Manual abstract:

and/or its affiliates in the U.S. and certain other countries. Copyright © 2006 Cisco Systems, Inc. All rights reserved. @@@@@@Look for the following items when reading this User Guide: This checkmark means there is a note of interest and is something you should pay special attention to while using the Router. This exclamation point means there is a caution or warning and is something that could damage your property or the Router. This question mark provides you with a reminder about something you might need to do while using the Router. In addition to these symbols, there are definitions for technical terms that are presented like this: word: definition. Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this: Figure 0-1: Sample Figure Description Figure numbers and descriptions can also be found in the "List of Figures" section in the "Table of Contents".

WRV200-UG-60407NC BW Wireless-G VPN Router with RangeBooster Table of Contents Chapter 1: Introduction Welcome What's in this Guide? 1 1 2 Chapter 2: Planning Your Wireless Network Network Topology Ad-Hoc versus Infrastructure Mode Network Layout 4 4 4 4 Chapter 3: Planning Your Virtual Private Network (VPN) Why do I need a VPN? What is a VPN? 6 6 7 Chapter 4: Getting to Know the Wireless-G VPN Router The Back Panel The Front Panel 9 9 10 Chapter 5: Connecting the Wireless-G VPN Router Overview Wired Connection to a PC Wireless Connection to a PC 11 11 11 12 Chapter 6: Configuring the Wireless-G VPN Router Overview How to Access the Web-based Utility The Setup Tab - Basic Setup The Setup Tab - DDNS The Setup Tab - MAC Address Clone The Setup Tab - Advanced Routing The Wireless Tab - Basic Wireless Settings The Wireless Tab - Wireless Security The Wireless Tab - Wireless Network Access The Wireless Tab - Advanced Wireless Settings The Firewall Tab - General 13 13 15 15 21 22 23 25 26 30 31 33 Wireless-G VPN Router with RangeBooster The Firewall Tab - Port Forwarding The Firewall Tab - Port Triggering The Firewall Tab - DMZ The Firewall Tab - Access Restriction The Firewall Tab - URL Filtering The VPN Tab The VPN Tab - VPN Client Access The VPN Tab - VPN Passthrough The VPN Tab - IPSec VPN The VPN Tab - VPN Summary The QoS Tab - Application-based QoS The QoS Tab - Port-based QoS The Administration Tab - Management The Administration Tab - Log The Administration Tab - Diagnostics The Administration Tab - Factory Defaults The Administration Tab - Firmware Upgrade The Administration Tab - Reboot The Status Tab - Router The Status Tab - Local Network The Status Tab - System Performance The Status Tab - VPN Clients 34 35 36 37 38 39 39 40 41 46 48 49 50 53 54 55 55 55 56 57 59 60 Appendix A: Troubleshooting Common Problems and Solutions Frequently Asked Questions 61 61 69 Appendix B: Wireless Security Security Precautions Security Threats Facing Wireless Networks 77 77 77 Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP Overview Before You Begin Using the Linksys QuickVPN Software 80 80 80 82 Wireless-G VPN Router with RangeBooster Appendix D: Configuring IPSec between a Windows 2000 or XP Computer and the Router Introduction Environment How to Establish a Secure IPSec Tunnel 84 84 84 85 Appendix E: Configuring a Gateway-to-Gateway IPSec Tunnel Overview Before You Begin Configuring the VPN Settings for the VPN Routers Configuring the Key Management Settings Configuring PC 1 and PC 2 Windows 98 or Me Instructions Windows 2000 or XP Instructions 95 95 95 96 98 99 100 101 Appendix F: Finding the MAC Address and IP Address for your Ethernet Adapter 100 Appendix G: SNMP Functions Appendix H: Upgrading Firmware Appendix I: Windows Help Appendix J: Glossary Appendix K: Specifications Appendix L: Warranty Information Appendix M: Regulatory Information Appendix N: Contact Information 102 103 104 105 110 111 112 118 Wireless-G VPN Router with RangeBooster List of Figures Figure 2-1: Network Diagram Figure 3-1: VPN Router to VPN Router Figure 3-2: Computer to VPN Router Figure 4-1: Back Panel Figure 4-2: Front Panel Figure 5-1: Connect to LAN Ports Figure 5-2: Connect to Internet Port Figure 5-3: Connect to Power Port Figure 5-4: Connect to Internet Port Figure 5-5: Connect to Power Port Figure 6-1: Login Screen Figure 6-2: Setup Tab - Automatic Configuration - DHCP Figure 6-3: Internet Connection Type - Static IP Figure 6-4: Internet Connection Type - PPPoE Figure 6-5: Internet Connection Type - PPTP Figure 6-6: Internet Connection Type - L2TP Figure 6-7: Static Table Figure 6-8: The Setup Tab - VLAN Figure 6-9: The Setup Tab - DDNS - DynDNS.org Figure 6-10: The Setup Tab - DDNS - TZO.com Figure 6-11: Setup Tab - MAC Address Clone Figure 6-12: The Setup Tab - Advanced Routing Figure 6-13: Routing Table Entry List Figure 6-14: The Wireless Tab - Basic Wireless Settings Figure 6-15: Wireless Security - WPA-Personal Figure 6-16: Wireless Security - WPA2-Personal Figure 6-17: Wireless Security - WPA Enterprise Figure 6-18: Wireless Security - WPA2 Enterprise Figure 6-19: Wireless Security - WPA2 Personal Mixed Figure 6-20: Wireless Security - WPA2 Enterprise Mixed 5 8 8 9 10 11 11 11 12 12 15 15 16 16 17 18 20 20 21 21 22 23 24 25 26 26 27 27 28 28 Wireless-G VPN Router with RangeBooster Figure 6-21: Wireless Security - RADIUS Figure 6-22: Wireless Security - WEP Figure 6-23: Wireless Tab - Wireless Network Access Figure 6-24: Networked Computers Figure 6-25: The Wireless Tab - Advanced Wireless Settings Figure 6-26: Wireless Tab - WDS Figure 6-27: The Firewall Tab - General Figure 6-28: The Firewall Tab - Port Forwarding Figure 6-29: The Firewall Tab - Port Triggering Figure 6-30: The Firewall Tab - DMZ Figure 6-31: The Firewall Tab - Access Restriction Figure 6-32: The Firewall Tab - URL Filtering Figure 6-33: The VPN Tab - VPN Client Access Figure 6-34: The VPN Tab - VPN Client Access Warning Figure 6-35: The VPN Tab - VPN Passthrough Figure 6-36: The VPN Tab - IPSec VPN Figure 6-37: Local Secure Group - Subnet and Remote Secure Group - IP Addr. Figure 6-38: Local Secure Group - IP Address and Remote Secure Group - IP Address Figure 6-39: Local Secure Group - Host and Remote Secure Group - IP Addr. Figure 6-40: Local Secure Group - IP Addr.

and Remote Secure Group - Any Figure 6-41: Key Exchange Method - Auto (IKE) Figure 6-42: Advanced Settings Figure 6-43: Global NAT Traversal Advanced Settings Figure 6-44: The VPN Tab - VPN Summary Figure 6-45: The QoS Tab - Application-based QoS -Priority Queue Figure 6-46: The QoS Tab - Application-based QoS -Bandwidth Allocation Figure 6-47: The QoS Tab - Port-based QoS Figure 6-48: The Administration Tab - Management Figure 6-49: The Administration Tab - Log Figure 6-50: The Administration Tab - Diagnostics Figure 6-51: Ping Test Figure 6-52: Traceroute Test Figure 6-53: The Administration Tab - Factory Default 29 29 30 30 31 32 33 34 35 36 37 38 39 39 40 41 41 42 42 42 43 43 45 46 48 48 49 50 53 54 54 54 55 Wireless-G VPN Router with RangeBooster Figure 6-54: The Administration Tab - Firmware Upgrade Figure 6-55: The Administration Tab - Reboot Figure 6-56: The Status Tab - Router Figure 6-57: The Status Tab - Local Network Figure 6-58: DHCP Active IP Table Figure 6-59: The Status Tab - Wireless Figure 6-60: The Status Tab - System Performance Figure 6-61: The Status Tab - VPN Clients Figure C-1: Access Restrictions - VPN Client Access Screen Figure C-2: Setup Wizard - Welcome Screen Figure C-3: QuickVPN Desktop Icon Figure C-4: QuickVPN Tray Icon - No Connection Figure C-5: QuickVPN Software - Profile Figure C-6: Connecting Figure C-7: Activating Policy Figure C-8: Verifying Network Figure C-9: QuickVPN QuickVPN Software - Status Figure C-10: QuickVPN Tray Icon - Connection Figure C-11: QuickVPN Tray Icon - No Connection Figure C-12: QuickVPN QuickVPN Software - Change Password Figure D-1: Local Security Screen Figure D-2: Rules Tab Figure D-3: IP Filter List Tab Figure D-4: IP Filter LIst Figure D-5: Filters Properties Figure D-6: New Rule Properties Figure D-7: IP Filter List Figure D-8: Filters Properties Figure D-9: New Rule Properties Figure D-10: IP Filter List Tab Figure D-11: Filter Action Tab Figure D-12: Security Methods Tab Figure D-13: Authentication Methods 55 55 56 57 57 58 59 60 80 81 82 82 82 82 82 82 83 83 83 83 85 85 85 86 86 86 87 87 87 88 88 88 89 Wireless-G VPN Router with RangeBooster Figure D-14: Preshared Key Figure D-15: New Preshared Key Figure D-16: Tunnel Setting Tab Figure D-17: Connection Type Tab Figure D-18: Properties Screen Figure D-19: IP Filter List Tab Figure D-20: Filter Action Tab Figure D-21: Authentication Methods Tab Figure D-22: Preshared Key Figure D-23: New Preshared Key Figure D-24: Tunnel Setting Tab Figure D-25: Connection Type Figure D-26: Rules Figure D-27: Local Computer Figure D-28: VPN Tab Figure E-1: Diagram of All VPN Tunnels Figure E-2: Login Screen Figure E-3: Security - VPN Screen (VPN Tunnel) Figure E-4: Security - VPN Screen (VPN Tunnel) Figure E-5: Auto (IKE) Advanced Settings Screen Figure F-1: IP Configuration Screen Figure F-2: MAC Address/Adapter Address Figure F-3: MAC Address/Physical Address Figure H-1: Upgrade Firmware 89 89 90 90 90 91 91 91 92 92 92 93 93 93 94 95 96 96 97 98 100 100 101 103 Wireless-G VPN Router with RangeBooster Wireless-G

VPN Router with RangeBooster Chapter 1: Introduction Welcome Thank you for choosing the Linksys Wireless-G VPN Router with RangeBooster.

The Wireless-G VPN Router will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely. How does the Wireless-G VPN Router do all of this? A router is a device that allows access to an Internet connection over a network. With the Wireless-G VPN Router, this access can be shared over the four switched ports or via the wireless network, broadcast at either 11Mbps for Wireless-B or 54Mbps for Wireless-G. To protect your data and privacy, the Wireless-G VPN Router can encrypt all wireless transmissions with up to 128-bit WEP encryption and supports the WPA standard, which provides greater security opportunities.

The Router also has a powerful Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) technology to protect your PCs against intruders and most known Internet attacks. Its Virtual Private Network (VPN) function creates encrypted "tunnels" through the Internet so up to 50 remote or traveling users can securely connect to your office network from off-site, or users in your branch office can connect to a corporate network. All of these security features, as well as full configurability, are accessed through the easy-to-use browser-based utility. But what does all of this mean? Networks are useful tools for sharing computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun. PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired". PCs equipped with wireless cards or adapters can communicate without cumbersome cables.

By sharing the same wireless settings, within their transmission radius, they form a wireless network. The Wireless-G VPN Router bridges wireless networks of both 802.11b and 802.11g standards and wired networks, allowing them to communicate with each other. With your networks all connected, wired, wireless, and the Internet, you can now share files and Internet access--and even play games. All the while, the Wireless-G VPN Router protects your networks from unauthorized and unwelcome users. vpn (virtual private network): A security measure to protect data as it leaves one network and goes to another over the Internet 802.11b: an IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz 802.11g: an IEEE wiremiddot; Appendix J: Glossary This appendix gives a brief glossary of terms frequently used in networking.

· Appendix K: Specifications This appendix provides the technical specifications for the Router. · Appendix L: Warranty Information This appendix supplies the warranty information for the Router. · Appendix M: Regulatory Information This appendix supplies the regulatory information regarding the Router. · Appendix N: Contact Information This appendix provides contact information for a variety of Linksys resources, including Technical Support. Chapter 1: Introduction What's in this Guide? 3 Wireless-G VPN Router with RangeBooster Chapter 2: Planning Your Wireless Network Network Topology A wireless local area network (WLAN) is exactly like a regular local area network (LAN), except that each computer in the WLAN uses a wireless device to connect to the network.

Computers in a WLAN share the same frequency channel and SSID, which is an identification name shared by the wireless devices belonging to the same wireless network. network: a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users lan (local area network): The computers and networking products that make up the network in your home or office ssid: your wireless network's name ad-hoc: a group of wireless devices communicating directly to each other (peer-to-peer) without the use of an access point infrastructure: a wireless network that is bridged to a wired network via an access point adapter: a device that adds network functionality to your PC ethernet: IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium access point: a device that allows wirelessequipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network Ad-Hoc versus Infrastructure Mode Unlike wired networks, wireless networks have two different modes in which they may be set up: infrastructure and ad-hoc. An infrastructure configuration is a WLAN and wired LAN communicating to each other through an access point. An ad-hoc configuration is wireless-equipped computers communicating directly with each other. Choosing between these two modes depends on whether or not the wireless network needs to share data or peripherals with a wired network or not. If the computers on the wireless network need to be accessible by a wired network or need to share a peripheral, such as a printer, with the wired network computers, the wireless network should be set up in Infrastructure mode. The basis of Infrastructure mode centers around an access point or wireless router, such as the Wireless-G VPN Router, which serves as the main point of communications in a wireless network. The Router transmits data to PCs equipped with wireless network adapters, which can roam within a certain radial range of the Router. You can arrange the Router and multiple access points to work in succession to extend the roaming range, and you can set up your wireless network to communicate with your Ethernet hardware as well. If the wireless network is relatively small and needs to share resources only with the other computers on the wireless network, then the Ad-Hoc mode can be used. Ad-Hoc mode allows computers equipped with wireless transmitters and receivers to communicate directly with each other, eliminating the need for a wireless router or access point. The drawback of this mode is that in Ad-Hoc mode, wireless-equipped computers are not able to communicate with computers on a wired network. And, of course, communication between the wirelessequipped computers is limited by the distance and interference directly between them. Network Layout The Wireless-G VPN Router has been specifically designed for use with both your 802.

11b and 802.11g products. Now, products using these standards can communicate with each other. Chapter 2: Planning Your Wireless Network Network Topology 4 Wireless-G VPN Router with RangeBooster The Wireless-G VPN Router is compatible with all 802.11b and 802.11g adapters, such as the Notebook Adapters (WPC54G, WPC11) for your laptop computers, PCI Adapter (WMP54G, WMP11) for your desktop PC, and USB Adapter (WUSB54G, WUSB11) when you want to enjoy USB connectivity. The Router will also communicate with the Wireless PrintServer (WPS54GU2, WPS11) and Wireless Ethernet Bridges (WET54G, WET11).

When you wish to connect your wireless network with your wired network, you can use the Router's three LAN ports. To add more ports, any of the Router's LAN ports can be connected to any of Linksys's switches (such as the EZXS55W or EZXS88W). With these, and many other, Linksys products, your networking options are limitless.

Go to the Linksys website at www.linksys.com for more information about products that work with the Wireless-G VPN Router with RangeBooster. Figure 2-1: Network Diagram Chapter 2: Planning Your Wireless Network Network Layout 5 Wireless-G VPN Router with RangeBooster Chapter 3: Planning Your Virtual Private Network (VPN) Why do I need a VPN? Computer networking provides a flexibility not available when using an archaic, paper-based system. With this flexibility, however, comes an increased risk in security.

This is why firewalls were first introduced. Firewalls help to protect data inside of a local network. But what do you do once information is sent outside of your local network, when e-mails are sent to their destination, or when you have to connect to your company's network when you are out on the road? How is your data protected? That is when a VPN can help. VPNs are called Virtual Private Networks because they secure data moving outside of your network as if it were still within that network. When data is sent out across the Internet from your computer, it is always open to attacks.

You may already have a firewall, which will help protect data moving around or held within your network from being corrupted or intercepted by entities outside of your network, but once data moves outside of your network--when you send data to someone via e-mail or communicate with an individual over the Internet--the firewall will no longer protect that data. At this point, your data becomes open to hackers using a variety of methods to steal not only the data you are transmitting but also your network login and security data. Some of the most common methods are as follows: 1) MAC Address Spoofing Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user. 2) Data Sniffing Data "sniffing" is a method used by hackers to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text. 3) Man in the middle attacks Once the hacker has either sniffed or spoofed enough information, he can now perform a "man in the middle" attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the Chapter 3: Planning Your Virtual Private Network (VPN) Why do I need a VPN? vpn (virtual private network): a security measure to protect data as it leaves one network and goes to another over the Internet packet: a unit of data sent over a network 6 Wireless-G VPN Router with RangeBooster data to a new destination.

Even though the data is not received by its intended recipient, it appears that way to the person sending the data. These are only a few of the methods hackers use and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet will often pass through many different servers around the world before reaching its final destination. That's a long way to go for unsecured data and this is when a VPN serves its purpose. What is a VPN? A VPN, or Virtual Private Network, is a connection between two endpoints--a VPN Router, for instance--in different networks that allows private data to be sent securely over a shared or public network, such as the Internet. This establishes a private network that can send data securely between these two locations or networks. This is done by creating a "tunnel". A VPN tunnel connects the two PCs or networks and allows data to be transmitted over the Internet as if it were still within those networks. Not a literal tunnel, it is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques--IPSec, short for IP Security--the VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. Virtual Private Networking can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN Router using any computer with the Linksys VPN client software.) There are two basic ways to create a VPN connection: · VPN Router to VPN Router · Computer (using the Linksys VPN client software) to VPN Router IMPORTANT: You must have at least one VPN Router on one end of the VPN tunnel. At the other end of the VPN tunnel, you must have a second VPN Router or a computer with the Linksys VPN client software.

The VPN Router creates a "tunnel" or channel between two endpoints, so that data transmissions between them are secure. A computer with the Linksys VPN client software can be one of the two endpoints (refer to "Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP"). If you choose not to run the VPN client software, any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN Router to create a VPN tunnel using IPSec (refer to "Appendix D: Configuring IPSec between a Windows 2000 or XP PC Chapter 3: Planning Your Virtual Private Network (VPN) What is a VPN? encryption: encoding data transmitted in a network ip (internet protocol): a protocol used to send data over a network software: instructions for the computer 7 Wireless-G VPN Router with RangeBooster and the Router"). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed. VPN Router to VPN Router An example of a VPN Router-to-VPN Router VPN would be as follows.

At home, a telecommuter uses his VPN Router for his always-on Internet connection. His router is configured with his office's VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected.

For more information, refer to "Appendix E: Configuring VPN Tunnels." Computer (using the Linksys VPN client software) to VPN Router The following is an example of a computer-to-VPN Router VPN. In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has the Linksys VPN client software, which is configured with her office's IP address. She accesses the Linksys VPN client software and connects to the VPN Router at the central office.

As VPNs utilize the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office's network, as if she were physically connected. For additional information and instructions about creating your own VPN, please visit Linksys's website at www.linksys.com. You can also refer to "Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP", "Appendix D: Configuring IPSec between a Windows 2000 or XP PC and the Router," and "Appendix E: Configuring VPN Tunnels." Figure 3-1: VPN Router to VPN Router Figure 3-2: Computer to VPN Router Chapter 3: Planning Your Virtual Private Network (VPN) What is a VPN? 8 Wireless-G VPN Router with RangeBooster Chapter 4: Getting to Know the Wireless-G VPN Router The Back Panel The Router's ports, where a network cable is connected, are located on the back panel. Power The Power port is where you will connect the power adapter. Figure 4-1: Back Panel Reset Button There are two ways to reset the Router's factory defaults. Either press the Reset Button, for approximately five seconds, or restore the defaults from the Administration tab - Factory Defaults in the Router's Web-based Utility. The Ethernet ports connect to your PCs and other network devices. The Internet port connects to your cable or DSL modem. Ethernet (1-4) Internet IMPORTANT: If you reset the Router, all of your settings, including Internet connection, wireless, and security, will be deleted and replaced with the factory defaults. Do not reset the Router if you want to retain these settings. Chapter 4: Getting to Know the Wireless-G VPN Router The Back Panel 9 Wireless-G VPN Router with RangeBooster The Front Panel The Router's LEDs, where information about network activity is displayed, are located on the front panel. Figure 4-2: Front Panel Power DMZ Green. The Power LED lights up when the Router is powered on. Red. The DMZ LED lights up when the Router has an available DMZ port. If the LED is flashing, the Router is sending or receiving data over the DMZ port. Green. The Internet LED lights up when the Router is connected to your cable or DSL modem. If the LED is flashing, the Router is sending or receiving data over the Internet port. Green. The Wireless-G LED lights whenever there is a successful wireless connection. If the LED is flashing, the Router is actively sending or receiving data over the wireless network. Green. The LAN LED serves two purposes. If the LED is solidly lit, the Router is connected to a device through the corresponding port (LAN 1, 2, or 3). If the LED is flashing, the Router is sending or receiving data over that port.

Internet Wireless Ethernet (1-4) Chapter 4: Getting to Know the Wireless-G VPN Router The Front Panel 10 Wireless-G VPN Router with RangeBooster Chapter 5: Connecting the Wireless-G VPN Router Overview To begin installation of the Router, you will connect the Router to your PCs, other network devices, and cable or DSL modem. If you want to use a PC with an Ethernet adapter to configure the Router, go to "Wired Connection to a PC." If you want to use a PC with a wireless adapter to configure the Router, go to "Wireless Connection to a PC." Wired Connection to a PC 1. Make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem. 2. Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the Router. Then connect the other end to an Ethernet port on a PC. 3. Repeat step 2 to connect additional PCs or other network devices to the Router.
4. Connect a different Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel. 5. Power on the cable or DSL modem. NOTE: You should always plug the Router's power adapter into a power strip with surge protection.
6. Connect the power adapter to the Router's Power port, and then plug the power adapter into a power outlet. The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting.
" 7. Power on one of your PCs that is connected to the Router. The Router's hardware installation is now complete. Go to "Chapter 6: Configuring the Wireless-G VPN Router with RangeBooster." Figure 5-3: Connect to Power Port Chapter 5: Connecting the Wireless-G VPN Router Overview Figure 5-1: Connect to LAN Ports Figure 5-2: Connect to Internet Port 11 Wireless-G VPN Router with RangeBooster Wireless Connection to a PC If you want to use a wireless connection to access the Router, follow these instructions: 1. Make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem. 2. Connect an Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel. 3. Power on the cable or DSL modem.

4. Connect the power adapter to the Router's Power port, and then plug the power adapter into a power outlet. NOTE: You should always plug the Router's power adapter into a power strip with surge protection. Figure 5-4: Connect to Internet Port The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting." 5. Power on one of the PCs on your wireless network(s). 6. For initial access to the Router through a wireless connection, make sure the PC's wireless adapter has its SSID set to linksys (the Router's default setting) and its WEP encryption disabled.
After you have accessed the Router, you can change the Router and this PC's adapter settings to match your usual network settings. Figure 5-5: Connect to Power Port The Router's hardware installation is now complete. Go to "Chapter 6: Configuring the Wireless-G VPN Router with RangeBooster." NOTE: You should change the SSID from its default, linksys, and enable security after you have accessed the Router. Chapter 5: Connecting the Wireless-G VPN Router Wireless Connection to a PC 12 Wireless-G VPN Router with RangeBooster Chapter 6: Configuring the Wireless-G VPN Router Overview Linksys recommends using the Setup CD-ROM for first-time installation of the Router.

If you do not wish to run the Setup Wizard on the Setup CD-ROM, then follow the steps in this chapter and use the Router's Web-based Utility to configure the Router. For advanced users, you may configure the Router's advanced settings through the Web-based Utility. This chapter will describe each web page in the Utility and each page's key functions. The Utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users only have to use the following screens of the Utility: Basic Setup.

On the Basic Setup screen, enter the settings provided by your ISP. Management. Click the Administration tab and then the Management tab. The Router's default password is admin. To secure the Router, change the Password from its default. There are seven main tabs: Setup, Wireless, Firewall, VPN, QoS, Administration, and Status. Additional tabs will be available after you click one of the main tabs. NOTE: When first installing the Router, you should use the Setup Wizard on the Setup CDROM. If you want to configure advanced settings, use this chapter to learn about the Web-based Utility. HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol.

Refer to "Appendix I: Windows Help" for more information on TCP/IP. NOTE: For added security, you should change the password through the Administration screen of the Web-based Utility. Setup · Basic Setup. Enter the Internet connection and network settings on this screen. · VLAN. The Router provides a port-based VLAN feature. · DDNS. On this screen, enable the Router's Dynamic Domain Name System (DDNS) feature. · MAC Address Clone. If you need to clone a MAC address onto the Router, use this screen.

· Advanced Routing. On this screen, configure the dynamic and static routing configuration. nat (network address translation): NAT technology translates IP addresses of a local area network to a different IP address for the Internet Wireless · Basic Wireless Settings. You can choose your wireless network settings on this screen. · Wireless Security.

You can choose your wireless security settings on this screen. Chapter 6: Configuring the Wireless-G VPN Router Overview 13 Wireless-G VPN Router with RangeBooster · Wireless Network Access. This screen displays your network access list. · Advanced Wireless Settings. For advanced users, you can alter data transmission settings on this screen.

· WDS. This tab is used for Wireless Distribution System (WDS). Firewall · General. On this screen, you can configure a variety of filters to enhance the security of your network. · Port Forwarding. To set up public services or other specialized Internet applications on your network, click this tab. · Port Triggering. To set up triggered ranges and forwarded ranges for Internet applications, click this tab. · DMZ. Click this tab to allow one local user to be exposed to the Internet for use of special-purpose services.

· Access Restriction. This tab allows you to block or allow specific kinds of Internet usage and traffic during specific days and times. · URL Filtering. This tab allows you to create an URL Filtering policy. VPN · VPN Client Access. Use this screen to designate VPN clients and their passwords. · VPN Passthrough. This tab is used to allow VPN tunnels to pass through the Router's firewall using IPSec, L2TP, or PPTP protocols. · IPSec VPN. The VPN Router creates a tunnel or secure channel between two endpoints, so that the transmitted data or information between these endpoints is secure.

· VPN Summary. This page summarizes the comprehensive details of IPSec VPN Tunnels. QoS · Application-based QoS. This involves Internet traffic, which may involve demanding, real-time applications, such as videoconferencing. · Port-based QoS.

This ensures better service to a specific LAN port. Chapter 6: Configuring the Wireless-G VPN Router Overview 14 Wireless-G VPN Router with RangeBooster Administration · Management. Alter the Router's password, its access privileges, SNMP settings, and UPnP settings. · Log. If you want to view or save activity logs, click this tab.

· Diagnostics. Use this screen to check the connection between the Router and a PC. · Factory Defaults. If you want to restore the Router's factory defaults, then use this screen. · Firmware Upgrade. Click this tab if you want to upgrade the Router's firmware. · Reboot. Use this to restart the Router. Status · Router. This screen provides status information about the Router.

· Local Network. This provides status information about the local network. · Wireless. Status information about the wireless network is displayed here. · System Performance. Status information is provided for all network traffic. · VPN Clients. This screen provides status information about the Router's VPN clients. Figure 6-1: Login Screen How to Access the Web-based Utility To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, 192.168.

1.1, in the Address field. Then press Enter. A password request page will appear. (Windows XP users will see a similar screen.

) Enter admin (the default user name) in the User Name field, and enter admin (the default password) in the Password field. Then click the OK . Make the necessary changes through the Utility. When you have finished making changes to a screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. Help information is shown on the right-hand side of a screen.

For additional information, click More. The Setup Tab - Basic Setup The first screen that appears is the Basic Setup tab. This tab allows you to change the Router's general settings. Chapter 6: Configuring the Wireless-G VPN Router How to Access the Web-based Utility Figure 6-2: Setup Tab - Automatic Configuration - DHCP 15 Wireless-G VPN Router with RangeBooster Internet Setup The Internet Setup section configures the Router for your Internet connection type. This information can be obtained from your ISP. Internet Connection Type The Router supports four connection types: Automatic Configuration - DHCP (the default connection type), PPPoE, Static IP, and PPTP. Each Basic Setup screen and available features will differ depending on what kind of connection type you select. Figure 6-3: Internet Connection Type - Static IP Automatic Configuration - DHCP By default, the Router's Configuration Type is set to Automatic Configuration - DHCP, and it should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address. static ip address: a fixed address assigned to a computer or device connected to a network. subnet mask: an address code that determines the size of the network default gateway: a device that forwards Internet traffic from your local area network Static IP If you are required to use a permanent IP address to connect to the Internet, then select Static IP.

IP Address. This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here. Subnet Mask. This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask. Default Gateway. Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address. Primary DNS (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. Figure 6-4: Internet Connection Type - PPPoE PPPoE Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE. pppoe: a type of broadband connection that provides authentication (username and password) in addition to data transport Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - Basic Setup 16 Wireless-G VPN Router with RangeBooster User Name and Password.

Enter the User Name and Password provided by your ISP. Then, enter the Password again to confirm it. Auth Type: Select from two authentication protocols as required by your ISP: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time).

If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes.

Figure 6-5: Internet Connection Type - PPTP PPTP Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe and Israel only. IP Address. This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here. Subnet Mask. This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask. Default Gateway. Your ISP will provide you with the Default Gateway Address. PPPTP Server IP.

Enter the IP address of the PPPTP server. User Name and Password. Enter the User Name and Password provided by your ISP. Auth Type: Select from two authentication protocols as required by your ISP: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Connect on Demand: Max Idle Time.

You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - Basic Setup 17 Wireless-G VPN Router with RangeBooster due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. Keep Alive Option: Redial Period.

If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. L2TP Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries. Check with your ISP for the necessary setup information. IP Address.

This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here. Subnet Mask. This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask. Default Gateway. Your ISP will provide you with the Default Gateway Address. L2TP Server IP. Enter the IP address of the L2TP server. User Name and Password.

Enter the User Name and Password provided by your ISP. Auth Type: Select from two authentication protocols as required by your ISP: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Connect on Demand and Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specific period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects. Keep Alive and Redial Period. This option keeps your Internet access connected indefinitely, even when it sits idle.

If you select this option, the Router will periodically check your Internet connection. If the connection Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - Basic Setup Figure 6-6: Internet Connection Type - L2TP 18 Wireless-G VPN Router with RangeBooster is down, then the Router will automatically re-establish the connection. To use this option, click the radio button next to Keep Alive. The default Redial Period is 30 seconds. Click the Save Settings button. Then click the Status tab, and click the Connect button.

Optional Settings (Required by some ISPs) Some of these settings may be required by your ISP. Verify with your ISP before making any changes. Host Name and Domain Name. These fields allow you to supply a host and domain name for the Router.

Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work. MTU. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select Enabled and enter the value desired. It is recommended that you leave this value in the 1200 to 1500 range. For most DSL users, it is recommended to use the value 1492. By default, MTU is set at 1500 when disabled. LAN Setup The LAN Setup section allows you to change the Router's local network settings.

LAN IP The Router's Local IP Address and Subnet Mask are shown here. In most cases, you can keep the defaults. Local IP Address. The default value is 192.168.

1.1. Subnet Mask. The default value is 255.255.

255.0. Network Address Server Settings (DHCP) The Router can be used as your network's DHCP (Dynamic Host Configuration Protocol) server, which automatically assigns an IP address to each PC on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server. Local DHCP Server. DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to Disabled. If you disable DHCP, assign a static IP address to the Router. Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - Basic Setup 19 Wireless-G VPN Router with RangeBooster Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses.

This value must be 192.168.1. 2 or greater, but smaller than 192.168.1.254, because the default IP address for the Router is 192.168.1.1, and 192. 168.1.255 is the broadcast IP address. Number of Address. Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users. IP Address Range.

The range of DHCP addresses is displayed here. Client Lease Time. This is the amount of time a DHCP client can keep the assigned IP address before it sends a renewal request to the DHCP server. The Static Table shows the mapping of MAC addresses to IP addresses. To use this feature, enter the Static IP Address and MAC address in the fields, then click Add. To edit an entry, highlight the entry in the table, click the Edit button, make your changes in the fields, then click Add. To remove an entry, highlight the entry, then click Remove. Manual DNS Setting. To enter the DNS IP addresses manually, enter up to two in the fields provided. Figure 6-7: Static Table Time Setting This is where you set the time for the Router.

You can set the time and date manually or automatically. Manually. Select the date from the Date drop-down menus. Then enter the time in the Time fields. Automatically. Select your time zone from the Time Zone drop-down menu. If you want to enable the Automatic Daylight Savings feature, click the Enabled radio button. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. The Setup Tab - VLAN The Router provides a port-based VLAN feature. Port-based VLAN.

Select Enabled to enable the feature. When enabled, and a VLAN is selected, VLAN1 will be enabled as a default VLAN, so you will have two VLANs. Select Disabled to disable the feature. When this feature is disabled, all LAN ports are on the same LAN. Number of VLAN.

Select the number of the VLAN from the drop-down menu. Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - Basic Setup Figure 6-8: The Setup Tab - VLAN 20 Wireless-G VPN Router with RangeBooster VLAN No. Select the VLAN number to associate with the desired port. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. 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 and your ISP does not give you a fixed IP address. 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. ddns: allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address DDNS If your DDNS service is provided by DynDNS.

org, then select DynDNS.org in 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. Figure 6-9: The Setup Tab - DDNS - DynDNS.org 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.

When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. For help information, click More. TZO.com Email, TZO Password Key, and Domain Name. Enter the Email Address, TZO Password Key, and Domain Name of the service you set up with TZO.

Figure 6-10: The Setup Tab - DDNS - TZO.com Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, this will change. Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - DDNS 21 Wireless-G VPN Router with RangeBooster Status. The status of the DDNS service connection is displayed here. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. The Setup Tab - MAC Address Clone The Router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. Some ISPs 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 using the MAC Address Clone feature.

If you need to find your adapter's MAC address, follow the instructions in "Appendix F: Finding the MAC Address and IP Address for Your Ethernet Adapter." MAC Address Clone To use MAC address cloning, select Enabled.

MAC Clone Address. Enter the MAC Address registered with your ISP. Then click the Save Settings button. Clone My MAC Address. If you want to clone the MAC address of the PC you are currently using to configure the Router, then click the Clone My MAC Address button. The Router will automatically detect your PC's MAC address, so you do NOT have to call your ISP to change the registered MAC address to the Router's MAC address. It is recommended that the PC registered with the ISP is used to open the MAC Address Clone tab. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes.

For help information, click More. Figure 6-11: Setup Tab - MAC Address Clone mac address: the unique address that a manufacturer assigns to each networking device. Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - MAC Address Clone 22 Wireless-G VPN Router with RangeBooster The Setup Tab - Advanced Routing The Advanced Routing screen allows you to configure the dynamic and static routing settings. Advanced Routing Operation Mode. Select Gateway or Router from the drop-down menu.

If this Router is hosting your network's connection to the Internet, keep the default, Gateway, which will also enable NAT. If you have a different router hosting your Internet connection, then select Router. Dynamic Routing With Dynamic Routing you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

Dynamic Routing (RIP). To use dynamic routing, click the Enabled radio button. Receive RIP Versions. To use dynamic routing for reception of network data, select the protocol you want: RIPv1 or RIPv2. Transmit RIP Versions. To use dynamic routing for transmission of network data, select the protocol you want: RIPv1 or RIPv2. Figure 6-12: The Setup Tab - Advanced Routing Static Routing If the Router is connected to more than one network, you can configure static routes to direct packets to the destination network (A static route is a pre-determined pathway that a packet must travel to reach a specific host or network.) To create a static route, change the following settings: Route Entries. Select the number of the static route from the drop-down menu. The Router supports up to 5 static route entries.

Delete This Entry. If you need to delete a route, select its number from the drop-down menu, and click the Delete This Entry button. Enter Router Name. Enter the name of your Router. LAN IP Address. The LAN IP Address 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 Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - Advanced Routing 23 Wireless-G VPN Router with RangeBooster 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.

1.1. Based on this address, the address of the routed network is 192.168.1, with the last digit determining the Router's place on the network. Therefore you would enter the IP address 192.168.1.0 if you wanted to route to the Router's entire network, rather than just to the Router. Subnet Mask. The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion. Take, for example, a network in which the Subnet Mask is 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. Gateway. Enter the IP address of the gateway device that allows for contact between the Router and the remote network or host. Interface. Select LAN & Wireless or Internet, depending on the location of the static route's final destination.

Show Routing Table. Click the Show Routing Table button to open a screen displaying how packets are routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click the Refresh button to update the information. Click the Close button to exit this screen. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. For help information, click More. Figure 6-13: Routing Table Entry List Chapter 6: Configuring the Wireless-G VPN Router The Setup Tab - Advanced Routing 24 Wireless-G VPN Router with RangeBooster The Wireless Tab - Basic Wireless Settings The basic settings for wireless networking are configured on this screen. Wireless Network Wireless 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 G-Only. If you have only 802.11b devices, select B-Only. If you do not have any 802.11g and 802.11b devices in your network, select Disable.

Wireless Network Name (SSID). The SSID is the network name shared among all points 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 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (linksys-g) to a unique name. TX Rate Limitation. 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 and the Router will negotiate the connection speed between the Router and a wireless client by this rate. Wireless 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, Enable. If you do not want to broadcast the Router's SSID, then select Disabled. WMM. WMM (Wi-Fi Multimedia) is a component of the IEEE 802.11e wireless LAN standard for quality of service (OoS). It specifically supports priority tagging and queuing. Click the WMM check box to enable WMM. Wireless Channel. Select the appropriate channel from the drop-down menu.

All devices in your wireless network must transmit using the same channel in order to function correctly. You may need to change the wireless channel to improve the communication quality. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes.

Help information is shown on the right-hand side of a screen. For additional information, click More.
Figure 6-14: The Wireless Tab - Basic Wireless Settings Chapter 6: Configuring the Wireless-G VPN Router The Wireless Tab - Basic Wireless Settings 25 Wireless-G VPN Router with RangeBooster The Wireless Tab - Wireless Security The Wireless Security settings configure the security of your wireless network. There are eight wireless security mode options supported by the Router: WPA-Personal, WPA2-Personal, WPA Enterprise, WPA2 Enterprise, WPA2Personal-Mixed, WPA2-Enterprise Mixed, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) Select the appropriate security mode for your network; all devices on your network must use the same security mode and settings to work correctly.
For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security." Select SSID. Select the SSID that you want to apply the wireless security settings to. Allow PCs on the same wireless network name (SSID) to see each other. This feature is enabled by default. Wireless PCs that are associated to the same Network Name (SSID), can see and transfer files between each other. By disabling this feature, Wireless PCs will not be able to see each other. This feature is very useful when setting up a wireless hotspot location. Figure 6-15: Wireless Security - WPA-Personal wpa (wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server WPA-Personal. WPA gives you two encryption methods with dynamic encryption keys.

Select TKIP or AES from the Enryption drop-down menu. Enter a Shared Secret (Pre-Shared Key) of 8-32 characters. Then enter the Key Renewal, which instructs the Router how often it should change the encryption keys. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click More. WPA2-Personal. WPA2 gives you the encryption method AES. Enter a Shared Secret of 8-32 characters. Then enter the Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys.
When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click More. Figure 6-16: Wireless Security - WPA2-Personal Chapter 6: Configuring the Wireless-G VPN Router The Wireless Tab - Wireless Security 26 Wireless-G VPN Router with RangeBooster WPA Enterprise. This option features WPA used in coordination with a RADIUS server.
(This should only be used when a RADIUS server is connected to the Router.) Enter the RADIUS server's IP address. Select TKIP or AES from the WPA Algorithm drop-down menu. Enter the RADIUS server's port number, along with the Shared Secret key, which is the key shared between the Router and the server. Last, enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.
When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click More. Figure 6-17: Wireless Security - WPA Enterprise radius: a protocol that uses an authentication server to control network access WPA2 Enterprise. This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Enter the RADIUS server's IP address. Enter the RADIUS server's port number, along with the Shared Secret key, which is the key shared between the Router and the server. Last, enter the Key Renewal period, which instructs the Router how often it should change the encryption keys. When you have finished making changes to the screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes.

Help information is shown on the right-hand side of a screen. For additional information, click More. Figure 6-18: Wireless Security - WPA2 Enterprise Chapter 6: Configuring the Wireless-G VPN Router The Wireless Tab - Wireless Security 27 Wireless-G VPN Router with RangeBooster WPA2 Personal Mixed. WPA2 Personal Mixed gives you either WPA-Personal (TKIP) or PSK2 (AES) encryption. Enter a Shared Secret of 8-63 characters. Then enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. Figure 6-19: Wireless Security - WPA2 Personal Mixed WPA2 Enterprise Mixed. This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Enter the RADIUS server's IP address and port number, along with the shared secret (authentication key) shared by the Router and the server. Last, enter the Key Renewal period, which instructs the Router how often it should change the encryption keys. Figure 6-20: Wireless Security - WPA2 Enterprise Mixed Chapter 6: Configuring the Wireless-G VPN Router The Wireless Tab - Wireless Security 28 Wireless-G VPN Router with RangeBooster RADIUS. This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) First, enter the RADIUS server's IP address and port number in the RADIUS Server IP Address and RADIUS Server Port fields.
Enter the key shared between the Router and the server in the Shared Secret field. To indicate which WEP key to use, select the appropriate Default Transmit Key number. Then, select the level of WEP encryption, 64 bits 10 hex digits or 128 bits 26 hex digits. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance. Instead of manually entering WEP keys, you can enter a Passphrase to generate one or more WEP keys.
The Passphrase is case-sensitive and should have no more than 32 alphanumeric characters. 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(s) manually, then enter it in the Key 1-4 field(s). (Do not leave a 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.