

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.

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

Figure 6-17: VPN

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.

The screenshot shows the 'Security' tab of the router's configuration interface. The 'VPN' sub-tab is selected, and the 'Manual' key exchange method is chosen. The configuration fields are as follows:

Section	Field	Value
VPN Passthrough	IPSec Passthrough	Enabled
	PPTP Passthrough	Enabled
	L2TP Passthrough	Enabled
VPN Tunnel	Select Tunnel Entry	Tunnel 1 (-)
	VPN Tunnel	Enabled
Local Secure Group	IP Address	0.0.0.0
	Mask	0.0.0.0
Remote Secure Group	IP Address	0.0.0.0
	Mask	0.0.0.0
Remote Secure Gateway	IP Address	0.0.0.0
	Mask	0.0.0.0
Key Management	Key Exchange Method	Manual
	Encryption Algorithm	DES (DES:16 HEX 3DES:48 HEX)
	Encryption Key	0000000000000000
	Authentication Algorithm	MD5 (MD5:32 HEX SHA1:40 HEX)
	Authentication Key	0000000000000000
	Inbound SPI	100 (HEX, 100-FFFFFF)
Outbound SPI	100 (HEX, 100-FFFFFF)	

Buttons at the bottom: **Advanced VPN Tunnel Setup**, **Save Settings**, **Cancel Changes**.

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.

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.

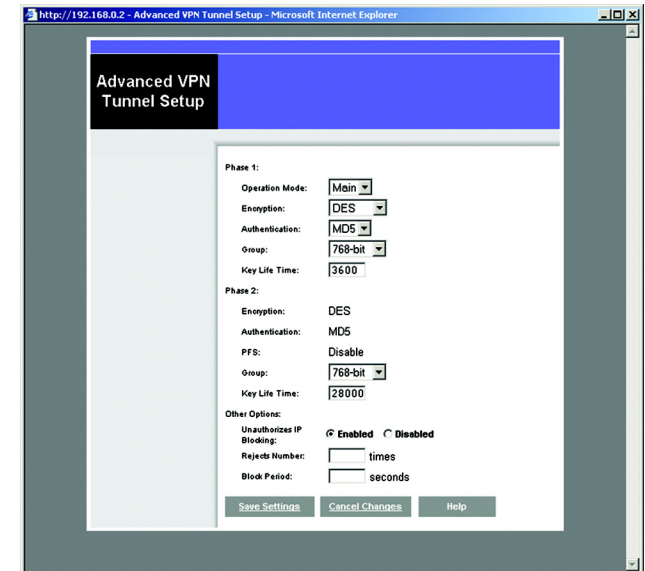


Figure 6-19: Advanced VPN Tunnel Setup

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.

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.

The screenshot shows the Linksys Wireless-G VPN Router configuration interface. The top navigation bar includes 'Setup', 'Wireless', 'Security' (selected), 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Security' tab is active, and the '802.1x Setup' sub-tab is selected. The 'Authentication Type' is set to 'EAP-MD5'. The 'Radius Server IP Address' is 192.168.0.1, 'Radius Server Port' is 1812, and 'Shared Secret' is 'testtest'. The 'Authentication' dropdown is set to 'Disable'. The 'WEP Settings' button is visible. Below it, the 'Dynamic WEP Key Length' is set to 64, 'Key Renewal Timeout' is 900 seconds, 'Port Inactivity Timeout' is 3600 seconds, and 'Port Connectivity Timeout' is 30 seconds. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

Figure 6-20: 802.1x

- **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.

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 6-21: WEP

Figure 6-22: Access Restriction

- 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.
- If you wish to Deny or Allow Internet access for those PCs you listed on the List of PCs screen, click the option.
- 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.
- By selecting the appropriate setting next to Days and Time, choose when Internet access will be filtered.
- Lastly, click the **Save Settings** button to activate the policy.

To create an Inbound Traffic Policy

- Enter a Policy Name in the field provided. Select **Inbound Traffic** as the Policy Type.
- 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.
- Select **Deny** or **Allow** as appropriate.
- 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.

Internet Filter Summary

No.	Name	Type	Days	Time of Day
1	default	Internet Access	S M T W T F S	24hrs.
2	---	---	S M T W T F S	---
3	---	---	S M T W T F S	---
4	---	---	S M T W T F S	---
5	---	---	S M T W T F S	---
6	---	---	S M T W T F S	---
7	---	---	S M T W T F S	---
8	---	---	S M T W T F S	---
9	---	---	S M T W T F S	---
10	---	---	S M T W T F S	---

Close

Figure 6-23: Internet Filter Summary

List of PCs

Enter MAC Address of the PCs in this format: (xx:xx:xx:xx:xx:xx)

MAC 01: [00:00:00:00:00:00] MAC 05: [00:00:00:00:00:00]
 MAC 02: [00:00:00:00:00:00] MAC 06: [00:00:00:00:00:00]
 MAC 03: [00:00:00:00:00:00] MAC 07: [00:00:00:00:00:00]
 MAC 04: [00:00:00:00:00:00] MAC 08: [00:00:00:00:00:00]

Enter the IP Address of the PCs

IP 01: 192.168.0.[0] IP 04: 192.168.0.[0]
 IP 02: 192.168.0.[0] IP 05: 192.168.0.[0]
 IP 03: 192.168.0.[0] IP 06: 192.168.0.[0]

Enter the IP Range of the PCs

IP Range 01: 192.168.0.[0] ~ [0] IP Range 02: 192.168.0.[0] ~ [0]

Apply Cancel Close

Figure 6-24: List of PCs

Service Name

[]

Protocol

ICMP

Port Range

[] ~ []

Add Modify Delete

DNS [53~53]
 Ping [0~0]
 HTTP [80~80]
 HTTPS [443~443]
 FTP [21~21]
 POP3 [110~110]
 IMAP [143~143]
 SMTP [25~25]
 NNTP [119~119]
 Telnet [23~23]
 SNMP [161~161]
 TFTP [69~69]

Apply Cancel Close

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.

Application	Start	End	Protocol	IP Address	Enabled
msnmsn	10997	10997	UDP	192.168.0.4	☒
msnmsn	22239	22239	Both	192.168.0.8	☒
msnmsn	20962	20962	UDP	192.168.0.8	☒
msnmsn	55014	55014	Both	192.168.0.5	☒
msnmsn	39392	39392	UDP	192.168.0.5	☒
msnmsn	51451	51451	Both	192.168.0.0	☐
msnmsn	22755	22755	UDP	192.168.0.0	☐
msnmsn	27892	27892	Both	192.168.0.0	☐
	0	0	Both	192.168.0.0	☐
	0	0	Both	192.168.0.0	☐

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.

Application	Triggered Range		Forwarded Range		Protocol	Enabled
	Start Port	End Port	Start port	End Port		
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐
	0	to 0	0	to 0	Both	☐

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.

Application	Ext. Port	Int. Port	Protocol	IP Address	Enabled
					☐
					☐
					☐
					☐
					☐
					☐
					☐
					☐
					☐
					☐

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.

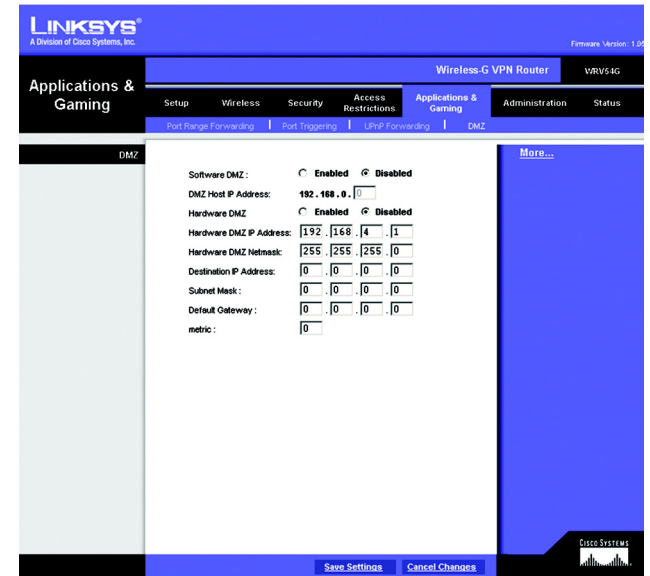


Figure 6-29: DMZ

The Administration Tab

Management

The Management screen, shown in Figure 6-30, allows you to change the Router's access settings as well as configure the SNMP and UPnP (Universal Plug and Play) features.

Router Password

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.

- **User Name.** Enter the default **admin**.
- **Router Password.** It is recommended that you change the default password to one of your choice.
- **Re-enter to confirm.** Re-enter the Router's new Password to confirm it.

Remote Router Access. This feature allows you to access the Router from a remote location, via the Internet.

- **Remote Management.** This feature allows you to manage the Router from a remote location, via the Internet. To enable Remote Management, click **Enabled**.
- **Management Port.** Select the port number you will use to remotely access the Router from the drop-down menu.

SNMP

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol. To enable SNMP, click **Enabled**. To disable SNMP, click **Disabled**.

- **Identification.** In the Contact field, enter contact information for the Router. In the Device Name field, enter the name of the Router. In the Location field, specify the area or location where the Router resides.
- **Get Community.** Enter the password that allows read-only access to the Router's SNMP information.
- **Set Community.** Enter the password that allows read/write access to the Router's SNMP information.
- **SNMP Trusted Host.** You can restrict access to the Router's SNMP information by IP address. Enter the IP address in the SNMP Trusted Host field. If this field is left blank, then access is permitted from any IP address.

The screenshot displays the Linksys Administration interface for a Wireless-G VPN Router. The 'Administration' tab is selected, and the 'Management' sub-tab is active. The interface is divided into several sections: 'Router Password' (Local Router Access and Remote Router Access), 'SNMP' (Identification and Community settings), and 'UPnP'. The 'Local Router Access' section shows the default username 'admin' and password fields. The 'Remote Router Access' section has 'Remote Management' set to 'Enabled' and 'Management Port' set to '8080'. The 'SNMP' section includes fields for 'Contact', 'Device Name', 'Location', 'Get Community', 'Set Community', 'SNMP Trusted Host', and 'SNMP Trap-Community'. The 'UPnP' section has checkboxes for 'Allow User to make Configuration Changes' and 'Allow User to disable Internet Access'. The bottom of the page features 'Save Settings' and 'Cancel Changes' buttons.

Figure 6-30: Management

- **SNMP Trap-Community.** Enter the password required by the remote host computer that will receive trap messages or notices sent by the Router.
- **SNMP Trap-Destination.** Enter the IP address of the remote host computer that will receive the trap messages.

UPnP

UPnP allows Windows XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. To enable UPnP, click **Enabled**.

- **Allow User to make Configuration Changes.** When enabled, this feature allows you to make manual changes while still using the UPnP feature.
- **Allow users to disable Internet access.** When enabled, this feature allows you to prohibit any and all Internet connections.

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.

Log

The Log tab, shown in Figure 6-31, provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

Email Alert

To enable E-Mail Alert, click **Enabled**.

- **E-Mail Address for General Logs.** Enter the **E-Mail Address for General Logs** in the field.
- **E-Mail Address for Alert Logs.** Enter the **E-Mail Address for Alert Logs** in the field.
- **Return E-Mail address.** Enter the **address for the return E-Mail**.
- **E-Mail Server IP Address.** Enter the **IP Address of the E-Mail Server** in the fields.

Syslog Notification

To enable Syslog, click **Enabled**.

- **Device Name.** Enter the **Device Name** in the field.

The screenshot shows the Linksys Wireless-G VPN Router Administration tab, specifically the Log section. The interface is divided into several sections for configuration:

- Email Alert:** Includes radio buttons for **Enabled** and **Disabled**. Fields for **E-Mail Address for General Logs**, **E-Mail Address for Alert Logs**, **Return E-Mail address**, and **E-Mail Server IP Address** (with four input boxes for IP octets).
- Syslog Notification:** Includes radio buttons for **Enabled** and **Disabled**. Fields for **Device Name**, **Syslog Server IP Address** (with four input boxes for IP octets), and **Syslog Priority** (a dropdown menu).
- Notification Queue Length:** Fields for **Log Queue Length** (with a value of 20) and **Log Time Threshold** (with a value of 600 seconds).
- Alert Log:** Includes checkboxes for **Syn Flooding**, **IP Spoofing**, **Win Nuke**, **Ping Of Death**, and **Unauthorized Login Attempt** (which is checked).
- General Log:** Includes checkboxes for **System Error Messages**, **Deny Policies**, **Allow Policies**, **Content Filtering**, **Data Inspection**, **Authorized Login** (checked), and **Configuration Changes** (checked).

At the bottom of the page, there are buttons for **Save Settings** and **Cancel Changes**, and a **More...** link on the right side.

Figure 6-31: Log

- Syslog Server IP Address. Enter the **IP Address of the Syslog Server**.
- Syslog Priority. Select the **priority** from the drop-down list.

Notification Queue Length

- Log queue Length. Enter the **number** of entries in the log queue in the field.
- Log Time Threshold. Enter the **time** for the threshold in the field.

Alert Log

Select the type of attacks that you want to be alerted to. Select Syn Flooding, IP Spoofing, Win Nuke, Ping of Death, or Unauthorized Login attempt.

General Log.

Select the type of activity you would like to log. Select System Error Messages, Deny Policies, Allow Policies, Content Filtering, Data Inspection, authorized Login, or Configuration Changes.

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.

Diagnostics

Ping Test (See Figure 6-32.)

Ping Test Parameters

Ping Target IP. Enter the IP Address that you want to ping in the field.

No. of Pings. Enter the number of times that you want to ping.

Ping Size. Enter the size of the ping packets.

Ping Interval. Enter the ping interval in Milliseconds.

Ping Timeout. Enter the time in Milliseconds.

Click the **Start Test** button to start the Ping Test. Click the **Abort Test** button to stop the test. Click the **Clear Result** button to clear the results. The results of the test will display in the window.

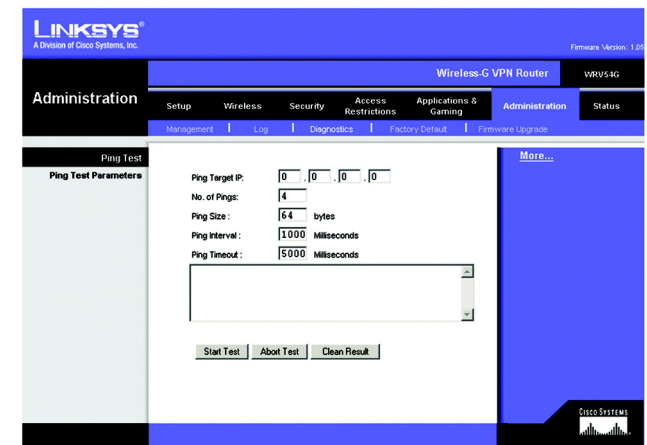


Figure 6-32: Ping Test

Factory Default (See Figure 6-33.)

If you have exhausted all other options and wish to restore the Router to its factory default settings and lose all your settings, click **Yes**.

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.

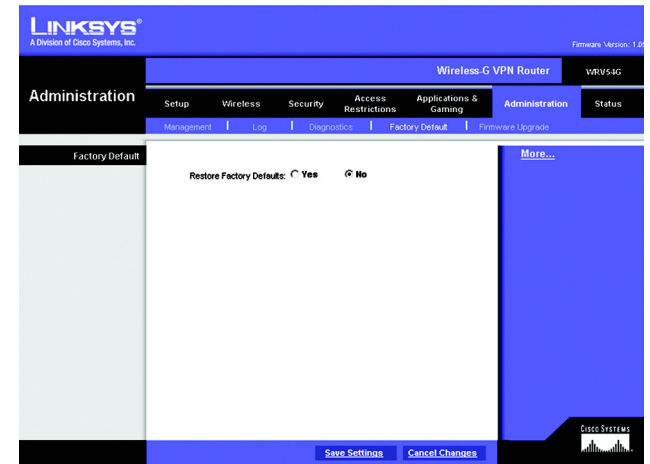


Figure 6-33: Factory Default

Firmware Upgrade (See Figure 6-34.)

To upgrade the Router's firmware:

1. Click the **Browse** button to find the firmware upgrade file that you downloaded from the Linksys website and then extracted.
2. Double-click the firmware file you downloaded and extracted. Click the **Upgrade** button, and follow the instructions there.

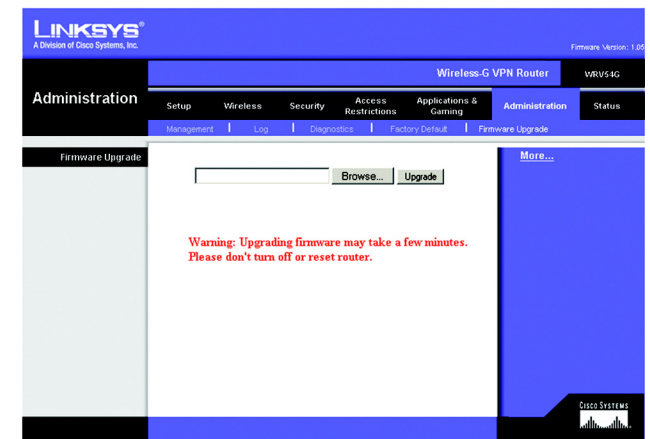


Figure 6-34: Firmware Upgrade

Status

Router

This screen displays information about your Router and its WAN (Internet) Connections. (See Figure 6-35.)

Information

The information displayed is the Hardware Version, Software Version, MAC Address, Local MAC Address, and System Up Time.

WAN Connections

The WAN Connections displayed are the Network Access, WAN IP Address, Subnet Mask, Default Gateway, and DNS.

Click the **Refresh** button if you want to Refresh your screen.

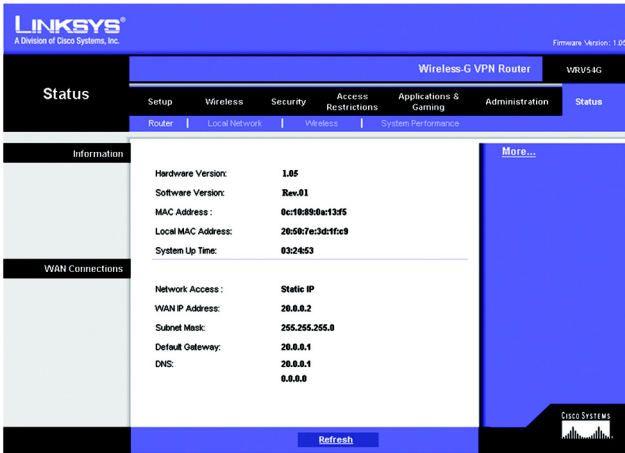


Figure 6-35: Router