PSK Enterprise

This option features PSK used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption. Select the algorithm(s) you want to use, **TKIP** or **AES.** (AES is a stronger encryption method than TKIP.)

RADIUS Server. Enter the IP address of your RADIUS server.

RADIUS Port. Enter the port number of your RADIUS server.

Shared Key. Enter the key shared by the Router and RADIUS server.

Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-19: WIRELESS Tab - WIRELESS SECURITY - PSK Enterprise

PSK2 Enterprise

This option features PSK2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption. Select the algorithm(s) you want to use, **AES** or **TKIP or AES.** (AES is a stronger encryption method than TKIP.)

RADIUS Server. Enter the IP address of your RADIUS server.

RADIUS Port. Enter the port number of your RADIUS server.

Shared Key. Enter the key shared by the Router and RADIUS server.

Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-20: WIRELESS Tab - WIRELESS SECURITY - PSK2 Enterprise

WEP

WEP is a basic encryption method offering two levels of encryption; 128-bit is stronger than 40/64-bit encryption.

Encryption. Select the appropriate level of encryption, **40/64-bit (10 hex digits)** or **128-bit (26 hex digits)**.

Passphrase. To automatically generate keys, enter your passphrase. Then click the **Generate** button.

Key 1-4. If you want to manually enter the WEP keys, then enter them in the *Key 1-4* fields.

TX Key. To indicate which WEP key to use, select a transmit key number.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-21: WIRELESS Tab - WIRELESS SECURITY - WEP

The WIRELESS Tab - WIRELESS MAC FILTER

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.

Wireless MAC Filter

To filter wireless users by MAC Address, either permitting or blocking access, click **Enable**. If you do not wish to filter users by MAC Address, select **Disable**.

Access Restrictions

Prevent. Click this button to block wireless access from the devices listed on this screen.

Permit. Click this button to allow wireless access by the devices listed on this screen.

MAC Address Filter List

Click the **Wireless Client List** button to display the Wireless Client List. It shows computers and other devices on the wireless network. The list is shown by MAC Address. Enter the MAC addresses of the devices whose wireless access you want to block or allow. When you have finished making changes to the *Wireless Client List*, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-22: WIRELESS Tab - WIRELESS MAC FILTER

The WIRELESS Tab - ADVANCED WIRELESS SETTINGS

These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Advanced Wireless Setting

Transmission Rate. The rate of data transmission should be set depending on the speed of your wireless network. Select from a range of transmission speeds, or select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default setting is **Auto.**

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode's allows the Router to automatically use this Mode when your Wireless-N and Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-N and Wireless-G transmissions but severely decreases performance. The default setting is **Auto.**

Beacon Interval. This value indicates the frequency interval of the beacon which is a packet broadcast by the Router to synchronize the wireless network. Enter a value between a-65535 mscs.The default value is **100 msc**.

DTIM Interval. This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The value can be between 1 and 255 The default value is **1.**

Fragmentation Threshold. This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, a slight increase should help. Too low a setting may result in poor network performance. Only minor reduction of the default value is recommended. The value can be between 256 and 2346. In most cases, it should remain at its default value of **2346**.

RTS Threshold. Should you encounter inconsistent data flow, only minor reduction of the default value, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. In most cases, keep its default value of **2346.**

Network Density. Adjust the density allowed on the network. The default is **Low.**

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGE** to undo your changes.

Figure 5-23: WIRELESS Tab - ADVANCED WIRELESS SETTINGS

The WIRELESS Tab - WISH

Figure 5-24: WIRELESS Tab - WISH

The SECURITY Tab - FIREWALL

The *FIREWALL* screen offers a firewall and filters that block specific Internet data types.

Firewall

Firewall Protection. A firewall enhances network security and uses Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network. Select **Enable** to use a firewall, or **Disable** to disable it.

Block WAN Request

Block WAN Requests. When enabled, this feature keeps your network from being "pinged," or detected, by other Internet users. It also hides your network ports. Both make it more difficult for outside users to enter your network. Click in the box to block anonymous internet requests.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGE** to undo your changes.

Figure 5-25: SECURITY Tab - FIREWALL

The SECURITY Tab - VPN PASSTHROUGH

The *VPN PASSTHROUGH* screen allows you to allow VPN tunnels usingPPPoE, IPSec, PPTP or L2TP protocols to pass through the Router.

VPN Passthrough

PPPoE Passthrough. PPPoe (Point-to-Point Protocol over Ethernet) allows a PPP session to be initiated on a simple bridging Ethernet connected client. To allow PPPoE Passthrough, click the **Enable** button. To disable PPPoE Passthrough, click the **Disable** button.

IPSec Passthrough. IPSec (Internet Protocol Security) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enable** button. To disable IPSec Passthrough, click the **Disable** button.

PPTP Passthrough. PPTP (Point-to-Point Tunneling Protocol) allows the Point-to-Point (PPP) to be tunneled through an IP network. To allow PPTP Passthrough, click the **Enable** button. To disable PPTP Passthrough, click the **Disable** button.

L2TP Passthrough. L2TP (Layer 2 Tunneling Protocol) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, click the **Enable** button. To disable L2TP Passthrough, click the **Disable** button.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-26: SECURITY Tab - VPN PASSTHROUGH

***vpn**: a security measure to protect data as it leaves one network and goes to another over the Internet.*

***pppoe**: a signaling protocol defined within PPPoE as well as the encapsulation method.*

***ipsec**: a VPN protocol used to implement secure exchange of packets at the IP layer.*

***pptp**: a VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.*

The ACCESS RESTRICTIONS Tab - INTERNET ACCESSS POLICY

The *INTERNET ACCESS POLICY* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, websites, and inbound traffic during specific days and times.

INTERNET ACCESS POLICY

Internet Access. Use these settings to choose an access policy to see a summary of, or delete. Select a policy from the drop-down menu. You can then click the **Delete This Entry** button or you can click the **Summary** button. On the *Summary* screen, the policies are listed with the following information: **No.**, Policy **Name**, Access, Days, **Time**, and status (Enabled).

Apply Policy. Enter the Policy Name in the field provided and to enable, click to have it **Enabled** or **Disabled.** Click the **Edit List** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of PCs. Click the appropriate option, **Deny** or **Allow,** depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.

Access Restrictions. You can choose to block or allow Internet Access, during specific times by clicking on the **Deny** or **Allow** button and then selecting the time(s) in the Schedule section.

Schedule. Decide which days and what times you want this policy to be enforced. Select **Everyday or** the individual days during which the policy will be in effect. You can also select the Times in which deny or allow internet access. Enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours.**

Web Blocking by URL Address. You can block websites with specific URL addresses. Enter each URL in a separate field next to *Website Blocking by URL Address.*

Blocked Applications. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.). From the Applications list, select the application you want to block. Then click the >> button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the << button. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the *Application Name* field. Enter its range in the *Port Range* fields. Select its protocol from the *Protocol* drop-down menu. Then click the **Add** button. To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click the **Modify** button. To delete a service, select it from the Application list. Then click the **Delete** button.

Click **SAVE Settings** to save your changes, or click **CANCEL CHANGES** to cancel your changes.

Figure 5-27: ACCESS RESTRICTION Tab - INTERNET ACCESS POLICY

The APPLICATIONS & GAMING Tab - SINGLE PORT FORWARDING

When you click the APPLICATIONS & GAMING tab, you will see the *SINGLE PORT FORWARDING* screen. You can customize port services for common applications on this screen.

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).

Single Port Forwarding

Common applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Click the **Enable** checkbox to activate this entry.

For additional applications, complete the following fields:

Application Name. Enter the name of the application.

External Port. Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.

Internal Port. Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.

Protocol. Select the protocol **TCP** or **UDP**, or select **Both**.

To IP Address. Enter the IP address of the server that should receive the requests. To find the IP address, go to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter." If you assigned a static IP address to the server, then you can click the **DHCP Reservation** button on the *Basic Setup* screen to look up its static IP address.

Enable. Click the **Enable** checkbox to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-28: APPLICATIONS & GAMING Tab - SINGLE PORT FORWARDING

***tcp**: a network protocol for transmitting data that requires acknowledgement from the recipient of data sent.*

***udp**: a network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.*

The APPLICATIONS & GAMING Tab - PORT RANGE FORWARDING

Port range forwarding sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).

If you need to forward all ports to one PC, click the **DMZ** tab.

Port Range Forwarding

To add an application, complete the following fields:

Application Name. Enter the name of the application.

Start ~ End Port. Enter the number or range of port(s) used by the server or Internet application. Check with the Internet application documentation for more information.

Protocol. Select the protocol **TCP** or **UDP**, or select **Both**.

To IP Address. Enter the IP address of the server that you want the Internet users to be able to access. To find the IP address, go to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter." If you assigned a static IP address to the server, then you can click the **DHCP Reservation** button on the *Basic Setup* screen to look up its static IP address.

Enable. Click the **Enable** checkbox to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-29: APPLICATIONS & GAMING Tab - PORT RANGE FORWARDING

The APPLICATIONS & GAMING Tab - PORT RANGE TRIGGERING

This screen instructs the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is sent to the proper computer by way of IP address and port mapping rules.

Port Range Triggering

To add an application, complete the following fields:

Application Name. Enter the name of the application.

Triggered Range. Enter the starting and ending port numbers of the triggered port range. Check with the Internet application documentation for the port number(s) needed.

Forwarded Range. Enter the starting and ending port numbers of the forwarded port range. Check with the Internet application documentation for the port number(s) needed.

Enable. Click the **Enable checkbox** to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-30: APPLICATIONS & GAMING Tab - PORT RANGE TRIGGERING

The APPLICATIONS & GAMING Tab - DMZ

The *DMZ* screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ

To use this feature, select **Enabled**. To disable DMZ hosting, select **Disabled**.

DMZ Host IP Address. If you want to specify the DMZ host by IP address, complete the IP address in the field provided.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-31: APPLICATIONS & GAMING Tab - DMZ

The APPLICATIONS & GAMING Tab - QOS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

QoS (Quality of Service)

Enable/Disable. To use the QoS policies, select **Enable.** Otherwise, select **Disable.**

Figure 5-32: APPLICATIONS & GAMING Tab - QOS

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

The ADMINISTRATION Tab- MANAGEMENT

When you click the Administration tab, you can select the *MANAGEMENT* screen. This screen allows you to change the Router's access settings and configure the UPnP (Universal Plug and Play) features. You can also back up and restore the Router's configuration file.

Local Router Access

To ensure the Router's security, you will be asked for your password when you access the Router's Web-based Utility. The default password is **admin**.

Router Password and Re-enter to Confirm. It is recommended that you change the default password to one of your choice. Enter a new Router password and then enter it again in the *Re-enter to Confirm* field.

HTTPS Web Access

HTTPS Access Server: If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's Web-based Utility. You will only be able to access the Utility via a wired connection if you disable the setting. Select **Enabled** to allow wireless access to the Utility, or select **Disabled** to block wireless access to the Utility.

Remote Router Access

Remote Management. To permit remote access of the Router, from outside the local network, select **Enabled**. Otherwise, keep the default setting, **Disabled**.

Management Port. Enter the port number that will be open to outside access.

Use HTTPs. HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. For more security when using the remote router, click on **HTTPS**.

UPnP

Universal Plug and Play (UPnP) allows Windows Me and XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing.

UPnP. If you want to use UPnP, keep the default setting, **Enabled**. Otherwise, select **Disabled**.

Allow Users to Disable Internet Access. Select **Enabled**, if you want to be able to prohibit any and all Internet connections. Otherwise, keep the default setting, **Disabled**.

Figure 5-33: ADMINISTRATION Tab - MANAGEMENT

Allow Users to modify Virtual Server Mappings. Select **Enabled**, if you want to allow manual changes to the Router while using the UPnP feature. Otherwise, keep the default setting, **Disabled**.

Multicast

Multicast Passthrough. If you want to allow multicast passthrough, select **Enabled**. Otherwise, select **Disabled**.

Reboot

Reboot the Device. To restore the Router's configuration settings, click this button and follow the on-screen instructions. (You must have previously backed up the Router's configuration settings.)

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

The ADMINISTRATION Tab - LOG

When you click the Administration tab, you can select the *Log* screen. It provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

Log Options

View. Click in a box to view the log for **Firewall Security**, the **System**, or the **Router Status**. You can also select the level of the log you want to see, **Critical, Warning** or **Informational.**

The Firewall Security log displays the login information for the Web-based Utility. The System Log will display a the source IP addresses, destination port numbers for the incoming Internet traffic, the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic. Router Status will display the LAN DHCP server status information.

Log Details

Click the **Save the Log** button to save this information to a file on your PC's hard drive. Click the **Refresh** button to update the log. Click the **Clear** button to clear all the information that is displayed.

NOTE: When you are in a remote location and wish to manage the Router, enter *http://<Internet IP Address>: port* or *https://<Internet IP Address>: port*, depending on whether you use HTTP or HTTPS. Enter the Router's specific Internet IP address in place of *<Internet IP Address>*, and enter the Administration Port number in place of the word *port*.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to undo your changes.

Figure 5-34: ADMINISTRATION Tab - LOG

The ADMINISTRATION Tab - DIAGNOSTICS

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network devices, including the connection to the Internet.

Ping Test. The Ping test will check the status of a connection. Enter the IP address or Domain Name of the PC whose connection you wish to test, the packet size (default is **32** bytes), and how many times you wish to test it. Then, click the **start test** button. The screen will then display the test results. To stop the test before it is finished, click the **abort test** button. Click the **clear** button to clear the test results.

Traceroute Test. To test the performance of a connect, enter the IP address or Domain Name of the PC whose connection you wish to test and click the **start test** button. The screen will then display the test results. To stop the test before it is finished, click the **abort test** button. Click the **clear** button to clear the test results.

Figure 5-35: ADMINISTRATION Tab - DIAGNOSTICS

The ADMINISTRATION Tab - FACTORY DEFAULT

The *FACTORY DEFAULT* screen allows you to restore the Router's configuration to its factory default settings.

Factory Defaults

Restore Factory Defaults. To clear all of the Router's settings and reset them to its factory defaults, click the **Restore Factory Defaults** button.

Click on **SAVE SETTINGS** to confirm your choice. Click on **CANCEL CHANGES** if you do not want to reset the Router's settings to the Factory Defaults.

Figure 5-36: ADMINISTRATION Tab - FACTORY DEFAULT

The ADMINISTRATION Tab - FIRMWARE UPGRADE

The *FIRMWARE UPGRADE* screen allows you to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.

NOTE: Do not restore the factory defaults unless you are having difficulties with the Router and have exhausted all other troubleshooting measures. Once the Router is reset, you will have to re-enter all of your configuration settings.

Before upgrading the firmware, download the Router's firmware upgrade file from the Linksys website, *www.linksys.com*. Then extract the file.

Firmware Upgrade

Please Select a File to Upgrade. In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.

Upgrade. After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Figure 5-37: ADMINISTRATION Tab -FIRMWARE UPGRADE

firmware: *the programming code that runs a networking device.*

download*: to receive a file transmitted over a network.*

upgrade: *to replace existing software or firmware with a newer version.*

The STATUS Tab - ROUTER

The *ROUTER* screen displays information about the Router and its current settings. The on-screen information will vary depending on the Internet Connection Type selected on the *SETUP* screen.

Router Status

Firmware Version. This is the version number of the Router's current firmware.

NOTE: The Router may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings.

NAT. This shows whether the NAT is enabled or disabled.

Current Time. This shows the time set on the Router.

System Up Time. This displays the amount of time the system has been operating in this session.

Internet Connections

Connection Type. This indicates the type of Internet connection you are using.

Internet IP Address. The Router's Internet IP address is displayed here.

Subnet Mask. The Router's Subnet Mask for DHCP and static IP connections is displayed here.

Default Gateway. The Default Gateway address is displayed here for DHCP and static IP connections.

DNSIP Address. Shown here are the DNS (Domain Name System) IP addresses currently used by the Router.

MAC Address. This is the Router's MAC address, as seen by your ISP.

Click the **Renew** button to replace the current IP address—of the device connected to the Router's Internet port—with a new IP address. (Available for a DHCP connection).

Click the **Release** button to release the current IP address of the device connected to the Router's Internet port. (Available for a DHCP connection.)

Click **REFRESH** to update the on-screen information.

Figure 5-38: STATUS Tab - ROUTER

The STATUS Tab - LOCAL NETWORK

The *LOCAL NETWORK* screen displays information about the local network.

Local Network Status

MAC Address. The MAC Address of the Router's local interface is displayed here.

IP Address. This shows the Router's IP address, as it appears on your local network.

Subnet Mask. The Router's Subnet Mask is shown here.

DHCP Server. The status of the Router's DHCP server function is displayed here.

Start IP Address. For the range of IP addresses used by devices on your local network, the beginning IP address is shown here.

End IP Address. For the range of IP addresses used by devices on your local network, the ending IP address is shown here.

DHCP Client Table. Click the **DHCP Client Table** button to view the DHCP Routing Table. It lists computers and other devices that have been assigned IP addresses by the Router. The list displays each Hardware Address, Assigned IP Address, Host Name, and Expired Time (how many seconds are left for the current IP address). To retrieve the most up-to-date information, click **REFRESH**. To exit this screen and return to the *Local Network* screen, click **CLOSE WINDOW**.

Figure 5-39: STATUS Tab - LOCAL NETWORK

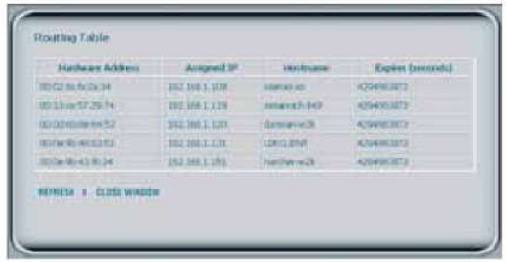

Figure 5-40: DHCP Client Table - Routing Table

The STATUS Tab - WIRELESS NETWORK

The *WIRELESS NETWORK* screen displays the status information of your wireless network.

Wireless Status

MAC Address. The MAC Address of the Router's wireless interface is displayed here.

Mode. Displayed here is the wireless mode (Mixed, Wireless-N Only, Wireless-G Only, Wireless-B Only, or Disabled) used by the network.

SSID (Network Name). Displayed here is the name of the wireless network or SSID.

Channel. Displayed here is the Channel selected on the *Basic Wireless Settings* screen.

Encryption Mode. Displayed here is the Encryption Mode setting selected on the *Wireless Security* screen.

Click **REFRESH** to update the on-screen information.

Figure 5-41: STATUS Tab - WIRELESS NETWORK

Appendix A: Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

Common Problems and Solutions

1. ***I'm trying to access the Router's Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, "404 Forbidden."***
   If you are using Windows Explorer, perform the following steps until you see the Web-based Utility's login screen (Netscape Navigator will require similar steps):
   1. Click **File**. Make sure *Work Offline* is NOT checked.
   2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.
   3. Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

2. ***I need to set a static IP address on a PC.***
   You can assign a static IP address to a PC by performing the following steps:
   - For Windows 98SE and Me:
     1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
     2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the **Properties** button.
     3. In the TCP/IP properties window, select the **IP address** tab, and select **Specify an IP address**. Enter a unique IP address that is not used by any other computer on the network connected to the Router. Make sure that each IP address is unique for each PC or network device.
     4. Click the **Gateway** tab, and in the New Gateway prompt, enter **192.168.1.1**, which is the default IP address of the Router. Click the **Add** button to accept the entry.
     5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
     6. Click the **OK** button in the TCP/IP properties window, and click **Close** or the **OK** button for the Network window.
     7. Restart the computer when asked.

- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the **Properties** option.
  3. In the Components checked are used by this connection box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  5. Enter the Subnet Mask, **255.255.255.0**.
  6. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
  7. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
  9. Restart the computer if asked.
- For Windows XP:
  The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.
  1. Click **Start** and **Control Panel**.
  2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
  3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
  4. In the This connection uses the following items box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
  5. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  6. Enter the Subnet Mask, **255.255.255.0**.
  7. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
  8. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

3. I want to test my Internet connection.

A Check your TCP/IP settings.

For Windows 98SE, Me, 2000, and XP:

- Refer to Windows Help for details. Make sure Obtain IP address automatically is selected in the settings.

B Open a command prompt.

For Windows 98SE and Me:

- Click **Start** and **Run**. In the *Open* field, type **command**. Press the **Enter** key or click the **OK** button.

For Windows 2000 and XP:

- Click **Start** and **Run**. In the *Open* field, type **cmd**. Press the **Enter** key or click the **OK** button. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.
- If you get a reply, the computer is communicating with the Router.
- If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

C In the command prompt, type **ping** followed by your Internet or WAN IP address and press the **Enter** key. The Internet or WAN IP Address can be found on the Status screen of the Router's web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.

- If you get a reply, the computer is connected to the Router.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

D In the command prompt, type **ping www.yahoo.com** and press the **Enter** key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

4. I am not getting an IP address on the Internet with my Internet connection.

- Refer to "Problem #3, I want to test my Internet connection" to verify that you have connectivity.
- If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix E: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of "Chapter 5: Configuring the Wireless-N Gigabit Gaming Router" for details.
- Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 5: Configuring the Wireless-N Gigabit Gaming Router" for details on Internet connection settings.
- Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.
- Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's web-based utility shows a valid IP address from your ISP.
- Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router's web-based utility to see if you get an IP address.

5. I am not able to access the Setup page of the Router's web-based utility.

- Refer to "Problem #3, I want to test my Internet connection" to verify that your computer is properly connected to the Router.
- Refer to "Appendix E: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
- Set a static IP address on your system; refer to "Problem #2: I need to set a static IP address."
- Refer to "Problem #10: I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window."

6. I need to set up a server behind my Router and make it available to the public.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.

1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications & Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the Application Name.
3. Enter the Start and End Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
4. Select the protocol(s) you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enabled** option for the port services you want to use. Consider the example below:

Application Name	Start and End Port	Protocol	To IP Address	Enabled
Web server	80 to 80	Both	192.168.1.100	X
FTP server	21 to 21	TCP	192.168.1.101	X
SMTP (outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (incoming)	110 to 110	Both	192.168.1.102	X

When you have completed the configuration, click the **Save Settings** button.

7. I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Router's web interface by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications & Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the Application Name.
3. Enter the Start and End Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Select the protocol(s) you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enabled** option for the port services you want to use. Consider the example below:

Application Name	Start and End Port	Protocol	To IP Address	Enabled
UT	7777 to 27900	Both	192.168.1.100	X
Halflife	27015 to 27015	Both	192.168.1.105	X
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

When you have completed the configuration, click the **Save Settings** button.

8. I can't get the Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.)