Router IP

IP Address and Subnet Mask. This shows both the Router's IP Address and Subnet Mask, as seen by your network. The default IP Address is **192.168.16.1**, and the default Subnet Mask is **255.255.255.0**. In most cases, keeping the default values will work.

DHCP Server Setting

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, you must make sure there is no other DHCP server on your network.

DHCP Server. DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then select **Disabled** (no other DHCP features will be available).

Static DHCP. Every time a PC reboots, it is assigned a new local IP address by the Router. If you want a PC to be assigned the same IP address every time it reboots, then click the **Static IP** button.

On the *DHCP Client List* screen, enter the static local IP address in the *Assign this IP* field, and enter the MAC address of the PC in the *To this MAC* field. Then click the **Enabled** checkbox. When you have finished your entries, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel your changes. To exit this screen, click the **Close** button.

If you want to see a list of DHCP clients, click the **DHCP Client Table** button. On the *DHCP Client Table* screen, you will see a list of DHCP clients with the following information: Client Name, Interface, IP Addresse, and MAC Addresse. To save the information, select **Static DHCP Client List**. From the *To Sort by* drop-down menu, you can sort the table by Client Name, Interface, 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.

Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.16.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. The default Starting IP Address is **192.168.16.100**.

Maximum Number of Users. Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

IP Address Range. The range of DHCP addresses is displayed here.

Client Lease Time. The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased"

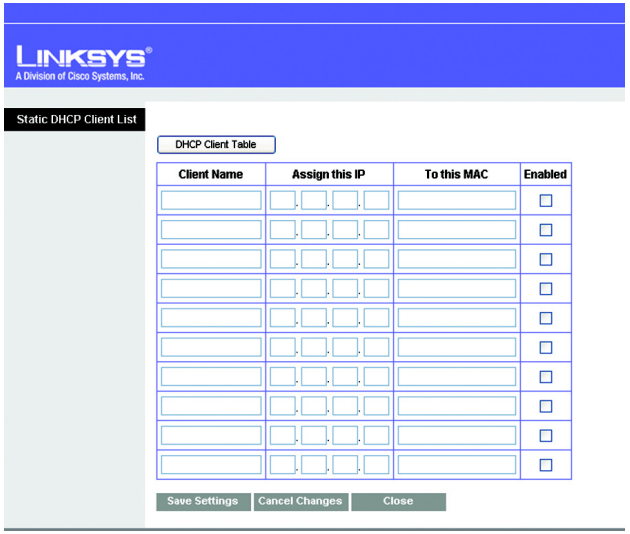

Figure 5-9: Static DHCP Client List

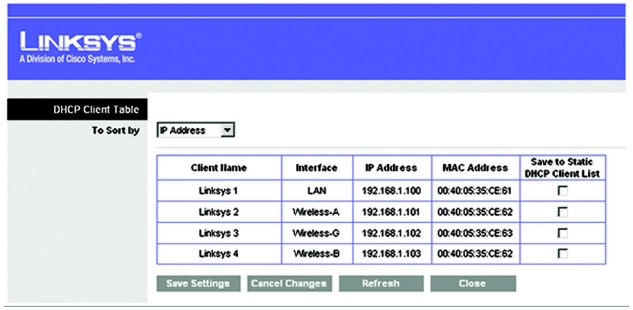

Figure 5-10: DHCP Client Table

this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day.

***dynamic ip address**: a temporary IP address assigned by a DHCP server.*

Static DNS (1-3). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

WINS. The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Time Settings

Change the time zone in which your network functions from this pull-down menu. Click the checkbox if you want the Router to automatically adjust for daylight savings time.

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 Setup Tab - DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router.

Before you can use this feature, you need to sign up for DDNS service at one of two DDNS service providers, DynDNS.org or TZO.com. If you do not want to use this feature, keep the default setting, **Disabled**.

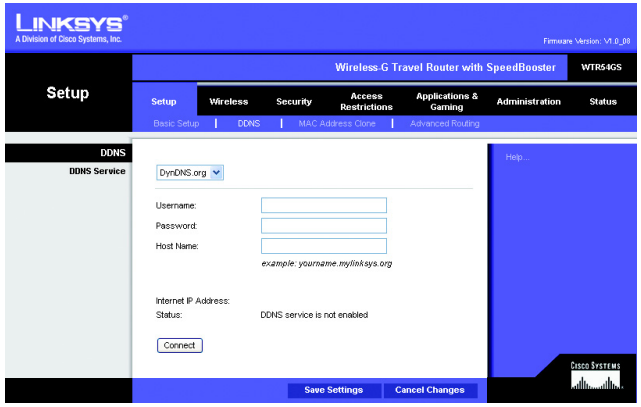

Figure 5-11: DynDNS.org

DDNS

DDNS Service. If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. If your DDNS service is provided by TZO, then select **TZO.com**. The features available on the ***DDNS*** screen will vary, depending on which DDNS service provider you use.

DynDNS.org

User Name, Password, and Host Name. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.

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

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

TZO.com

E-mail Address, TZO 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.

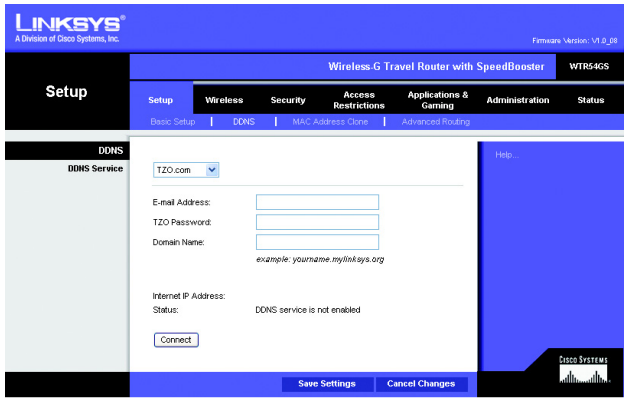

Figure 5-12: TZO.com

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.

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.

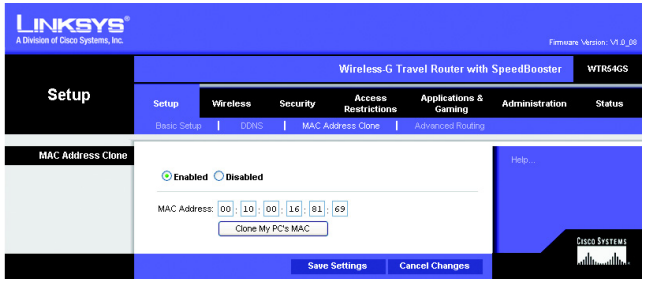

Figure 5-13: Setup Tab - MAC Address Clone

***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.

NAT (**Network Address Translation).** NAT technology translates IP addresses of a local area network to a different IP address for the Internet. To enable NAT, click **Enabled**. To disable NAT, click **Disabled**.

Dynamic Routing (RIP). 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.

Static Routing. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To set up a static route between the Router and another network, enter the information described below to set up a new static route by clicking the **Add New Entry** button to add an entry. Click the **Update Selected Entry** button to change an existing entry. (Click the **Delete** button to delete a static route.)

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. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0. For example, the Router's standard IP address is 192.168.16.1. Based on this address, the address of the routed network is 192.168.16, with the last digit determining the Router's place on the network. Therefore you would enter the IP address 192.168.16.0 if you wanted to route to the Router's entire network, rather than just to the Router.

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. For example, a network may have the Subnet Mask of 255.255.255.0. This determines (by using the values 255) that the first three numbers of a network IP address identify this particular network, while the last digit (from 1 to 254) identifies the specific host.

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) or the **Internet** (WAN). 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.

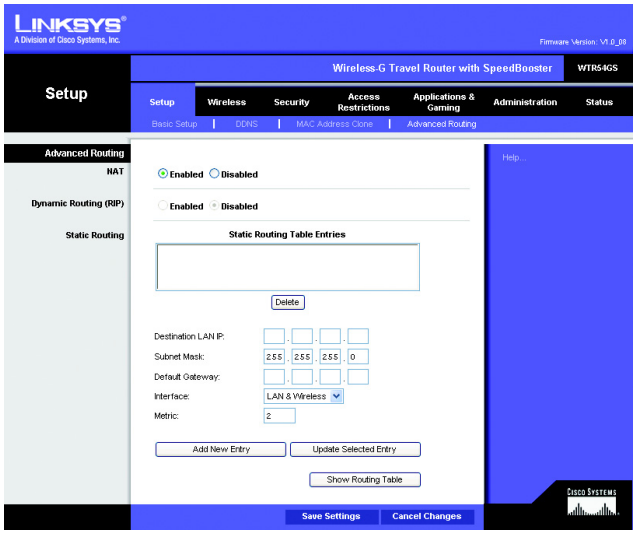

Figure 5-14: Setup Tab - Advanced Routing

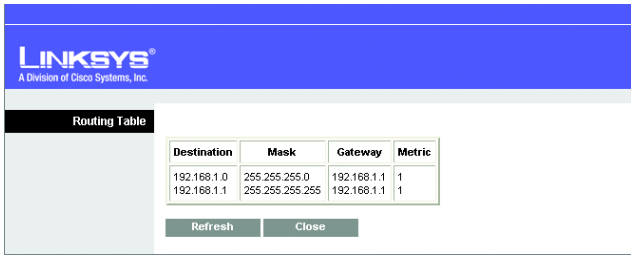

Figure 5-15: Setup Tab - Advanced Routing - Routing Table

Metric. This determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network, such as PCs, print servers, routers, etc.

Click the **Show Routing Table** button to view the Static Routes you've already set up. Show Routing Table. For each route, the Destination (LAN IP address), (Subnet) Mask, (Default) Gateway, and Metric are displayed. Click the **Refresh** button to update the information. Click the **Close** button to close the table.

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.

Basic Wireless Settings

Wireless. To use your Router's wireless connection, click **Enabled**. To disable your connection, click **Disabled**.

Network 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 **Wireless-G Only**. If you have only 802.11b devices, select **Wireless-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**.

Encryption. The wireless security used on your wireless network is displayed here.

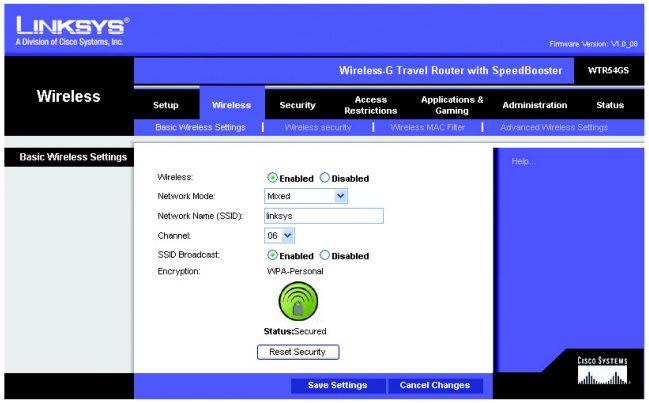

Figure 5-16: Wireless Tab - Basic Wireless Settings

SecureEasySetup Button. The status of the Router's SecureEasySetup feature is displayed here. If you want to use the SecureEasySetup feature, click the **SecureEasySetup** button.

You will be asked to press the SecureEasySetup button (hardware or software) on your wireless client (computer or other network device) within two minutes to complete the SecureEasySetup process. Click the **OK** button to continue.

A new screen will be displayed while the Router is waiting for you to push the SecureEasySetup button on your wireless client.

When the SecureEasySetup process is complete, the ***Basic Wireless Settings*** screen will appear, and the Current Encryption and Status information will be updated.

Status. The status of your wireless security is displayed here.

Reset Security. If you already set up the network using the SecureEasySetup feature and you want to replace your current settings with new SecureEasySetup settings, click the **Reset Security** button. A new screen will appear. You will be asked to confirm that you want to reset your wireless security settings. Click the **OK** button to continue.

The Router will generate a new network name (SSID) and set of keys.

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 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, 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."

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Wireless Security

WEP. WEP is a basic encryption method. Select a level of WEP encryption, **40/64-bit Hex digits** or **128-bit Hex digits**. 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.

- Passphrase. Instead of manually entering WEP keys, you can enter a passphrase. It is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 32 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, make a note of the WEP key generated in the Key 1 field, and enter it manually in the wireless client.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

- TX Key Select which WEP key (1-4) will be used when the Router sends data. Make sure that the receiving device (wireless client) is using the same key.

- WEP Keys 1-4. WEP keys enable you to create an encryption scheme for wireless network transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes; they are not valid key values.) If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F".

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.

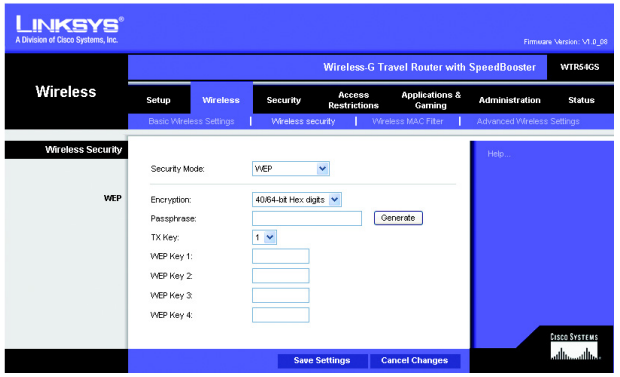

Figure 5-17: Wireless Tab - Wireless Security (WEP)

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

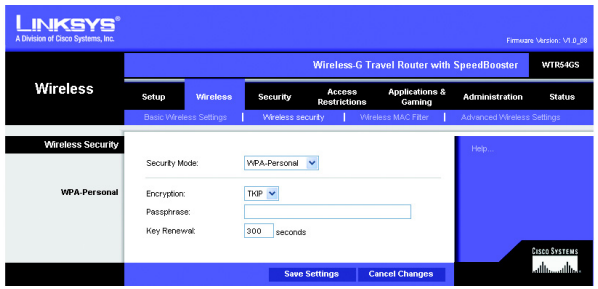

Figure 5-18: Wireless Tab - Wireless Security (WPA Personal)

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

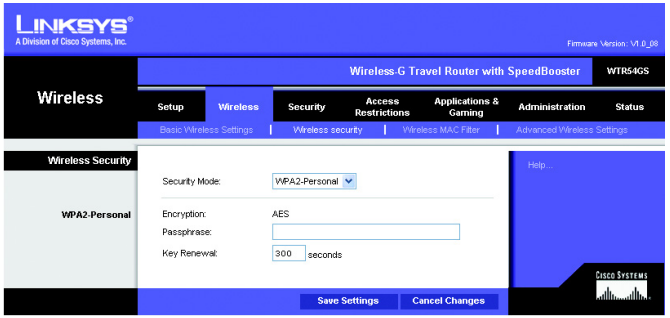

Figure 5-19: Wireless Tab - Wireless Security (WPA2-Personal)

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

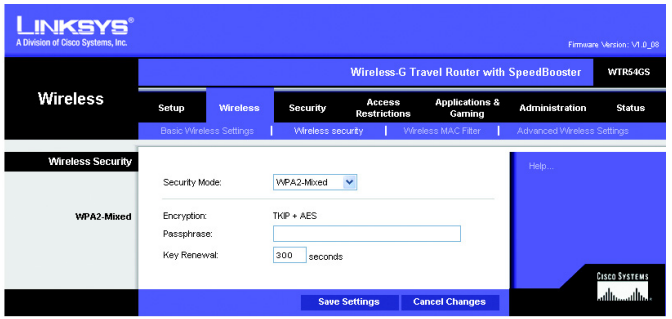

Figure 5-20: Wireless Tab - Wireless Security (WPA2-Mixed)

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 **Enabled**. If you do not wish to filter users by MAC Address, select **Disabled**.

Access Restriction

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

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

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, MAC Address, or Expires. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

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.

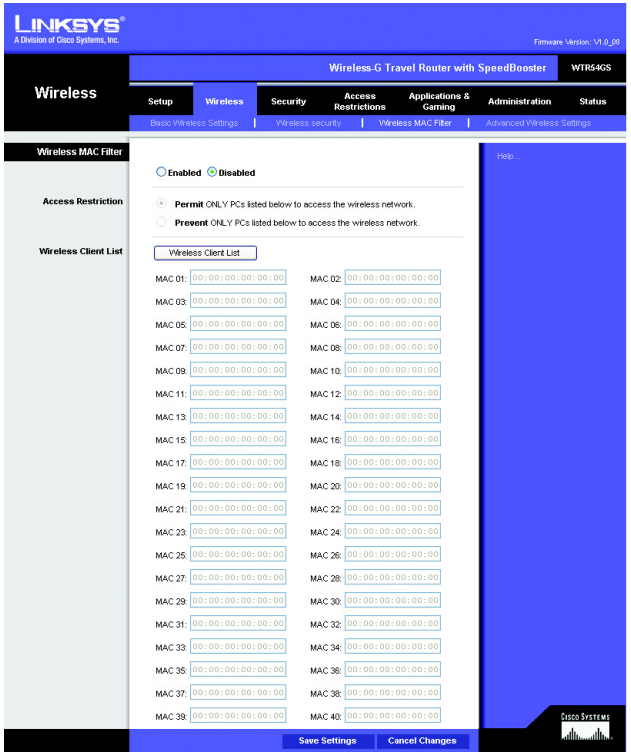

Figure 5-21: Wireless Tab - Wireless MAC Filter

Figure 5-22: 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

Frame Burst Mode. Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, **Enabled (Default)**.

AP Isolation. This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, click **Enabled**. AP Isolation is disabled by default.

Authentication Type. The default is set to **Open System**, 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.

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.

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)**.

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.

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.

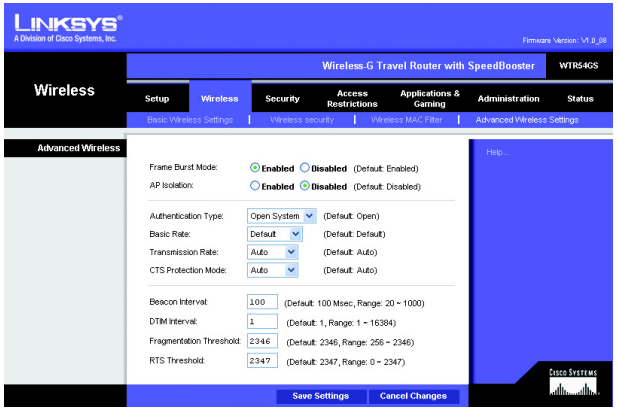

Figure 5-23: Wireless Tab - Advanced Wireless Settings

***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.*

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**.

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**.

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**.

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.

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

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

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.

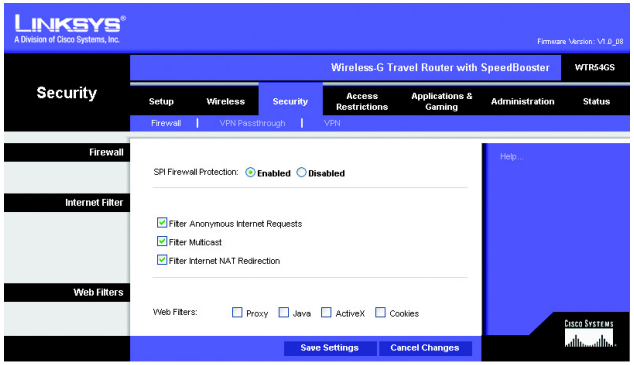

Figure 5-24: Security Tab - Firewall

Firewall

- SPI Firewall Protection. Enable this feature to employ Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network environment.
- Filter 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.

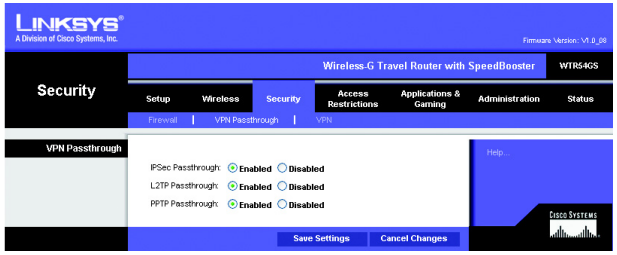

Figure 5-25: Security Tab - VPN Passthrough

***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 Security Tab - VPN

Use the settings on this tab to create VPN tunnels. The Wireless-G Travel Router creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure.

VPN Tunnel

Establishing a Tunnel

The Router creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure. To establish this tunnel, select the tunnel you wish to create in the *Select Tunnel Entry* drop-down menu. It is possible to create up to two simultaneous tunnels. To delete a tunnel, click the **Delete** button. To view a summary of that tunnel, click the **Summary** button. The *VPN Settings Summary* screen displays the number, name, local group, remote group, remote gateway, and security method.

Then check the box next to **Enable** to enable the tunnel. Once the tunnel is enabled, enter the name of the tunnel in the *Tunnel Name* field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

Figure 5-26: Security Tab - VPN

Local Secure Group and Remote Secure Group

A Local Secure Group is a computer(s) on your network that can access the tunnel. A Remote Secure Group is a computer (s) on the remote end of the tunnel that can access the tunnel. Under Local Secure Group and Remote Secure Group, you may choose one of three options: Subnet, IP Address, and IP Range. Under Remote Secure Group, you have two additional options: Host and Any.

Subnet. If you select Subnet (which is also the default), this will allow all computers on the local subnet to access the tunnel. When using the Subnet setting, the default values of 0 should remain in the last fields of the IP and Mask settings.

IP Address. If you select IP Address, only the computer with the specific IP Address that you enter will be able to access the tunnel.

IP Range. If you select IP Range, it will be a combination of Subnet and IP Address. You can specify a range of IP Addresses within the Subnet which will have access to the tunnel.

The next to options are for Remote Secure Groups only.

Host. If you select Host for the Remote Secure Group, then the Remote Secure Group will be the same as the Remote Security Gateway setting: IP Address, FQDN (Fully Qualified Domain Name), or Any.

Any. If you select Any for the Remote Security Group, the local VPN Router will accept a request from any IP address. This setting should be chosen when the other endpoint is using DHCP or PPPoE on the Internet side.

Remote Security Gateway

The Remote Security Gateway is the VPN device, such as a second VPN Router, on the remote end of the VPN tunnel. Under Remote Security Gateway, you have three options: IP Address, FQDN, and Any. In this section, you can also set the levels and types of encryption and authentication.

IP Address. If you select IP Address, enter the IP Address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. The IP Address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Router, but the IP Address of the remote VPN Router or device with which you wish to communicate.

FQDN (Fully Qualified Domain Name). If you select FQDN, enter the FQDN of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. The FQDN is the host name and domain name for a specific computer on the Internet, for example, vpn.myvpnserver.com.

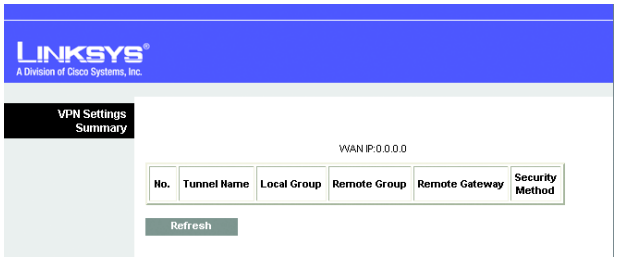

Figure 5-27: Security Tab - VPN - Summary

Any. If you select Any for the Remote Security Gateway, the VPN device at the other end of the tunnel will accept a request from any IP address. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. If the remote user has an unknown or dynamic IP address (such as a professional on the road or a telecommuter using DHCP or PPPoE), then Any should be selected.

Encryption. Using Encryption also helps make your connection more secure. There are two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable.

Authentication. Authentication acts as another level of security. There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication.

Key Management

In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a "key" to the encryption code. Under Key Management, you may choose automatic or manual key management.

Automatic Key Management. Select Auto (IKE) and enter a series of numbers or letters in the Pre-shared Key field. Check the box next to PFS (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. In the example shown the word **chappy** is used. Based on this word, which MUST be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.

Manual Key Management. Similarly, you may choose Manual keying, which allows you to generate the key yourself. Enter your key into the Encryption KEY field. Then enter an Authentication KEY into that field. These fields must both match the information that is being entered in the fields at the other end of the tunnel. Up to 24 alphanumeric characters are allowed to create the Encryption Key. Up to 20 alphanumeric characters are allowed to create the Authentication Key.

The Inbound SPI and Outbound SPI fields are different, however. The Inbound SPI value set here must match the Outbound SPI value at the other end of the tunnel. The Outbound SPI here must match the Inbound SPI value at the other end of the tunnel. That is, the Inbound SPI and Outbound SPI values would be opposite on the other end of the tunnel. Only numbers can be used in these fields. After you click the **Save Settings**

button, hexadecimal characters (series of letters and numbers) are displayed in the Inbound SPI and Outbound SPI fields.

The ***Status*** field at the bottom of the screen will show when a tunnel is active.

To connect a VPN tunnel, click the **Connect** button. The **View Logs** button, when logging is enabled on the Log screen of the Administration tab, will show you VPN activity on a separate screen. The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used. For more advanced VPN options, click the **Advanced Setting** button to open the Advanced Setting screen.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Advanced VPN Tunnel Setup

From the Advanced Settings screen you can adjust the settings for specific VPN tunnels.

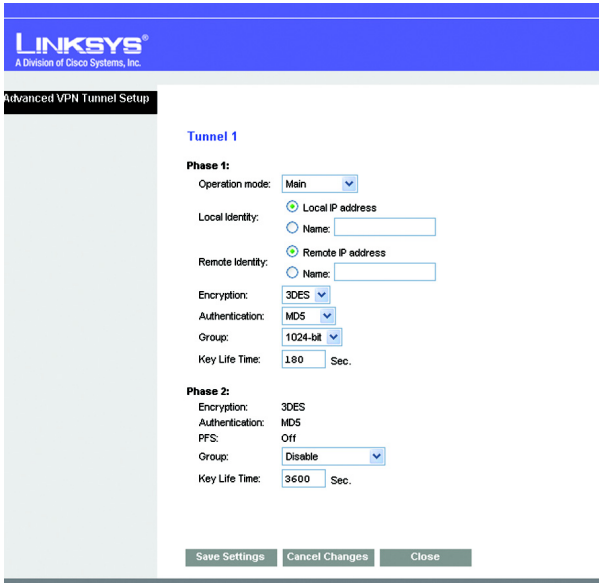

Figure 5-28: Security Tab - VPN - Advanced VPN Tunnel Setup

Phase 1. Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.

Operation Mode. There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Router will accept both Main and Aggressive requests from the remote VPN device. If a user on one side of the tunnel is using a Unique Firewall Identifier, this should be entered under the **Username** field.

Encryption. Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.

Authentication. Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.

Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Lifetime. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Phase 2

Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Lifetime. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

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.

On the *Internet Access PCs List* screen, 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. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Click the **Close** button to exit this screen.

To create an Internet Access policy:

1. Select a number from the *Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select **Enable** from the *Status* drop-down menu.
4. Click the **Edit List** button to select which PCs will be affected by the policy. The *Internet Access PCs List* 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. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button.

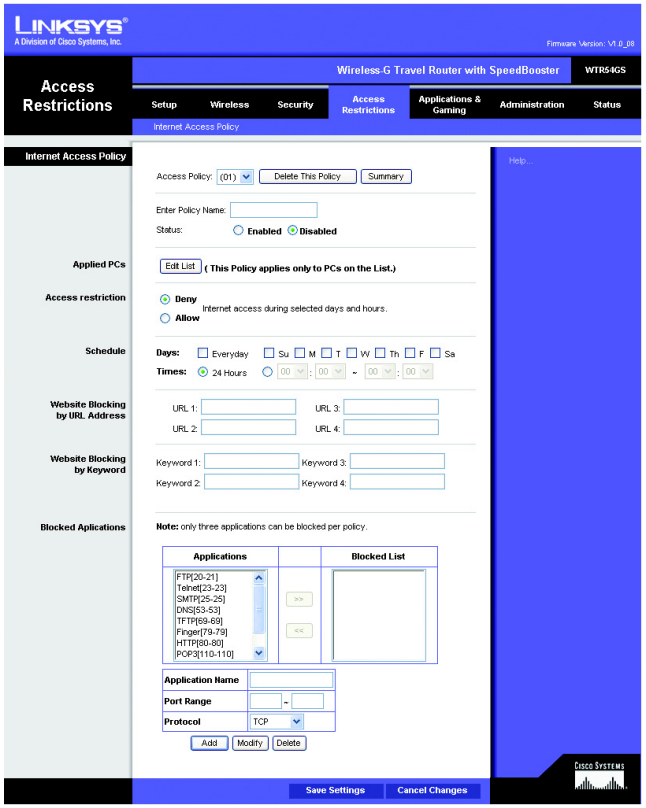

Figure 5-29: Access Restrictions Tab - Internet Access Policy

5. 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.

6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

7. You can filter access to various applications accessed over the Internet, such as FTP or telnet, by selecting up to three applications from the drop-down menus under *Applications*.

   The Blocked List menu offers a choice of ten preset applications. For the preset applications you select, the appropriate range of ports will automatically be displayed. Click the **>>** button to add to the Blocked Services list.

   If the application you want to block is not listed or you want to edit an application's settings, then create a new one by entering an Application Name, Port Range, and Protocol. Then, click **Add**.

8. You can also block access by URL address by entering it in the *Website Blocking by URL* Address field or by Keyword by entering it in the *Website Blocking by Keyword* field.

9. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.

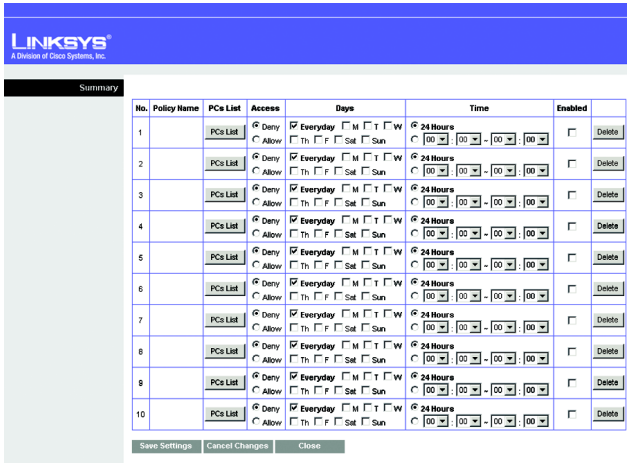

Figure 5-30: Access Restrictions Tab - Summary

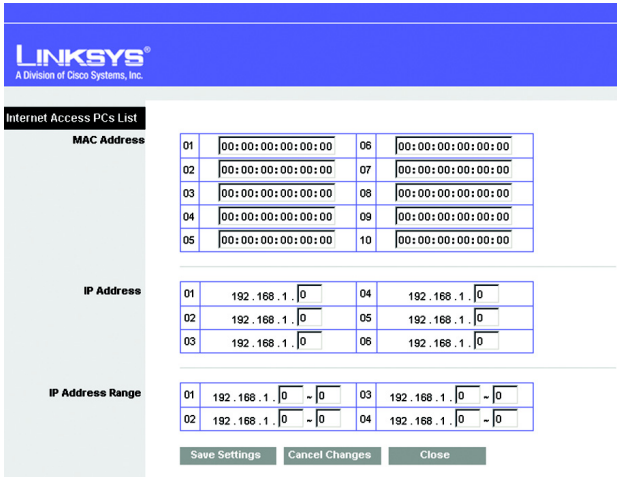

Figure 5-31: Access Restrictions Tab - Internet Access PCs List