 255.255.255.0. This is necessary to ensure that your computer can communicate with your Prestige.

Your computer must have an Ethernet card and TCP/IP installed. TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

3.1 Windows 2000/NT/XP

1. In Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

2. In Windows XP, click **Network Connections**.

    In Windows 2000/NT, click **Network and Dial-up Connections**.

3. Right-click **Local Area Connection** and then click **Properties**.

4. Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

5. The **Internet Protocol TCP/IP Properties** screen opens (the **General tab** in Windows XP).

    - To have your computer assigned a dynamic IP address, click **Obtain an IP address automatically**.

    If you know your DNS sever IP address(es), type them in the **Preferred DNS server** and/or **Alternate DNS server** fields.

    -To configure a static IP address, click **Use the following IP Address** and fill in the **IP address** (choose one from192.168.1.2 to 192.168.1.254), **Subnet mask** (255.255.255.0), and **Default gateway** (192.168.1.1) fields.

    Then enter your DNS server IP address(es) in the **Preferred DNS server** and/or **Alternate DNS server** fields.

    If you have more than two DNS servers, click **Advanced**, the **DNS** tab and then configure them using **Add**.
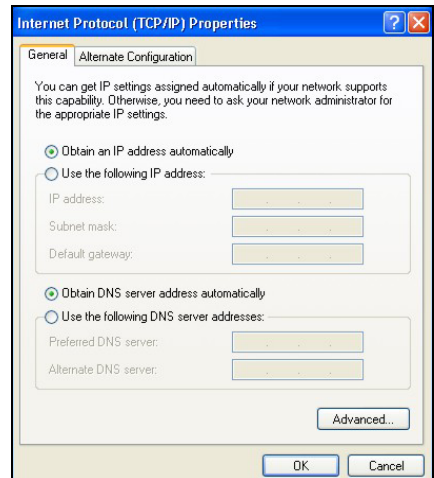
6. Click **Advanced**. Remove any previously installed gateways in the **IP Settin**gs tab and click **OK** to go back to the **Internet Protocol TCP/IP Properties** screen.

7. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8. Click **OK** to close the **Local Area Connection Properties** window.
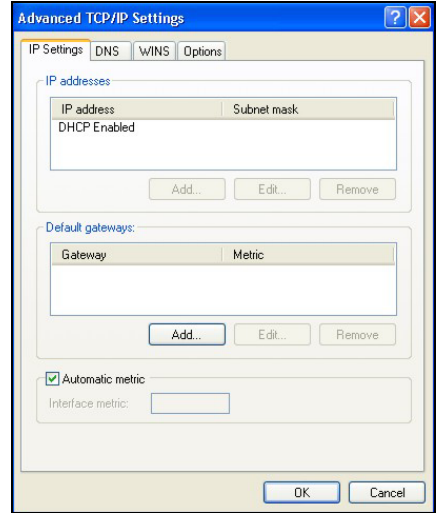
3.2 Checking/Updating Your Computer's IP Address

1. In the computer, click **Start**, (**All) Programs**, **Accessories** and then **Command Prompt**.

2. In the **Command Prompt** window, type "ipconfig" and then press **ENTER** to verify that your computer's IP address is in the correct range (192.168.1.2 to 192.168.1.254) with subnet mask 255.255.255.0. This is necessary in order to communicate with the Prestige.

Refer to your *User's Guide* for detailed IP address configuration for other Windows and Macintosh computer operating systems.

3.3 Testing the Connection to the Prestige

1. Click **Start**, (**All**) **Programs**, **Accessories** and then **Command Prompt**.

2. In the **Command Prompt** window, type "ping" followed by a space and the IP address of the Prestige (192.168.1.1 is the default).

3.   Press **ENTER** and the following screen displays.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms
```

Your computer can now communicate with the Prestige using the **LAN** port.

4 Configuring Your Prestige

This *Compact Guide shows* you how to use the web configurator only. See your *User's Guide* for background information on all Prestige features and SMT (System Management Terminal) configuration.

4.1 Accessing Your Prestige Via Web Configurator

Step 1.   Launch your web browser. Enter "192.168.1.1" as the web site address.

Figure 4 Entering Prestige LAN IP Address in Internet Explorer

Step 2.   An **Enter Network Password** window displays. Enter the user name ("admin" is the default), password ("1234" is the default) and click **OK**.
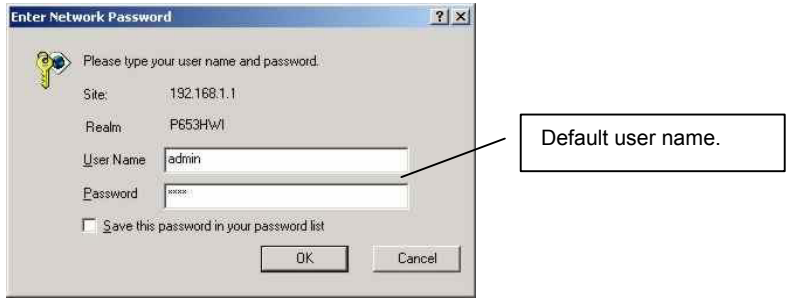
Figure 5 Web Configurator: Password Screen

Step 3. You should now see the web configurator **SITE MAP** screen.

➤ Click **Wizard Setup** to begin a series of screens to configure your Prestige for the first time.

➤ Click a link under **Advanced Setup** to configure advanced Prestige features.

➤ Click a link under **Maintenance** to see Prestige performance statistics, upload firmware and back up, restore or upload a configuration file.

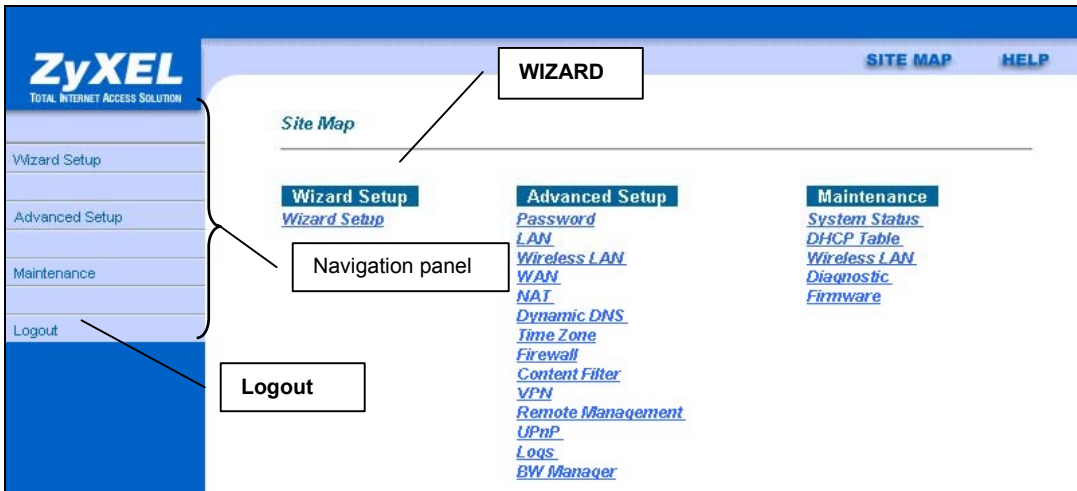➤ Click **Logout** in the navigation panel when you have finished a Prestige management session.

Figure 6 Web Configurator: SITE MAP Screen

The Prestige automatically logs you out if it is left idle for five minutes; press ENTER **to log back in again.**

4.2 Common Screen Command Buttons

The following table shows common command buttons found on many web configurator screens.

Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

4.3 Wizard Internet Access Configuration

Use the Wizard Setup screens to configure your system for Internet access settings and fill in the fields with the information in the *Internet Account Information* table. Your ISP may have already configured some of the fields in the wizard screens for you.

Step 1. In the **SITE MAP** screen click **Wizard Setup** to display the first wizard screen.

Wizard Setup - ISP Parameters for Internet Access

Mode	Routing
Encapsulation	RFC 1483
Multiplex	LLC
Virtual Circuit ID	
VPI	22
VCI	222

Next

From the **Mode** drop-down list box, select **Routing** (default) if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.

Select the encapsulation type your ISP uses from the **Encapsulation** drop-down list box. Choices vary depending on what you select in the **Mode** field.

Select the multiplexing method used by your ISP from the **Multiplex** drop-down list box.

Enter the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers supplied by your ISP in the **VPI** and **VCI** fields. These fields may already be configured.

Click **Next**.

Figure 7 Wizard Screen 1

Step 2. The second wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

If your ISP provides the name of your PPPoE service provider, enter it in the **Service Name** field.

Enter the user name and password *exactly* as your ISP assigned them.

Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the text box below.

Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out period (in seconds) in the **Max. Idle Timeout** field.

Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.

Figure 8 Internet Connection with PPPoE

From the **Network Address Translation** drop-down list box, select **SUA Only**, **Full Feature** or **None**. Refer to the *Network Address Translation* section for more information.

Enter the IP address given by your ISP in the **IP Address** field.

> **The** IP Address **field is not available for bridge mode.**

Refer to *Figure 8* for description of the **Network Address Translation** field.

Figure 9 Internet Connection with RFC 1483

In the **ENET ENCAP Gateway** field, enter the gateway IP address given by your ISP.

Refer to *Figure 8* for other field descriptions.

Figure 10 Internet Connection with ENET ENCAP

Refer to *Figure 8* for field descriptions.

> **The** IP Address **and** Network Address Translation **fields are *not* available for bridge mode.**

Figure 11 Internet Connection with PPPoA

Step 3. Verify the settings in the screen shown next. To change the LAN information on the Prestige, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration and skip to step 5.

Figure 12 Wizard Screen 3

Step 4. If you want to change your Prestige LAN settings, click **Change LAN Configuration** to display the screen as shown next.

Figure 13 Wizard: LAN Configuration

Enter the IP address of your Prestige in dotted decimal notation in the **LAN IP Address** field. For example, 192.168.1.1 (factory default).

> **If you change the Prestige's LAN IP address, you must use the *new* IP address if you want to access the web configurator again.**

Enter a subnet mask in dotted decimal notation in the **LAN Subnet Mask** field.

From the **DHCP Server** drop-down list box, select **On** to allow your Prestige to assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client. Select **Off** to disable DHCP server.

When DHCP server is used, set the following items:

Specify the first of the contiguous addresses in the IP address pool in the **Client IP Pool Starting Address** field.

Specify the size or count of the IP address pool in the **Size of Client IP Pool** field.

Enter the IP address(es) of the DNS server(s) in the **Primary DNS Server** and/or **Secondary DNS Server** fields.

Step 5. The Prestige automatically tests the connection to the computer(s) connected to the LAN ports. To test the connection from the Prestige to the ISP, click **Start Diagnose**. Otherwise click **Return to Main Menu** to go back to the **Site Map** screen.
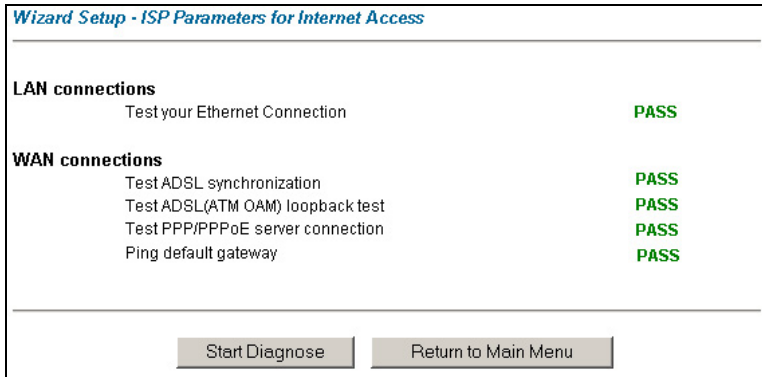

Figure 14 Wizard Screen 4

4.4 Test Your Internet Connection

Launch your web browser and navigate to www.zyxel.com. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the Wizard Setup are correct.

5 Advanced Configuration

This section shows how to configure some of the advanced features of the Prestige.

5.1 Wireless LAN Setup

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (the Internet, email, printer services, etc.) on the wired network without additional expensive network cabling infrastructure. In effect, a wireless LAN environment provides you the freedom to stay connected to the wired network while moving in the coverage area.

The WLAN screens are only available when a WLAN card is installed.

To configure wireless settings, click **Advanced Setup**, **Wireless** and then click **Wireless**.

Figure 15 Wireless LAN: Wireless

The following table describes the fields in this screen.

Table 3 Wireless LAN: Wireless

LABEL	DESCRIPTION
ESSID	(Extended Service Set IDentity) The ESSID is a unique name to identify the Prestige in the wireless LAN. Wireless clients associating to an Access Point (the Prestige) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters).
Hide ESSID	Select **Yes** to hide the ESSID so a wireless client cannot obtain the ESSID through passive scanning. Select **No** to make the ESSID visible so a wireless client can obtain the ESSID through passive scanning.
Channel ID	The range of radio frequencies used by IEEE 802.11g wireless devices is called a channel. Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. Adjacent APs with overlapping coverage areas should use different channels to reduce crosstalk. Crosstalk occurs when the radio signals from access points overlap and interfere with one another degrading performance.

Table 3 Wireless LAN: Wireless

LABEL	DESCRIPTION
RTS/CTS Threshold	Select this option to enable the RTS (Request To Send)/CTS (Clear To Send) threshold to minimize collisions. Enter a value between 0 and 2432. The default is 2432.
	Request To Send is the threshold (number of bytes) for enabling the RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC Service Data Unit) size turns off the RTS/CTS handshake.
Fragmentation Threshold	Fragmentation Threshold is the maximum data fragment size that can be sent.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting them over the wireless network.
	Select **Disable** to allow all wireless computers to communicate with the access points without any data encryption.
	Select **64-bit WEP** or **128-bit WEP** and then configure the keys in the fields provided to activate data encryption.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless clients must use the same WEP key for data transmission.
	If you chose 64-bit WEP, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F").
	Select only one key to be activated at any one time.

The wireless clients and Prestige must use the same ESSID, channel ID and WEP encryption key (if WEP is enabled) for wireless communication.

5.2 Wireless LAN Security Setup

For added security, set your Prestige to check the MAC address of the wireless client device against a list of allowed or denied MAC addresses.

To set up the MAC address list for wireless LAN, click **Advanced Setup** in the navigation panel, **Wireless** and then click the **MAC Filter** link.

Figure 16 Wireless LAN: MAC Address Filter

The following table describes the fields in this screen.

Table 4 Wireless LAN: MAC Address Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.

Table 4 Wireless LAN: MAC Address Filter

LABEL	DESCRIPTION
Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.
MAC Address	Enter the list of MAC addresses in this table.

5.3 Network Address Translation Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

If you have a single public IP address then select **SUA Only** in the **NAT-Mode** screen (see *Figure 17*). If you have multiple public IP addresses then you may use full feature mapping types (see the *User's Guide* for more details).

NAT supports five types of IP/port mapping. They are:

1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.

2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address.

3. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.

4. **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.

5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

5.4 Configuring SUA Server

An SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

Step 1. From the main screen click **Advanced Setup** and then **NAT** to open the **NAT-Mode** screen. Select **SUA Only**.

Figure 17 NAT: Mode

Step 2. Click **Edit Details**.

Figure 18 SUA/NAT Server

The following table describes the fields in this screen.

Table 5 SUA/NAT Server

LABEL	DESCRIPTION
Start Port No.	Type a port number in this field. To forward only one port, type the port number again in the **End Port** field. To forward a series of ports, type the start port number here and the end port number in the **End Port** field.
End Port No.	Type a port number in this field. To forward only one port, type the port number in the **Start Port** field above and then type it again in this field. To forward a series of ports, type the last port number in a series that begins with the port number in the **Start Port** field above.
IP Address	Enter the inside IP address of the server here.

5.5 Firewall Overview

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The Prestige's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Prestige can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The Prestige also has packet-filtering capabilities.

When activated, the firewall allows all traffic to the Internet that originates from the LAN, and blocks all traffic to the LAN that originates from the Internet. In other words the Prestige will:

> **Allow all sessions originating from the LAN to the WAN**
> **Deny all sessions originating from the WAN to the LAN**

LAN-to-WAN rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

The following figure illustrates a Prestige firewall application.
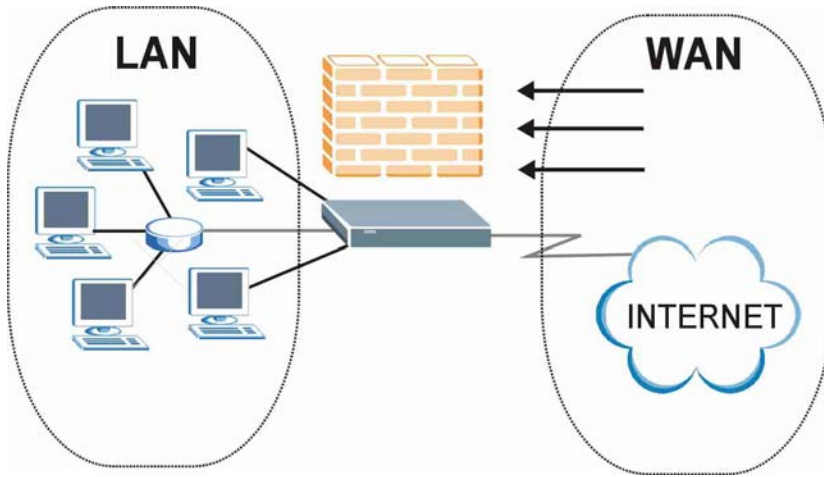
Figure 19 Prestige Firewall Application

5.6 Enabling the Firewall

From the main screen, click **Advanced Setup**, **Firewall** and then **Config** to open the **Configuration** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in the following screen.

Figure 20 Enabling the Firewall

5.7 Procedure for Configuring Firewall Rules

From the main screen, click **Advanced Setup**, **Firewall** and then **Rule Summary** (for either local network to Internet rules or Internet to local network rules) to open the **Summary** screen. The following table describes the fields in this screen.

Table 6 Summary Screen

LABEL	DESCRIPTION
The default action for packets not matching following rules	Should packets that do not match the following rules be blocked or forwarded? Make your choice from the drop down list box. Note that "block" means the firewall silently discards the packet.
Default Permit Log	Click this check box to log all matched rules in the ACL default set.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.	
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules.

Table 6 Summary Screen

LABEL	DESCRIPTION
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to **Any**.
Action	This is the specified action for that rule, either **Block** or **Forward**. Note that **Block** means the firewall silently discards the packet.
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**).
Rules Reorder	You may reorder your rules using this function. Select the rule you want to move. The ordering of your rules is important as rules are applied in turn.
To Rule Number	Select the number you want to move the rule to.
Move	Click **Move** to move the rule.

Follow these directions to create a new rule.

Step 1.   In the **Summary** screen, click a rule's index number. The **Edit Rule** screen opens.

Step 2.   In the **Available Services** text box, select the services you want. Configure customized ports for services not predefined by the Prestige by clicking the **Add** or **Edit** buttons under **Custom Port**. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Step 3.   Configure the **Source Address** and **Destination Address** for the rule.

Figure 21 Creating/Editing A Firewall Rule

The following table describes the fields in this screen.

Table 7 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Source Address	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. Please see the next section for more information on adding and editing source addresses.
Destination Address	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one. Please see the following section on adding and editing destination addresses.
Service Available/ Selected Services	Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.

Table 7 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Edit Available Service	Click this button to go to the list of available custom services.
Action for Matched Packets	Should packets that match this rule be blocked or forwarded? Make your choice from the drop down list box. Note that **Block** means the firewall silently discards the packet.
Log	This field determines if a log is created for packets that match the rule, don't match the rule, both or no log is created.
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.
Delete	Click **Delete** to remove this rule.

5.8 Configuring Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen**.** Either action displays the following screen.

Figure 22 Adding/Editing Source and Destination Addresses

The following table describes the fields in this screen.

Table 8 Adding/Editing Source and Destination Addresses

LABEL	DESCRIPTION
Address Type	Do you want your rule to apply to packets with a particular (single) IP address, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop down list box
Start IP Address	Enter the single IP address or the starting IP address in a range here.

Table 8 Adding/Editing Source and Destination Addresses

LABEL	DESCRIPTION
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.

5.9 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication. The following figure provides an example of a VPN application.
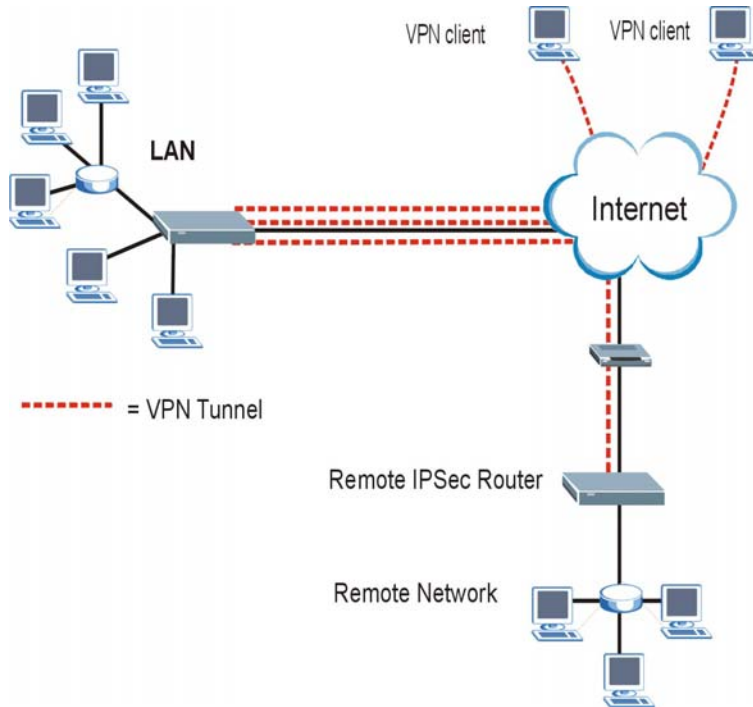
Figure 23 VPN Application

5.10 Summary Screen

Local and remote IP addresses must be static.

From the main screen, click **Advanced Setup**, **VPN**, and **Setup** to open the **Summary** screen. This is a read-only menu of your IPSec rules (tunnels).

Figure 24 VPN Summary

The following table describes the fields in this screen.

Table 9 VPN Summary

LABEL	DESCRIPTION
No.	The VPN policy index number
Name	This field displays the identification name for this VPN policy.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Local Address	This is the IP address(es) of computer(s) on your local network behind your Prestige. The same (static) IP address is displayed twice when the **Local Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Single Address**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Range Address**. A (static) IP address and a subnet mask are displayed when the **Local Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Subnet Address**.

Table 9 VPN Summary

LABEL	DESCRIPTION
Remote Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays **N/A** when the **Secure Gateway IP Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the **Remote Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Single Address**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Range Address**. A (static) IP address and a subnet mask are displayed when the **Remote Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Subnet Address**.
Encap	This field displays **Tunnel** or **Transport** mode (Tunnel is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase Prestige processing requirements and communications latency (delay).
Secure Gateway IP	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway IP Address** field in the **Configure-IKE** screen to **0.0.0.0.**

5.11 Configuring VPN Policies

Click an IPSec rule's index number to open the **VPN IKE** screen where you can configure the IPSec rule.

Figure 25 VPN IKE

The following table describes the fields in this screen.

Table 10 VPN IKE

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select this check box to have the Prestige automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the Prestige drops trailing spaces.
IPSec Key Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting.
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** for a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your Prestige. When the **Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the **Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your Prestige.
End/ Subnet Mask	When the **Address Type** field is configured to **Single**, this field is N/A. When the **Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind your Prestige.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** with a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.

Table 10 VPN IKE

LABEL	DESCRIPTION
IP Address Start	When the **Address Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the **Address Type** field is configured to **Single**, this field is N/A. When the **Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Local ID Type	Select **IP** to identify this Prestige by its IP address. Select **DNS** to identify this Prestige by a domain name. Select **E-mail** to identify this Prestige by an e-mail address.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer or leave the field blank to have the Prestige automatically use its own IP address. When you select **DNS** in the **Local ID Type** field, type a domain name (up to 31 characters) by which to identify this Prestige. When you select **E-mail** in the **Local ID Type** field, type an e-mail address (up to 31 characters) by which to identify this Prestige. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.
My IP Address	Enter the WAN IP address of your Prestige. The Prestige uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. The VPN tunnel has to be rebuilt if this IP address changes.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.

Table 10 VPN IKE

LABEL	DESCRIPTION
Content	When you select **IP** in the **Peer ID Type** field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the **Secure Gateway IP Address** field. When you select **DNS** in the **Peer ID Type** field, type a domain name (up to 31 characters) by which to identify the remote IPSec router. When you select **E-mail** in the **Peer ID Type** field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway IP Address** field below.
Secure Gateway IP Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**).
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
VPN Protocol	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below). Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described below).
Pre-shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Multiple SAs connecting through a secure gateway must have the same pre-shared key.
VPN Setup	Select **DES**, **3DES** or **NULL** from the drop-down list box. When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.

Table 10 VPN IKE

LABEL	DESCRIPTION
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Advanced	Click **Advanced** to configure more detailed settings of your IKE key management.
Delete	Click **Delete** to remove this rule.

5.12 Viewing SA Monitor

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only.

From the main screen, click **Advanced Setup**, and **Monitor** to view Security Associations.

> **When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires.**

5.13 UPnP Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

Windows ME and Windows XP support UPnP. See the Microsoft website for information about other Microsoft operating systems.

> **Make sure you apply Microsoft's UPnP security patch before enabling the UPnP feature. Refer to the Microsoft website.**

5.14 Configuring UPnP

Click **Advanced Setup** and then **UPnP** to open the **UPnP** screen.

UPNP

☐ Enable the Universal Plug and Play(UPnP) Service
☐ Allow users to make configuration changes through UPnP
☐ Allow UPnP to pass through Firewall

Apply   Cancel

Figure 26 UPnP

The following table describes the fields in this screen.

Table 11 UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Prestige's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the Prestige so that they can communicate through the Prestige, for example by using NAT Traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).

6 Troubleshooting

Table 12 Troubleshooting

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the Prestige.	Make sure that you have the correct power adapter connected to the Prestige and an appropriate power source. Check all cable connections. If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.
Cannot access the Prestige from the LAN.	Check the cable connection between the Prestige and your computer or hub. Refer to the *Rear Panel Connections* section for details. Ping the Prestige from a LAN computer. Make sure your computer's Ethernet adapter is installed and functioning properly.
Cannot ping any computer on the LAN.	If the LAN LEDs are all off, check the cable connections between the Prestige and your LAN computers. Verify that the IP address, subnet mask of the Prestige and the LAN computers are in the same IP address range.
Cannot ping any computer on the WLAN	Make sure the wireless card is properly inserted in the Prestige and the **WLAN** LED is on. Make sure the wireless card on the wireless client is working properly. Check that both the Prestige and wireless client(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).
Cannot get a WAN IP address from the ISP.	Check your **Encapsulation**, **Multiplex** and **VPI/VCI** settings (refer to section *4.3*). You need a user name and password if you're using PPPoE or PPPoA encapsulation. Make sure that you have entered the correct **Service Name** (PPPoE encapsulation only), **User Name** and **Password** (the username and password are case sensitive). Refer to section *4.3* for more information.
Cannot access the Internet.	Verify the Internet connection settings in the **DSL Setup** screen. Make sure you entered the correct user name and password. For wireless clients, check that both the Prestige and wireless client(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).