TZO.com

E-mail Address, Password, and Domain Name. Enter the Email Address, Password, and Domain Name of the service you set up with TZO.

Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, this will change.

Status. The status of the DDNS service connection is displayed here.

When you have finished making changes to this screen, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

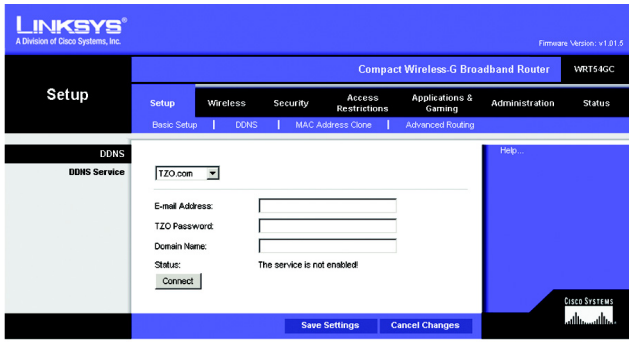

Figure 5-10: TZO.com

The Setup Tab - MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.

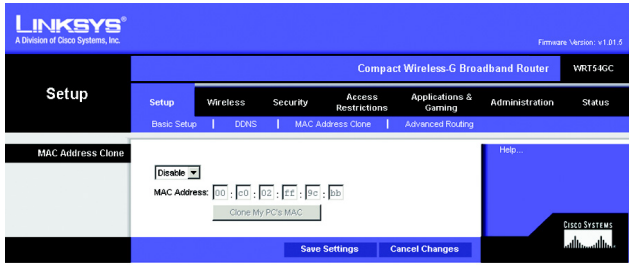

Figure 5-11: Setup Tab - MAC Address Clone

MAC Address Clone

Enabled/Disabled. To have the MAC Address cloned, select **Enabled** from the drop-down menu.

MAC Address. Enter the MAC Address registered with your ISP here.

Clone My PC's MAC. Clicking this button will clone the MAC address of the PC you are currently using.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

***mac address**: the unique address that a manufacturer assigns to each networking device.*

The Setup Tab - Advanced Routing

This tab is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing will automatically adjust how packets travel on your network. Static Routing sets up a fixed route to another network destination.

Figure 5-12: Setup Tab - Advanced Routing (Gateway)

Operating Mode. Select the mode in which this Router will function. If this Router is hosting your network's connection to the Internet, select **Gateway**. If another Router exists on your network, select **Router**. When Router is chosen, **Dynamic Routing** will be enabled.

Dynamic Routing. This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. This feature is **Disabled** by default. From the drop-down menu, you can also select **LAN & Wireless**, which performs dynamic routing over your Ethernet and wireless networks. You can also select **WAN**, which performs dynamic routing with data coming from the Internet. Finally, selecting **Both** enables dynamic routing for both networks, as well as data from the Internet.

Static Routing. To set up a static route between the Router and another network, select a number from the *Static Routing* drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.) Enter the information described below to set up a new static route. (Click the **Delete This Entry** button to delete a static route.)

Enter Route Name. Enter a name for the Route here, using a maximum of 25 alphanumeric characters.

Destination LAN IP. The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

Subnet Mask. The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

Default Gateway. This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

Interface. This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (Ethernet and wireless networks), the **WAN** (Internet), or a dummy network in which one PC acts like a network—necessary for certain software programs).

Figure 5-13: Setup Tab - Advanced Routing (Router)

Click the **Show Routing Table** button to view the Static Routes you've already set up.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Wireless Tab - Basic Wireless Settings

The basic settings for wireless networking are set on this screen.

Wireless Network

Wireless-G Settings

Mode. From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed**. If you have only 802.11g devices, select **G Only**. If you have only 802.11b devices, select **B Only**.

Network Name (SSID). The SSID is the network name shared by all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 keyboard characters in length. Make sure this setting is the same for all devices in your wireless network. For added security, you should change the default SSID (linksys) to a unique name.

Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must broadcast on the same channel in order to communicate.

SSID Broadcast. When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

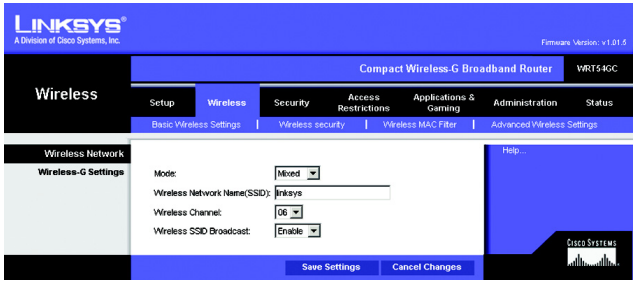

Figure 5-14: Wireless Tab - Basic Wireless Settings

The Wireless Tab - Wireless Security

The Wireless Security settings configure the security of your wireless network. There are three wireless security mode options supported by the Router: WPA Personal, WPA2 Personal, WPA2 Mixed Mode and WEP. (WEP stands for Wired Equivalent Privacy). These four are briefly discussed here. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."

Wireless Security

WEP. WEP is a basic encryption method. Select a level of WEP encryption, **64-bit** or **128-bit**. If you want to use a Passphrase, then enter it in the ***Passphrase*** field and click the **Generate** button. If you want to enter the WEP key manually, then enter it in the ***WEP Key 1-4*** field(s). To indicate which WEP key to use, select the appropriate ***TX Key*** number.

WPA Personal. This method offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of encryption method you want to use, **TKIP** or **AES**. Enter the Passphrase, which can have 8 to 63 characters. Then enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.

IMPORTANT: If you are using encryption, always remember that each device in your wireless network MUST use the same encryption method and encryption key, or else your wireless network will not function properly.

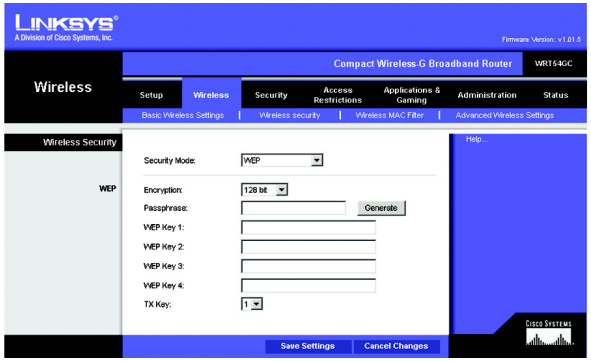

Figure 5-15: Wireless Tab - Wireless Security (WEP)

***wep** (wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.*

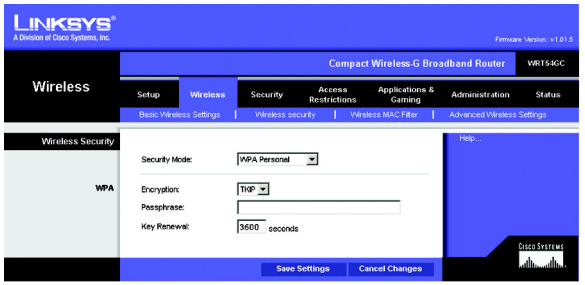

Figure 5-16: Wireless Tab - Wireless Security (WPA Personal)

WPA2 Personal. WPA2 gives you one encryption method, AES, with dynamic encryption keys. Enter a Passphrase of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.

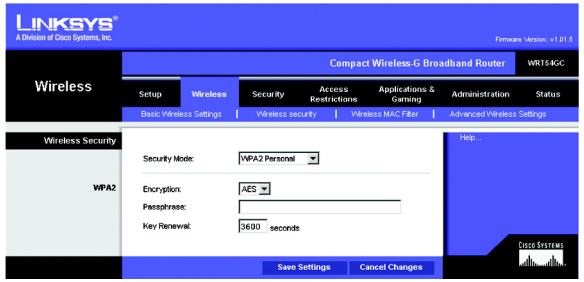

Figure 5-17: Wireless Tab - Wireless Security (WPA2 Personal)

WPA2 Mixed Mode. WPA2 gives you TKIP+AES encryption. Enter a Passphrase of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.

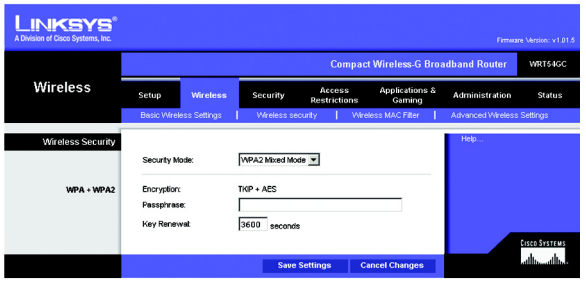

Figure 5-18: Wireless Tab - Wireless Security (WPA2 Mixed Mode)

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

Access Restrictions

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

Prevent PCs listed below from accessing the wireless network. Clicking this radio button will block wireless access by MAC Address.

Permit PCs listed below to access the wireless network. Clicking this radio button will allow wireless access by MAC Address.

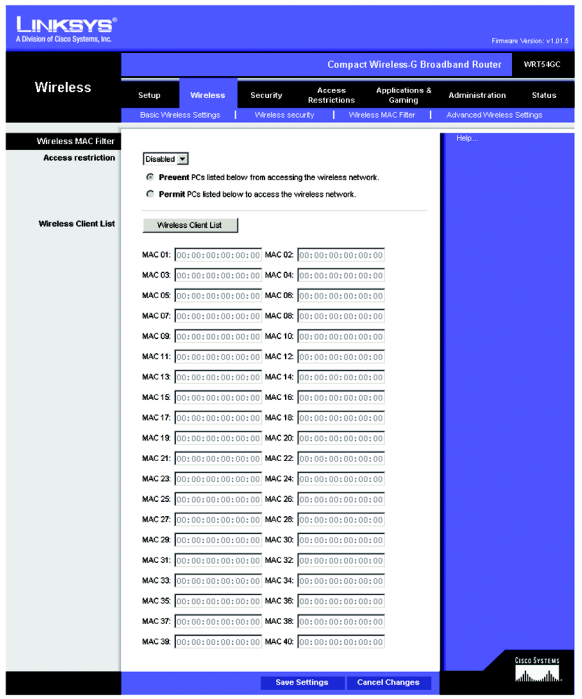

Figure 5-19: Wireless Tab - Wireless MAC Filter

Wireless Client List

Wireless Client List. Click the **Wireless Client MAC List** button to display a list of network users by MAC Address.From the ***To Sort by*** drop-down menu, you can sort the table by Client Name, IP Address, or MAC Address. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

List users, by MAC Address, whose wireless access you want to control.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

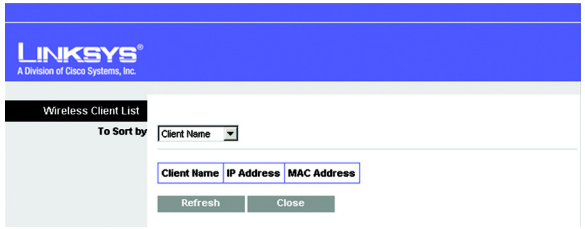

Figure 5-20: Wireless Tab - Wireless Client List

The Wireless Tab - Advanced Wireless Settings

This tab is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Advanced Wireless

Wireless-G Settings

Authentication Type. The default is set to **Auto (Default)**, allows either Open System or Shared Key authentication to be used. With **Open System** authentication, the sender and the recipient do NOT use a WEP key for authentication. With **Shared Key** authentication, the sender and recipient use a WEP key for authentication.

Transmission Rate. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto (Default)** 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 value is **Auto (Default)**.

Basic Rate. The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode should be set to **Auto (Default)**. The Router will automatically use CTS Protection Mode when your 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-G transmissions but will severely decrease performance.

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 default value is **1**.

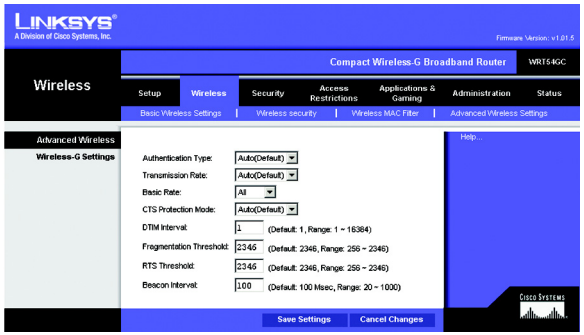

Figure 5-21: Wireless Tab - Advanced Wireless Settings

***cts** (clear to send): a signal sent by a wireless device, signifying that it is ready to receive data.*

***dtim**: a message included in data packets that can increase wireless efficiency.*

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, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

***fragmentation**: breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.*

RTS Threshold. Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, 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. The RTS Threshold value should remain at its default value of **2347**.

***beacon interval**: data transmitted on your wireless network that keeps the network synchronized.*

Beacon Interval. The default value is **100**. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

The Security Tab - Firewall

The *Firewall* screen offers Filters and the option to Block WAN Requests. Filters block specific Internet data types and block anonymous Internet requests. To enable a feature, select **Enabled** from the drop-down menu. To disable a feature, select **Disabled** from the drop-down menu.

Figure 5-22: Security Tab - Firewall

Firewall

- SPI Firewall Protection. Enable this feature to employ Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network environment.
- Block Anonymous Internet Requests. When enabled, this feature keeps your network from being "pinged," or detected, by other Internet users. It also reinforces your network security by hiding your network ports. Both functions of this feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Select **Disabled** to allow anonymous Internet requests.
- Filter Multicast. Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. Select Enable to filter multicasting, or Disable to disable this feature.
- Filter Internet NAT Redirection. This feature uses port forwarding to block access to local servers from local networked computers. Check the box to enable filter Internet NAT redirection, or uncheck the box to disable this feature.
- Web Filters

  Proxy. Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the checkbox.

  Java. Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. To enable Java filtering, click the checkbox.

  ActiveX. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click the checkbox.

  Cookies. A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click the checkbox.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

The Security Tab - VPN Passthrough

Use the settings on this tab to allow VPN tunnels using IPSec, L2TP, or PPTP protocols to pass through the Router's firewall.

VPN Passthrough

IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Pass-Through is enabled by default. To disable IPSec Passthrough, select **Disabled**.

L2TP Passthrough. Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass-Through is enabled by default. To disable L2TP Passthrough, select **Disabled**.

PPTP Passthrough. Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass-Through is enabled by default. To disable PPTP Passthrough, select **Disabled**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

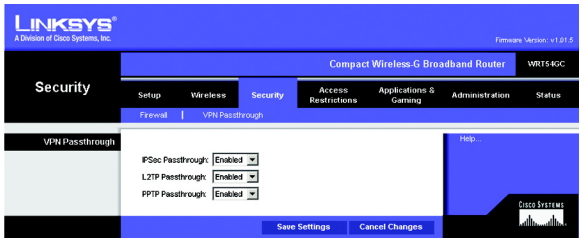

Figure 5-23: Security Tab - VPN Passthrough

***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 Access Policy

The *Internet Access Policy* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated applications, websites, and inbound traffic during specific days and times.

Internet Access Policy

Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete This Policy** button. To view all the policies, 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). You can change the type of access, days, and times of a policy. To activate a policy, click the **Enabled** checkbox. To delete a policy, click its **Delete** button. Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to cancel your changes. To return to the Internet Access Policy tab, click the **Close** button. To view the list of PCs for a specific policy, click the **PCs List** button.

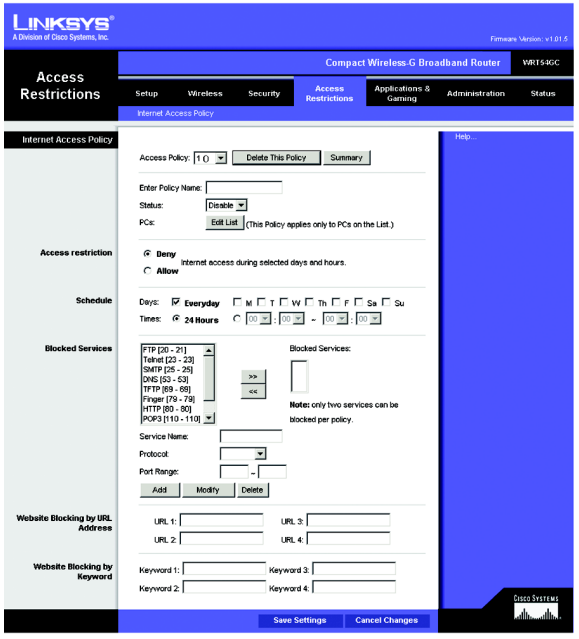

Figure 5-24: Access Restrictions Tab - Internet Access Policy