VPN

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. This connection is very specific as far as its settings are concerned; this is what creates the security. The VPN screen, shown in Figure 6-17, allows you to configure your VPN settings to make your network more secure.

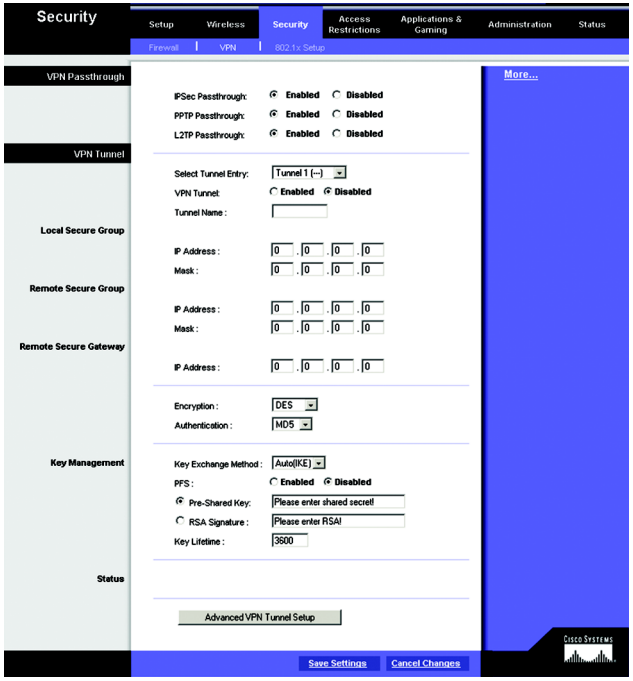

Figure 6-17: VPN

VPN PassThrough

- IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enabled** button. To disable IPSec Passthrough, click the **Disabled** button.
- PPTP Pass Through. Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enabled** button. To disable PPTP Passthrough, click the **Disabled** button.
- L2TP Pass Through. Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by to enable the operation of a virtual private network (VPN) over the Internet.To allow L2TP Passthrough, click the **Enabled** button. To disable L2TP Passthrough, click the **Disabled** button.

VPN Tunnel

The VPN 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 box. It is possible to create up to 50 simultaneous tunnels. Then click **Enabled** 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.
- Local Secure Group and Remote Secure Group. The Local Secure Group is the computer(s) on your LAN that can access the tunnel. The Remote Secure Group is the computer (s) on the remote end of the tunnel that can access the tunnel. Enter the **IP Address** and **Subnet Mask** of the local VPN Router in the fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).
- 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. 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.

- 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. In Figure 6-18, DES (which is the default) has been selected.

- 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. In Figure 6-18, MD5 (the default) has been selected.

- Key Management. Key Exchange Method. Select **Auto (IKE)** or **Manual** for the Key Exchange Method. The two methods are described below.

  Auto (IKE)
  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. 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 (See Figure 6-18.)
  Select **Manual,** then select the Encryption Algorithm from the drop-down menu. Enter the Encryption Key in the field (If, for your Encryption Algorithm, you chose DES, enter 16 hexadecimal characters. If you chose 3DES, enter 48 hexadecimal characters.) Select the Authentication Algorithm from the drop-down menu. Enter the Authentication Key in the field (If, for your Authentication Algorithm, you chose MD5, enter 32 hexadecimal characters. If you chose SHA1, enter 40 hexadecimal characters.) . Enter the Inbound and Outbound SPIs in the respective fields.

- Status. Click the **Advanced VPN Tunnel Setup** key and the Advanced VPN Tunnel Setup screen will appear. See Figure 6-20.

Figure 6-18: Manual Key Management

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. Advanced VPN Tunnel Setup

From the Advance VPN Tunnel Setup screen, shown in Figure 6-19, you can adjust the settings for specific VPN tunnels.

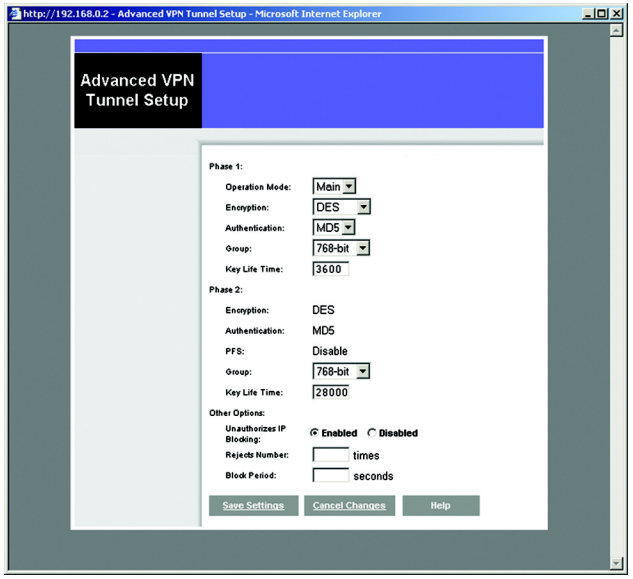

Figure 6-19: Advanced VPN Tunnel Setup

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.
- 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 Life Time. 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

- Encryption. The encryption method selected in Phase 1 will be displayed.
- Authentication. The authentication method selected in Phase 1 will be displayed.
- 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 Life Time. 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.

Other Options

- Unauthorized IP Blocking. Click **Enabled** to block unauthorized IP addresses. Enter in the Rejects Number field to specify how many times IKE must fail before blocking that unauthorized IP address. Enter the length of time that you specify (in seconds) in the Block Period field.

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. For further help on this tab, click the **Help** button.

Security

802.1x (See Figure 6-20.)

- Radius Server IP Address. Enter the Radius Server IP Address in the fields.
- Radius Server Port. Enter the Radius Server Port in the field.
- Shared Secret. Enter the Shared Secret in the field.
- Authentication Type. To enable EAP-TLS, click EAP-TLS. To enable EAP-TTLS, click EAP-TTLS. To enable EAP-MD5, click **EAP-MD5**,. To disable authentication, click **Disable**.
- WEP Settings. Click the **WEP Settings** button to edit the settings and Figure 7-22 will appear.
- Dynamic WEP Key Length. Select **64** or **128** bits from the drop-down menu.
- Key Renewal Timeout. Enter the time in seconds for key renewal.
- Port Inactivity Timeout. Enter the time in seconds for port inactivity.
- Port Connectivity Timeout. Enter the time in seconds for port connectivity.

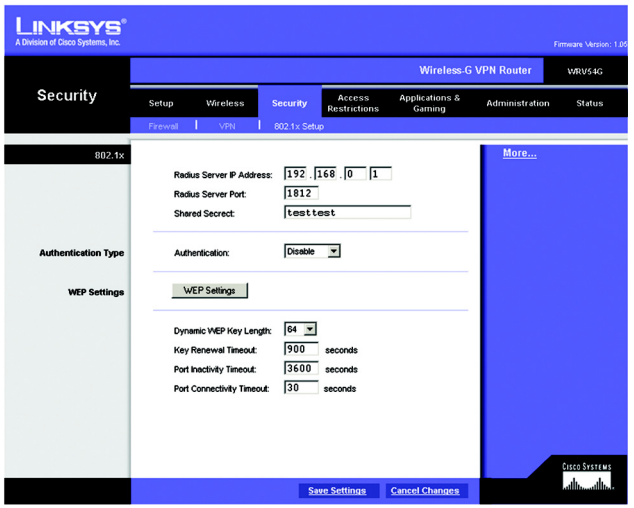

Figure 6-20: 802.1x

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.

WEP

The WEP screen allows you to configure your WEP settings. (See Figure 6-21.) WEP encryption should always be enabled to increase the security of your wireless network. Default Transmit Key. Select which WEP key (1-4) will be used when the Router sends data. Make sure that the receiving device is using the same key.

- WEP Encryption. Select the level of WEP encryption you wish to use, **64-bit 10 hex digits** or **128-bit 26 hex digits.** Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

- Passphrase. Instead of manually entering WEP keys, you can enter a Passphrase. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, enter the WEP key manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

- Keys 1-4. WEP keys enable you to create an encryption scheme for wireless LAN 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. These are not valid key values.)

  If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.

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.

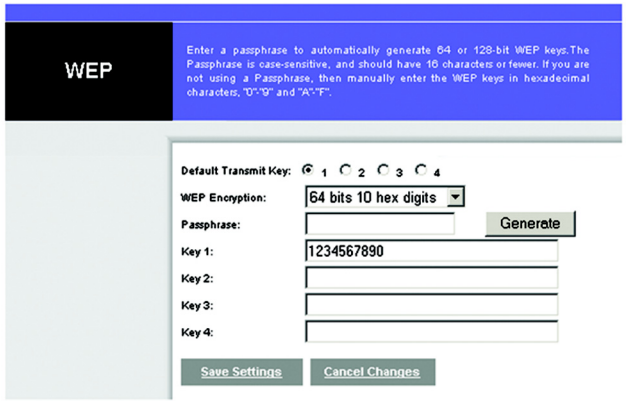

Figure 6-21: WEP

The Access Restrictions Tab

Access Restriction

The Access Restrictions tab, shown in Figure 6-22, allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific PCs and set up filters by using network port numbers.

- Internet Access Policy. Multiple Filters can be saved as Internet Access Policies. When you wish to edit one, select the number of the Policy from the drop-down menu. The tab will change to reflect the settings of this Policy. If you wish to delete this Policy, click the **Delete** button. To see a summary of all Policies, click the **Summary** button.

  The summaries are listed on this screen, shown in Figure 7-23, with their name and settings. To return to the Filters tab, click the **Close** button.

- Enter Policy Name. Policies are created from the fields presented here.

  To create an Internet Access policy:

1. Enter a Policy Name in the field provided. Select **Internet Access** as the Policy Type.

Figure 6-22: Access Restriction

2. Click the **Edit List** button. This will open the List of PCs screen, shown in Figure 6-24. From this screen, you can enter the IP address or MAC address of any PC to which this policy will apply. You can even enter ranges of PCs by IP address. Click the **Apply** button to save your settings, the **Cancel** button to undo any changes, and the **Close** button to return to the Filters tab.

3. If you wish to Deny or Allow Internet access for those PCs you listed on the List of PCs screen, click the option.

4. You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting a service from the drop-down menus next to Blocked Services. If a service isn't listed, you can click the **Add Service** button to open the Service screen, shown in Figure 6-25, and add a service to the list. You will need to enter a Service name, as well as the Protocol and Port Range used by the service.

5. By selecting the appropriate setting next to Days and Time, choose when Internet access will be filtered.

6. Lastly, click the **Save Settings** button to activate the policy.

To create an Inbound Traffic Policy

1. Enter a Policy Name in the field provided. Select **Inbound Traffic** as the Policy Type.

2. Enter the **IP Address** from which you want to block. Select the Protocol: **TCP**, **UDP**, or **Both**. Enter the **port** number or select **Any**. Enter the IP Address to which you want to block.

3. Select **Deny** or **Allow** as appropriate.

4. By selecting the appropriate setting next to Days and Time, choose when the Inbound Traffic will be filtered.

Lastly, click the **Save Settings** button to activate the policy.

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.

Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the Website Blocking by URL Address fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the Website Blocking by Keyword fields.

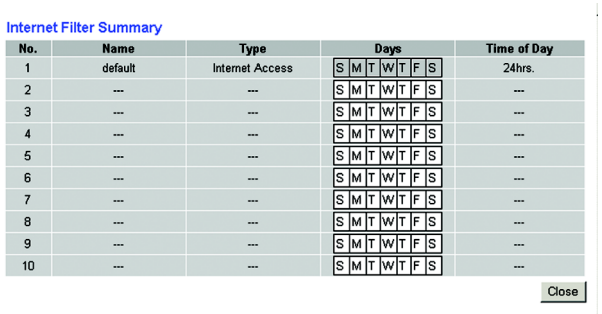

Figure 6-23: Internet Filter Summary

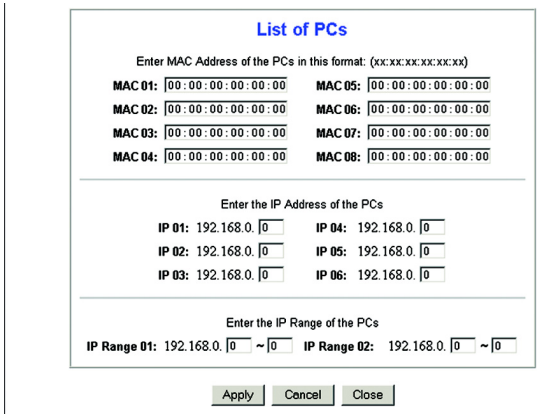

Figure 6-24: List of PCs

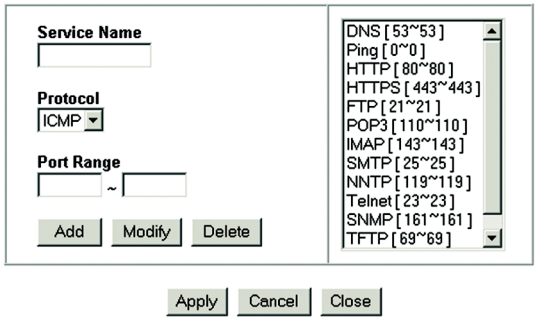

Figure 6-25: Blocked Services

The Applications and Gaming Tab

Port Range Forwarding

The Port Forwarding screen 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.) (See Figure 6-26.)

When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate PC. Any PC whose port is being forwarded must have its DHCP client function disabled and must have a new static IP address assigned to it because its IP address may change when using the DHCP function.

- Application. Enter the name you wish to give each application.
- Start and End. Enter the starting and ending numbers of the port you wish to forward.
- Protocol. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- IP Address. Enter the IP Address and Click **Enabled**.

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.

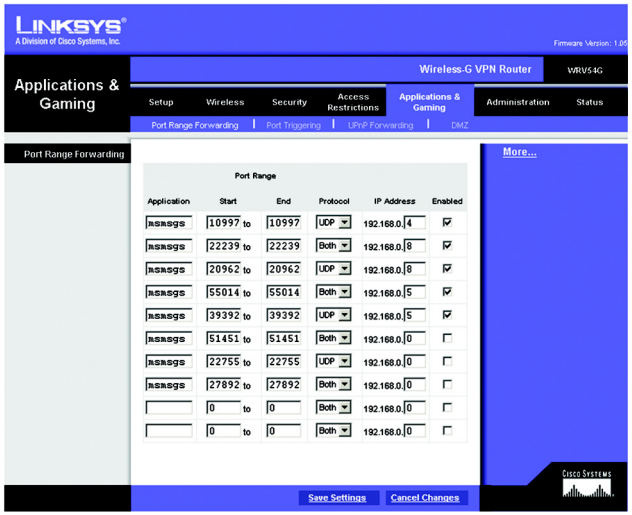

Figure 6-26: Port Range Forwarding

Port Triggering

Port Triggering is used for special Internet applications whose outgoing ports differ from the incoming ports. For this feature, the Router will watch outgoing data for specific port numbers. (See Figure 6-27.) The Router will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

- Application. Enter the name you wish to give each application.
- Start Port and End Port. Enter the starting and ending Triggered range numbers and the Forwarded Range numbers of the port you wish to forward.
- Protocol. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- Click **Enabled**.

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.

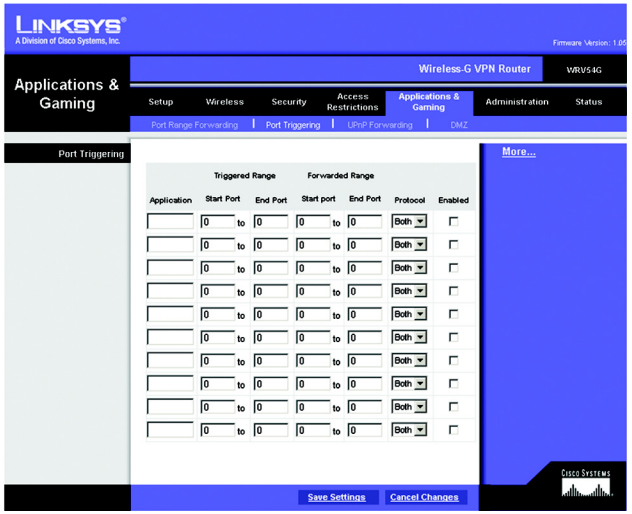

Figure 6-27: Port Triggering

UPnP Forwarding

The UPnP screen provides options for customization of port services for applications. (See Figure 6-28.)

Enter the Application in the field. Then, enter the External and Internal Port numbers in the fields. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**. Enter the IP Address in the field. Click **Enabled** to enable UPnP Forwarding for the chosen application.

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.

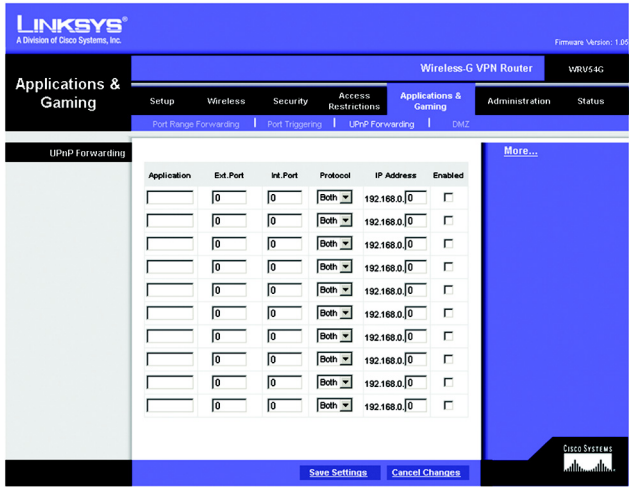

Figure 6-28: UPnP Forwarding

DMZ

The DMZ screen (see Figure 6-29) allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing, through Software DMZ, or a user can use LAN Port 4 as a DMZ Port, through Hardware DMZ. Whereas Port Range Forwarding can only forward a maximum of 10 ranges of ports, DMZ hosting forwards all the ports for one PC at the same time.

- Software DMZ. This feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enabled**. To disable DMZ , select **Disabled**.
- DMZ Host IP Address. To expose one PC, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter." Deactivate DMZ by entering a 0 in the field.
- Hardware DMZ. This feature allows a user to use LAN Port 4 as a DMZ Port. To use this feature, select **Enabled**. To disable DMZ , select **Disabled**.
- Hardware DMZ IP Address. Enter the IP Address of the computer in the fields.
- Hardware DMZ Netmask. Enter the Netmask in the fields.
- Destination IP Address. Enter the IP Address of the destination in the fields.
- Subnet Mask. Enter the Subnet Mask of the destination in the fields.
- Default Gateway. Enter the Default Gateway in the fields.
- metric. Enter the metric in the field.

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.

Figure 6-29: DMZ