

Prestige 660HW Series

ADSL 2+ 4-Port Gateway with 802.11g Wireless

Prestige 660H Series

ADSL 2+ 4-Port Gateway

Quick Start Guide

Version 3.40

01/2005



Table of Contents

| | |
|---|-----------|
| Introducing the Prestige | 3 |
| 1 Hardware Connections | 4 |
| 1.1 Front Panel LEDs | 5 |
| 2 Zero Configuration Internet Access | 7 |
| 3 Setting Up Your Computer's IP Address..... | 8 |
| 3.1 Windows 95/98/Me | 8 |
| 3.2 Windows 2000/NT/XP | 10 |
| 3.3 Verifying Your Computer's IP Address..... | 12 |
| 3.4 Testing the Connection to the Prestige..... | 12 |
| 4 Configuring Your Prestige | 13 |
| 4.1 Accessing Your Prestige Via Web Configurator..... | 13 |
| 4.2 Common Screen Command Buttons | 15 |
| 4.3 Internet Access Wizard | 15 |
| 4.4 Test Your Internet Connection | 21 |
| 5 Advanced Configuration..... | 22 |
| 5.1 Wireless LAN Setup (P660HW only) | 22 |
| 5.2 Wireless LAN Security Setup | 24 |
| 5.3 802.1x and WPA Overview | 26 |
| 5.4 OTIST | 26 |
| 5.5 Network Address Translation Overview | 28 |
| 5.6 Configuring SUA Server | 28 |
| 5.7 Firewall Overview..... | 30 |
| 5.8 Enabling the Firewall | 31 |
| 5.9 Procedure for Configuring Firewall Rules | 32 |
| 6 Troubleshooting..... | 38 |

Introducing the Prestige

The Prestige 660H (P660H) and Prestige 660HW (P660HW) are ADSL 2/2+ Gateways ideal for small networks connecting to the Internet via ADSL. Key features include NAT, Firewall, WPA (Wi-Fi Protected Access) and 802.1x wireless LAN security (P660HW only). See your *User's Guide* for more details on all Prestige features.

Wireless features in this guide relate to the P660HW only.

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): <input type="checkbox"/> VC <input type="checkbox"/> LLC | |
| Encapsulation: (choose one below) | |
| <input type="radio"/> RFC 1483 | |
| <input type="radio"/> ENET ENCAP | Ethernet Encapsulation Gateway IP Address: _____ |
| <input type="radio"/> PPPoA | User Name: _____ Password: _____ |
| <input type="radio"/> PPPoE | Service Name: _____ User Name: _____ Password: _____ |

Certifications

1. Go to www.zyxel.com
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

1 Hardware Connections

Both rear panels are the same except the P660HW has an antenna.

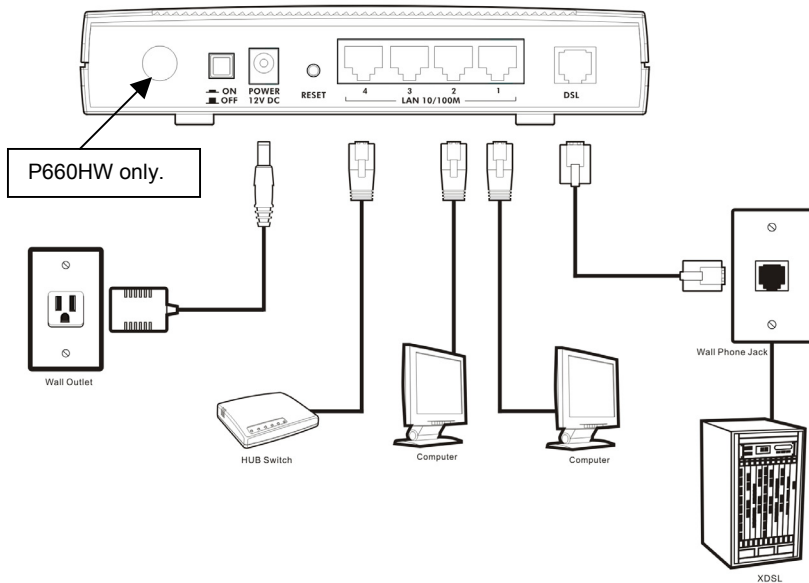


Figure 1 P660HW Hardware Connections

Table 1 Prestige Rear Panel Description

| LABEL | DESCRIPTION |
|----------------|--|
| DSL | Connect to a telephone jack using the included phone wire. |
| LAN 1 to LAN 4 | Connect to a computer/external hub using an Ethernet cable. |
| POWER | Connect to a power source using the power adaptor for your region (see your <i>User's Guide</i>). |

Table 1 Prestige Rear Panel Description

| LABEL | DESCRIPTION |
|-------|--|
| | <p>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.</p> <p>The PWR/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.</p> |
| RESET | <p>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 <i>User's Guide</i> for details).</p> |

1.1 Front Panel LEDs

Both front panel LEDs are the same except the P660HW has an additional WLAN LED.



Figure 2 P660HW Front Panel



Figure 3 P660H Front Panel

Refer to the following table for more detailed LED descriptions.

Table 2 P660HW Front Panel LED Description

| LED | COLOR | STATUS | DESCRIPTION |
|-----------------------|-------|---------------|--|
| PWR/SYS | Green | On | The Prestige is receiving power and functioning properly. |
| | | Blinking | The Prestige is rebooting. |
| | Red | On | Power to the Prestige is too low. |
| | | Off | The system is not ready or has malfunctioned. |
| LAN 1 to LAN 4 | Green | On | The Prestige has a successful 10Mb Ethernet connection. |
| | | Blinking | The Prestige is sending/receiving data. |
| | Amber | On | The Prestige has a successful 100Mb Ethernet connection. |
| | | Blinking | The Prestige is sending/receiving data. |
| | | Off | The LAN is not connected. |
| WLAN (P660HW only) | Green | On | The Prestige is ready, but is not sending/receiving data through the wireless LAN. |
| | | Blinking | The Prestige is sending/receiving data through the wireless LAN. |
| | | Off | The wireless LAN is not ready or has failed. |
| DSL/PPP | Green | Fast Blinking | The Prestige is sending/receiving non-PPP data. |
| | | Slow Blinking | The Prestige is initializing the DSL line. |
| | | On | The system is ready, but is not sending/receiving non-PPP data. |
| | Amber | On | The connection to the PPPoE server is up. |
| | | Blinking | The Prestige is sending/receiving PPP data. |
| | | Off | The DSL link is down. |

2 Zero Configuration Internet Access

Any computer connected to the Prestige can access the Internet without changing its network settings (such as the IP address and subnet mask).

1. Make the hardware connections and turn on the Prestige (refer to the Hardware Connections section for your model).
2. Wait until the **DSL/ACT** LED turns steady on. Launch your web browser and navigate to a web site (for example, www.zyxel.com). The Prestige automatically detects and configures your Internet connection. This may take about two minutes.
3. If you have a PPPoE or PPPoA connection type, a screen displays prompting you to enter your Internet account username and/or password. Enter the username, password and/or service name exactly as provided by your ISP. Click **Apply**.

Your PPPoE login username and password are wrong.

Enter the system password and username and password exactly as your ISP assigned them.

System Password

User Name

Password

4. You should be able to access the Internet. Otherwise, follow the on-screen instructions to solve the problem(s). Refer to the rest of this guide or the *User's Guide* to manually configure your Prestige for Internet connection and other advanced settings.

If an Internet access parameter changes, either change it manually or restart the device to have the Prestige automatically reconfigure your Internet connection.

3 Setting Up Your Computer's IP Address

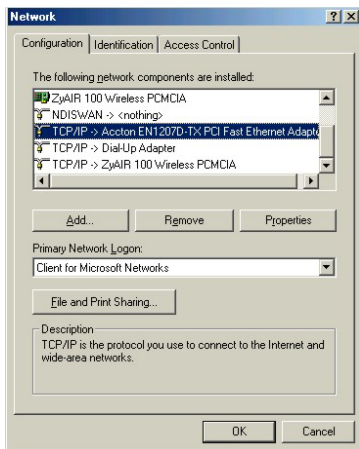
Skip this section if your computer is already set up to accept a dynamic IP address. This is the default for most new computers.

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 95/98/Me

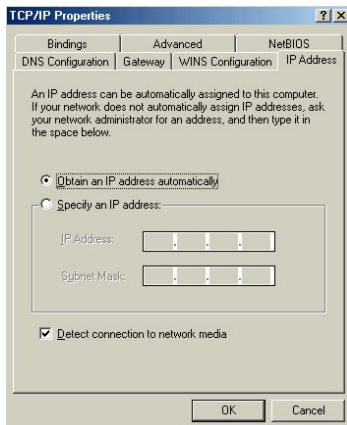
1. Click **Start, Settings, Control Panel** and double-click the **Network** icon to open the **Network** window.
2. The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.
3. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.



4. Click the **IP Address** tab.

-If your IP address is dynamic, select **Obtain an IP address automatically**.

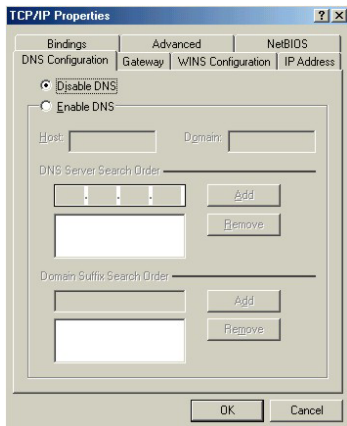
-If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



5. Click the **DNS Configuration** tab.

-If you do not know your DNS information, select **Disable DNS**.

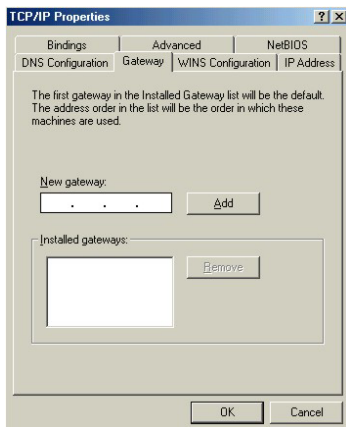
-If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



6. Click the **Gateway** tab.

-If you do not know your gateway's IP address, remove previously installed gateways.

-If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



7. Click **OK** to save and close the **TCP/IP Properties** window.
8. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
9. Turn on your Prestige and restart your computer when prompted.

Verifying Your Computer's IP Address

1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

3.2 Windows 2000/NT/XP

1. In Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.
2. In the Windows XP control panel, double-click **Network Connections**.
In the Windows 2000/NT control panel, double-click **Network and Dial-up Connections**.
3. In the network connections screen, 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 from 192.168.1.2 to 192.168.1.254), **Subnet mask** (255.255.255.0), and **Default gateway** (192.168.1.1) fields.

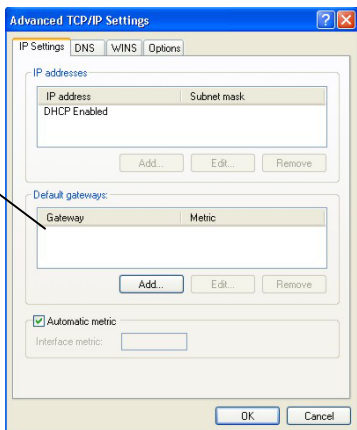
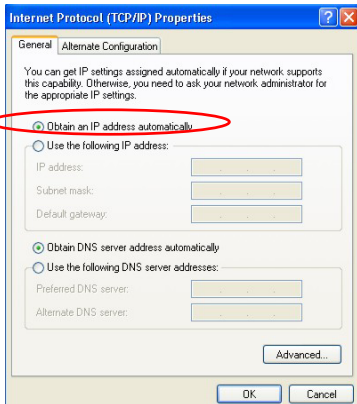
Then enter your DNS server IP address(es) in the **Preferred DNS server** and/or **Alternate DNS server** fields.

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 Settings** tab and click **OK** to go back to the **Internet Protocol TCP/IP Properties** screen.

Remove all previously installed gateways (if any).

7. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
8. Click **OK** (in Windows 2000/NT) or **Close** (in Windows XP) to close the **Local Area Connection Properties** window.



3.3 Verifying Your Computer's IP Address

1. In the computer desktop, 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 Macintosh computer operating systems.

3.4 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).

```
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
```

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

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

4 Configuring Your Prestige

This 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

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

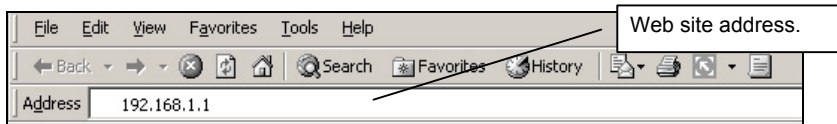


Figure 4 Entering Prestige LAN IP Address in Internet Explorer

2. An **Enter Network Password** window displays. Enter the password ("1234" is the default) and click **Login**.



Figure 5 Web Configurator: Password Screen

You should change the default password in the next screen. If you change it, you will not see the next screen the next time you log in.

Use this screen to change the password.

We recommend that you personalize the system administrator password by changing it to something besides the default '1234'.

The administrator password should must be between 1 - 30 characters.

New Password:

Retype to Confirm:

Figure 6 Change Password

- 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.

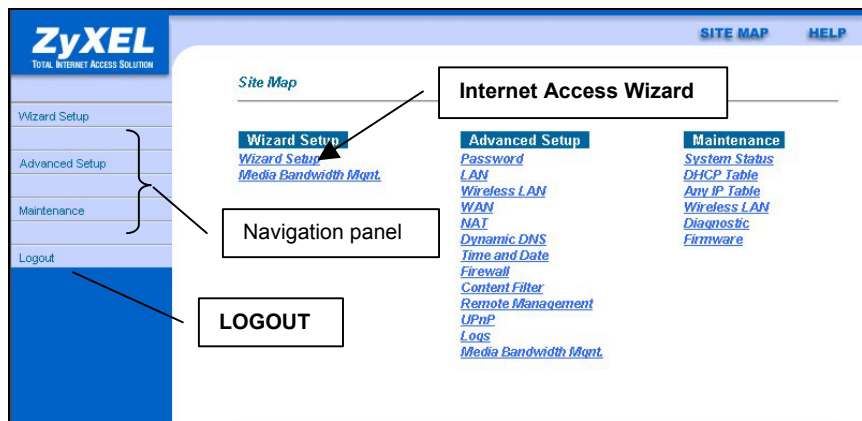


Figure 7 Web Configurator: Site Map Screen

The Prestige automatically times out after five minutes of inactivity. Simply log back into the Prestige if this happens to you.

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. |
| Reset/Cancel | Click Reset or Cancel to begin configuring this screen afresh. |

4.3 Internet Access Wizard

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.

1. In the **Site Map** screen click **Wizard Setup** to display the first wizard screen.

Wizard Setup - ISP Parameters for Internet Access

| | |
|---------------------------|--------------------------------------|
| Mode | <input type="text" value="Routing"/> |
| Encapsulation | <input type="text" value="PPPoA"/> |
| Multiplex | <input type="text" value="LLC"/> |
| Virtual Circuit ID | |
| VPI | <input type="text" value="8"/> |
| VCI | <input type="text" value="35"/> |

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 8 Wizard Screen 1

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.

Wizard Setup - ISP Parameters for Internet Access

Service Name

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout Secs

Nailed-Up Connection

Network Address Translation

Figure 9 Internet Connection with PPPoE

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

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.

Wizard Setup - ISP Parameters for Internet Access

IP Address

Network Address Translation

Figure 10 Internet Connection with RFC 1483

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.

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 9* for description of the **Network Address Translation** field.

Wizard Setup - ISP Parameters for Internet Access

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Subnet Mask

ENET ENCAP Gateway

Network Address Translation

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

Refer to *Figure 9* for other field descriptions.

Figure 11 Internet Connection with ENET ENCAP

Wizard Setup - ISP Parameters for Internet Access

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout Secs

Nailed-Up Connection

Network Address Translation

Refer to *Figure 9* for field descriptions.

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

Figure 12 Internet Connection with PPPoA

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 the following step.

Wizard Setup - ISP Parameters for Internet Access

WAN Information:
Mode: **Routing**
Encapsulation: **PPPoE**
Multiplexing: **LLC**
VPI/VCI: **8/35**
Service Name:
User Name: **user@isp.ch**
Password: *********
IP Address: **Obtain an IP Address Automatically**
NAT: **SUA Only**
Connect on Demand: **Max Idle Timeout 1500 Secs.**

LAN Information:
IP Address: **192.168.1.1**
IP Mask: **255.255.255.0**
DHCP: **ON**
Client IP Pool Starting Address: **192.168.1.33**
Size of Client IP Pool: **32**

Figure 13 Wizard Screen 3

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

Wizard Setup - ISP Parameters for Internet Access

LAN IP Address

LAN Subnet Mask

DHCP

DHCP Server

Client IP Pool Starting Address

Size of Client IP Pool

Primary DNS Server

Secondary DNS Server

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.

Figure 14 Wizard: LAN Configuration

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.

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.

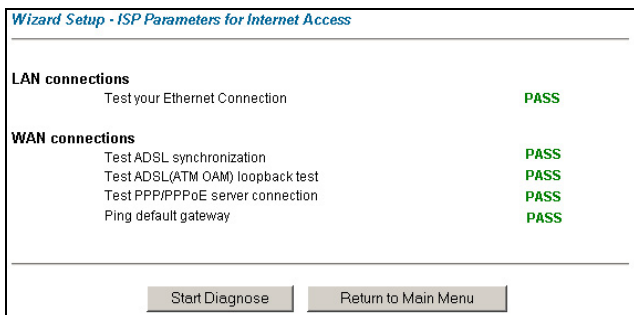


Figure 15 Wizard Screen 4

4.4 Test Your Internet Connection

Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the *User's Guide* for more detailed information on the complete range of Prestige features. 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 (P660HW only)

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 LAN** and then click **Wireless**.

Wireless LAN- Wireless

Enable Wireless LAN
 Enable 802.11g+

ESSID

Hide ESSID

Channel ID

RTS/CTS Threshold (0 ~ 2432)

Fragmentation Threshold (256 ~ 2432)

Passphrase

WEP Encryption

64-bit WEP: Enter 5 characters or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).
256-bit WEP: Enter 29 characters or 58 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).

Key1
 Key2
 Key3
 Key4

Figure 16 Wireless LAN: Wireless

The following table describes the fields in this screen.

Table 3 Wireless LAN: Wireless

| LABEL | DESCRIPTION |
|-------------------------|---|
| Enable Wireless LAN | The wireless LAN is turned off by default, before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN. |
| Enable 802.11g+ | Select this check box to allow the Prestige to communicate with any ZyXEL WLAN devices (that support this feature) at a higher transmission rate than the IEEE 802.11g standard. |
| 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 radio frequency used by IEEE 802.11b wireless devices is called a channel. Select a channel from the drop-down list box. |
| 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. This field is not configurable when you select Enable 802.11g+ . 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. This field is not configurable when you select Enable 802.11g+ . |
| Passphrase | Enter a "passphrase" (password phrase) of up to 63 case-sensitive printable characters and click Generate to have the Prestige create four different WEP keys. |

Table 3 Wireless LAN: Wireless

| LABEL | DESCRIPTION |
|----------------|---|
| Generate | After you enter the passphrase, click Generate to have the Prestige generate four different WEP keys automatically. |
| WEP Encryption | <p>WEP (Wired Equivalent Privacy) encrypts data frames before transmitting them over the wireless network.</p> <p>Select Disable allows all wireless computers to communicate with the access points without any data encryption.</p> <p>Select 64-bit WEP, 128-bit WEP or 256-bit WEP and then configure the keys in the fields provided to activate data encryption.</p> |
| Key 1 to Key 4 | <p>The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission.</p> <p>If you want to manually set the WEP keys, enter the key in the field provided.</p> <p>If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 256-bit WEP, then enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be used at any one time. The default key is key 1.</p> |

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 LAN** and then click the **MAC Filter** link.

Wireless LAN- MAC Filter

Active

Action

| MAC Address | |
|-------------|--|
| 1 | <input type="text" value="00:00:00:00:00:00"/> |
| 3 | <input type="text" value="00:00:00:00:00:00"/> |
| 5 | <input type="text" value="00:00:00:00:00:00"/> |
| 7 | <input type="text" value="00:00:00:00:00:00"/> |
| 9 | <input type="text" value="00:00:00:00:00:00"/> |
| 11 | <input type="text" value="00:00:00:00:00:00"/> |
| 13 | <input type="text" value="00:00:00:00:00:00"/> |
| 15 | <input type="text" value="00:00:00:00:00:00"/> |
| 17 | <input type="text" value="00:00:00:00:00:00"/> |
| 19 | <input type="text" value="00:00:00:00:00:00"/> |
| 21 | <input type="text" value="00:00:00:00:00:00"/> |
| 23 | <input type="text" value="00:00:00:00:00:00"/> |
| 25 | <input type="text" value="00:00:00:00:00:00"/> |
| 27 | <input type="text" value="00:00:00:00:00:00"/> |
| 29 | <input type="text" value="00:00:00:00:00:00"/> |
| 31 | <input type="text" value="00:00:00:00:00:00"/> |
| 2 | <input type="text" value="00:00:00:00:00:00"/> |
| 4 | <input type="text" value="00:00:00:00:00:00"/> |
| 6 | <input type="text" value="00:00:00:00:00:00"/> |
| 8 | <input type="text" value="00:00:00:00:00:00"/> |
| 10 | <input type="text" value="00:00:00:00:00:00"/> |
| 12 | <input type="text" value="00:00:00:00:00:00"/> |
| 14 | <input type="text" value="00:00:00:00:00:00"/> |
| 16 | <input type="text" value="00:00:00:00:00:00"/> |
| 18 | <input type="text" value="00:00:00:00:00:00"/> |
| 20 | <input type="text" value="00:00:00:00:00:00"/> |
| 22 | <input type="text" value="00:00:00:00:00:00"/> |
| 24 | <input type="text" value="00:00:00:00:00:00"/> |
| 26 | <input type="text" value="00:00:00:00:00:00"/> |
| 28 | <input type="text" value="00:00:00:00:00:00"/> |
| 30 | <input type="text" value="00:00:00:00:00:00"/> |
| 32 | <input type="text" value="00:00:00:00:00:00"/> |

Figure 17 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 MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the Prestige in these address fields. |

5.3 802.1x and WPA Overview

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption. WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can't use the Prestige's local user database for WPA authentication purposes since the local user database uses MD5 EAP which cannot be used to generate keys.

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

To change your Prestige's authentication settings, click the **Wireless LAN** link under **Advanced Setup** and then the **802.1x/WPA** tab. The screen varies by the wireless port control and key management protocol you select.

5.4 OTIST

OTIST (One-Touch Intelligent Security Technology) allows your Prestige to set the wireless client to use the same wireless settings as the Prestige.

The wireless client must also support OTIST and have OTIST enabled.

The following are the wireless settings that the Prestige assigns to the wireless client if OTIST is enabled on both devices and the OTIST setup keys are the same.

- SSID
- Security (WEP or WPA-PSK)

This will replace the pre-configured wireless settings on the wireless clients.

Figure 18 Wireless LAN: OTIST

The following table describes the fields in this screen.

Table 5 Wireless LAN: OTIST

| LABEL | DESCRIPTION |
|-------|--|
| Key | Enter the setup key from zero to eight ASCII characters. The default OTIST setup key is "01234567". If you change the OTIST setup key here, you must also make the same change on the wireless client(s). |
| Yes! | If the Prestige has no wireless security configured, select this checkbox to enable WPA-PSK security and automatically generate a WPA-PSK key on the Prestige. The WPA-PSK security settings can then be assigned to the wireless client when you start OTIST. |

5.5 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 19*). 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.

5.6 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.

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

NAT - Mode

Network Address Translation

None
 SUA Only [Edit Details](#)
 Full Feature [Edit Details](#)

Figure 19 NAT: Mode

2. Click Edit Details.

NAT - Edit SUA/NAT Server Set

| | Start Port No. | End Port No. | IP Address |
|----|----------------|--------------|------------|
| 1 | All ports | All ports | 0.0.0.0 |
| 2 | 0 | 0 | 0.0.0.0 |
| 3 | 0 | 0 | 0.0.0.0 |
| 4 | 0 | 0 | 0.0.0.0 |
| 5 | 0 | 0 | 0.0.0.0 |
| 6 | 0 | 0 | 0.0.0.0 |
| 7 | 0 | 0 | 0.0.0.0 |
| 8 | 0 | 0 | 0.0.0.0 |
| 9 | 0 | 0 | 0.0.0.0 |
| 10 | 0 | 0 | 0.0.0.0 |
| 11 | 0 | 0 | 0.0.0.0 |
| 12 | 0 | 0 | 0.0.0.0 |

Figure 20 SUA/NAT Server

The following table describes the labels in this screen.

Table 6 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. |

5.7 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.

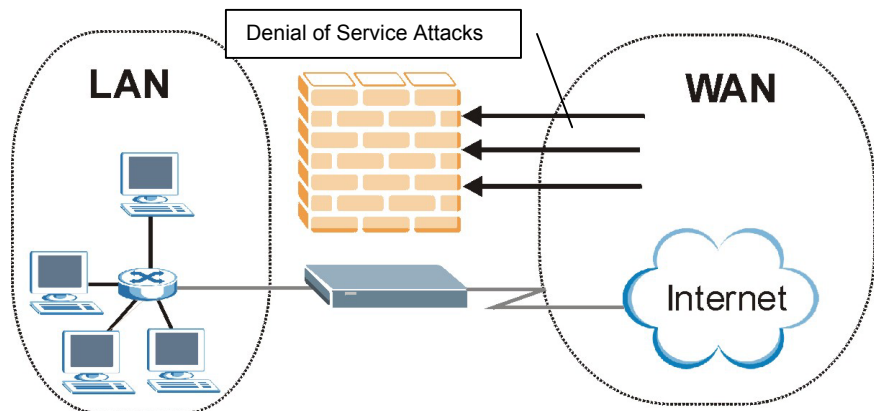


Figure 21 Prestige Firewall Application

5.8 Enabling the Firewall

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

Firewall - Default Policy

Enable Firewall

Allow Asymmetrical Route

CAUTION: When Allow Asymmetrical Route is checked, all LAN to LAN and WAN to WAN packets will bypass the Firewall check.

| Packet Direction | Default Action | Log |
|---------------------|--|-------------------------------------|
| LAN to LAN / Router | <input type="radio"/> Block <input checked="" type="radio"/> Forward | <input type="checkbox"/> |
| LAN to WAN | <input type="radio"/> Block <input checked="" type="radio"/> Forward | <input checked="" type="checkbox"/> |
| WAN to LAN | <input checked="" type="radio"/> Block <input type="radio"/> Forward | <input checked="" type="checkbox"/> |
| WAN to WAN / Router | <input checked="" type="radio"/> Block <input type="radio"/> Forward | <input checked="" type="checkbox"/> |

Back Apply Cancel

Figure 22 Enabling the Firewall

Table 7 Firewall: Default Policy

| LABEL | DESCRIPTION |
|--------------------------|---|
| Firewall Enabled | Select this check box to activate the firewall. The Prestige performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. |
| Allow Asymmetrical Route | Select this check box to have the Prestige firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology. |
| Packet Direction | This is the direction of travel of packets. Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, LAN to LAN/Router means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the Prestige or the Prestige itself. |
| Default Action | Use the radio buttons to select whether to Block (silently discard) or Forward (allow the passage of) packets that are traveling in the selected direction. |
| Log | Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below. |
| 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. |

5.9 Procedure for Configuring Firewall Rules

The ordering of your rules is very important as rules are applied in turn.

Click on **Firewall**, then **Rule Summary** to bring up the following screen. This screen is a summary of the existing rules. Note the order in which the rules are listed.

Firewall - Rule Summary

Firewall Rules Storage Space in Use (1%)

0% 100%

Packet Direction:

Default Policy: Forward, None Log

Create Rule: Insert new rule before rule number

Rules Reorder: Move rule number to rule number

Figure 23 Rule Summary

The following table describes the labels in this screen.

Table 8 Firewall: Rule Summary

| LABEL | DESCRIPTION |
|---|--|
| Firewall Rules Storage Space in Use | This read-only bar shows how much of the Prestige's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. |
| Packet Direction | Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules. |
| Default Policy | This field displays the default action and log policy you selected in the Default Rule screen for the packet direction shown in the field above. |
| 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. | |
| Rule | This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click a rule's number to go to the Firewall Edit Rule screen to configure or edit a firewall rule. |

Table 8 Firewall: Rule Summary

| LABEL | DESCRIPTION |
|----------------|--|
| Active | This field displays whether a firewall is turned on (Y) or not (N). |
| 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 . See <i>User's Guide</i> for more information. |
| Action | This is the specified action for that rule, either Block or Forward . Note that Block means the firewall silently discards the packet. |
| Schedule | This field tells you whether a schedule is specified (Yes) or not (No). |
| Log | This field shows you whether a log is created when packets match this rule (Enabled) or not (Disable). |
| Alert | This field tells you whether this rule generates an alert (Yes) or not (No) when the rule is matched. |
| Insert/Append | <p>Type the index number for where you want to put a rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.</p> <p>Click Insert to add a new firewall rule before the specified index number.</p> <p>Click Append to add a new firewall rule after the specified index number.</p> |
| Move | Type a rule's index number and the number for where you want to put that rule. Click Move to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering. |
| 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. |

Follow these directions to create a new rule.

1. In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
2. Click **Insert** to display this screen and refer to the following table for information on the labels.

Firewall - Edit Rule 1

Active

Action for Matched Packets: Block Forward

Source Address:

Address Type: Source Address List

Start IP Address: Add >>

End IP Address: Edit <<

Subnet Mask: Delete

Destination Address:

Address Type: Destination Address List

Start IP Address: Add >>

End IP Address: Edit <<

Subnet Mask: Delete

Service:

Available Services:

Selected Services

AIM/NEW-ICQ(TCP:5190) Add >>

AUTH(TCP:113)

BGP(TCP:179)

BOOTP_CLIENT(UDP:68) Remove

BOOTP_SERVER(UDP:67)

[Edit Customized Services](#)

Schedule:

Day to Apply:

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Apply : (24-Hour Format)

All day

Start hour minute End hour minute

Log:

Log Packet Detail Information.

Alert:

Send Alert Message to Administrator When Matched.

Back Apply Cancel Delete

Figure 24 Creating/Editing A Firewall Rule

The following table describes the labels in this screen.

Table 9 Firewall: Edit Rule

| LABEL | DESCRIPTION |
|------------------------------|---|
| Active | Select this option to enable this firewall rule. |
| Action for Matched Packet | Use the radio button to select whether to discard (Block) or allow the passage of (Forward) packets that match this rule. |
| Source/Destination Address | |
| Address Type | Do you want your rule to apply to packets with a particular (single) IP, 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 that includes: Single Address , Range Address , Subnet Address and Any Address . |
| Start IP Address | Enter the single IP address or the starting IP address in a range here. |
| End IP Address | Enter the ending IP address in a range here. |
| Subnet Mask | Enter the subnet mask here, if applicable. |
| Add | Click Add to add a new address to the Source or Destination Address box. You can add multiple addresses, ranges of addresses, and/or subnets. |
| Edit | To edit an existing source or destination address, select it from the box and click Edit . |
| Delete | Highlight an existing source or destination address from the Source or Destination Address box above and click Delete to remove it. |
| Services | |
| Available/ Selected Services | Please see <i>User's Guide</i> for more information on services available. Highlight a service from the Available Services box on the left, then click Add>> 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 Remove . |
| Available Service | Click the Available Services link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services. |

Table 9 Firewall: Edit Rule

| LABEL | DESCRIPTION |
|--|--|
| Schedule | |
| Day to Apply | Select everyday or the day(s) of the week to apply the rule. |
| Time of Day to Apply (24-Hour Format) | Select All Day or enter the start and end times in the hour-minute format to apply the rule. |
| Log | |
| Log Packet Detail Information | This field determines if a log for packets that match the rule is created (Enable) or not (Disable). Go to the Log Settings page and select the Access Control logs category to have the Prestige record these logs. |
| Alert | |
| Send Alert Message to Administrator When Matched | Select the check box to have the Prestige generate an alert when the rule is matched. |
| Back | Click Back to return to the previous screen. |
| Apply | Click Apply to save your customized settings and exit this screen. |
| Cancel | Click Cancel to exit this screen without saving. |
| Delete | Click Delete to remove this firewall rule and return to the Firewall Rule Summary screen. |

6 Troubleshooting

Table 10 Troubleshooting

| PROBLEM | CORRECTIVE ACTION |
|---|--|
| None of the LEDs turn on when you turn on the Prestige. | <p>Make sure that you have the correct power adaptor connected to the Prestige and plugged in to an appropriate power source. Check all cable connections.</p> <p>If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.</p> |

Table 10 Troubleshooting

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the Prestige from the LAN. | <p>Check the cable connection between the Prestige and your computer or hub. Refer to the 1 Hardware Connections section for details.</p> <p>Ping the Prestige from a LAN computer. Make sure your computer Ethernet adapter is installed and functioning properly.</p> |
| Cannot ping any computer on the LAN. | <p>If the LAN LEDs are all off, check the cable connections between the Prestige and your LAN computers.</p> <p>Verify that the IP address, subnet mask of the Prestige and the LAN computers are in the same IP address range.</p> |
| Cannot ping any computer on the WLAN (P660HW) | <p>Make sure the WLAN LED is on.</p> <p>Make sure the wireless card on the wireless client is working.</p> <p>Check that both the Prestige and wireless client(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).</p> |
| Cannot get a WAN IP address from the ISP. | <p>The WAN IP is provided after the ISP verifies the MAC address, host name or user ID. Find out the verification method used by your ISP and configure the corresponding fields.</p> <p>If the ISP checks the user ID, check your service type, user name, and password in the WAN Setup screen.</p> |
| Cannot access the Internet. | <p>Verify the Internet connection settings in the WAN Setup screen.</p> <p>Make sure you entered the correct user name and password.</p> <p>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).</p> |