Manual abstract:

and/or its affiliates in the U.S. and certain other countries. Copyright © 2003 Cisco Systems, Inc. All rights reserved. @@@@@@The ADSL Modem function gives you a blazing fast connection to the Internet, far faster than a dial-up, and without tying up your phone line. Connect your computers to the Gateway via the built-in 4-port 10/100 Ethernet Switch to jump start your home network. You can share files, printers, hard drive space and other resources, or play head-to-head computer games. Attach four computers directly, or connect more hubs and switches to create as big a network as you need. The built-in Wireless-G (802.

11g) Access Point allows up to 32 wireless devices to connect to your network at a blazing 54Mbps, without running cables through the house. It's also compatible with Wireless-B (802.11b) devices, at 11Mbps. The Gateway ties it all together and lets your whole network share that high-speed Internet connection. To protect your data and privacy, the Wireless-G ADSL Gateway features an advanced firewall to keep Internet intruders and attackers out. Wireless transmissions can be protected by powerful data encryption. Safeguard your family with Parental Control features like Internet Access Time Limits and Key Word Blocking. Configuration is a snap with any web browser. With the Linksys Wireless-G ADSL Gateway at the heart of your home network, you're connected to the future. Chapter 1: Introduction Welcome 1 Wireless-G ADSL Gateway What's in this Guide? This user guide covers the steps for setting up and using the Wireless-G ADSL Gateway.

· Chapter 1: Introduction This chapter describes the Wireless-G ADSL Gateway Wireless-G ADSL Gateway applications and this User Guide. · Chapter 2: Planning your Network This chapter describes the basics of networking. · Chapter 3: Getting to Know the Wireless-G ADSL Gateway This chapter describes the physical features of the Gateway. · Chapter 4: Connecting the Wireless-G ADSL Gateway This chapter instructs you on how to connect the Gateway to your network. · Chapter 5: Configuring the Gateway This chapter explains how to use the Web-Based Utility to configure the settings on the Gateway. · Appendix A: Troubleshooting This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G ADSL Gateway. · Appendix B: Wireless Security This appendix explains the risks of wireless networking and some solutions to reduce the risks. · Appendix C: Configuring IPSec between a Windows 2000 Computer and the Gateway This appendix instructs you on how to establish a secure IPSec tunnel using preshared keys to join a private network inside the VPN Gateway and a Windows 2000 or XP computer. · Appendix D: Upgrading Firmware This appendix instructs you on how to upgrade the firmware on your Gateway if you should need to do so. · Appendix E: Finding the MAC Address and IP Address for your Ethernet Adapter.

This appendix describes how to find the MAC address for your computer's Ethenet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Gateway. · Appendix F: Glossary This appendix gives a brief glossary of terms frequently used in networking. Chapter 1: Introduction What's in this Guide? 2 Wireless-G ADSL Gateway · Appendix G: Specifications This appendix provides the technical specifications for the Gateway. · Appendix H: Warranty Information This appendix supplies the warranty information for the Gateway. · Appendix I: Regulatory Information This appendix supplies the regulatory information regarding the Gateway. · Appendix J: 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 ADSL Gateway Chapter 2: Planning your Network The Gateway's Functions A Gateway is a network device that connects two networks together. In this instance, the Gateway connects your Local Area Network (LAN), or the group of computers in your home or office, to the Internet. The Gateway processes and regulates the data that travels between these two networks. The Gateway's NAT feature protects your network of computers so users on the public, Internet side cannot "see" your computers.

This is how your network remains private. The Gateway protects your network by inspecting every packet coming in through the Internet port before delivery to the appropriate computer on your network. The Gateway inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate computer on the LAN side. Remember that the Gateway's ports connect to two sides. The LAN ports connect to the LAN, and the ADSL port connects to the Internet.

The LAN ports transmit data at 10/100Mbps. IP Addresses What's an IP Address? IP stands for Internet Protocol. Every device on an IP-based network, including computers, print servers, and Gateways, requires an IP address to identify its "location," or address, on the network. This applies to both the Internet and LAN connections. There are two ways of assigning an IP address to your network devices.

You can assign static IP addresses or use the Gateway to assign IP addresses dynamically. Figure 2-1: Network LAN: the computers and networking products that make up your local network Static IP Addresses A static IP address is a fixed IP address that you assign manually to a computer or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses must be unique and are commonly used with network devices such as server computers or print servers. NOTE: Since the Gateway is a device that connects two networks, it needs two IP addresses--one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address." Since the Gateway uses NAT technology, the only IP address that can be seen from the Internet for your network is the Gateway's Internet IP address. However, even this Internet IP address can be blocked, so that the Gateway and network seem invisible to the Internet-- see the Block WAN Requests description under Security in "Chapter 5: Configuring the Gateway." 4 Chapter 2: Planning your Network The Gateway's Functions Wireless-G ADSL Gateway Since you use the Gateway to share your DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Gateway.

You can get that information from your ISP.

Dynamic IP Addresses A dynamic IP address is automatically assigned to a device on the network, such as computers and print servers. These IP addresses a Gateway-to-VPN Gateway VPN would be as follows. (See Figure 2-3.) At home, a telecommuter uses his VPN Gateway for his always-on Internet connection. His Gateway is configured with his office's VPN settings. When he connects to his office's Gateway, the two Gateways 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 additional information and instructions about creating your own VPN, please visit Linksys's website at www.

linksys.com or refer to "Appendix C: Configuring IPSec between a Windows 2000 or XP computer and the VPN Gateway." Figure 2-2: Computer-to-VPN Gateway IMPORTANT: You must have at least one VPN Gateway on one end of the VPN tunnel. At the other end of the VPN tunnel, you must have a second VPN Gateway or a computer with VPN client software that supports IPSec. Why do I need a VPN? Computer networking provides a flexibility not available when using a paper-based system.

With this flexibility, however, comes an increased risk in security. This is why firewalls were first introduced. Firewalls help to Chapter 2: Planning your Network Why do I need a VPN? 6 Wireless-G ADSL Gateway protect data inside of a local network. But what do you do once information is sent outside of your local network, when emails 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 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 email 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 Figure 2-3: VPN Gateway-to-VPN Gateway 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 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. Chapter 2: Planning your Network Why do I need a VPN? 7 Wireless-G ADSL Gateway Chapter 3: Getting to Know the Wireless-G ADSL Gateway The Back Panel The Gateway's ports, where a network cable is connected, are located on the back panel. Figure 3-1: Back Panel ADSL LAN (1-4) Power Reset Button The ADSL port connects to the ADSL line. The LAN (Local Area Network) ports connect to your computer and other network devices. The Power port is where you will connect the power adapter.

There are two ways to Reset the Gateway's factory defaults. Either press the Reset Button, for approximately ten seconds, or restore the defaults from the Factory Defaults screen of the Administration tab in the Gateway's Web-Based Utility. Important: Resetting the Gateway to factory defaults will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.) and replace them with the factory defaults. Do not reset the Gateway if you want to retain these settings.

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 Gateway. Chapter 3: Getting to Know the Wireless-G ADSL Gateway The Back Panel 8 Wireless-G ADSL Gateway The Front Panel The Gateway's LEDs, where information about network activity is displayed, are located on the front panel.

Figure 3-2: Front Panel Power WLAN Green. The Power LED lights up when the Gateway is powered on. Green. The WLAN LED lights up whenever there is a successful wireless connection. If the LED is blinking, the Gateway is actively sending or receiving data to or from one of the devices on the network. Green. The LAN LED serves two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through the LAN port. If the LED is blinking, it is an indication of any network activity. Green.

The ADSL LED lights up whenever there is a successful modem connection. The LED blinks while establishing the ADSL connection. Green. The Act LED blinks when there is network activity across the ADSL connection. Green. The Session LED lights up when a PPPoE or PPPoA session is established. LAN (1-4) ADSL Act Session Chapter 3: Getting to Know the Wireless-G ADSL Gateway The Front Panel 9 Wireless-G ADSL Gateway Chapter 4: Connecting the Wireless-G Broadband Gateway Overview The Gateway's setup consists of more than simply plugging hardware together. You will have to configure your networked computers to accept the IP addresses that the Gateway assigns them (if applicable), and you will also have to configure the Gateway with setting(s) provided by your Internet Service Provider (ISP). The installation technician from your ISP should have left the setup information for your modem with you after installing your broadband connection.

If not, you can call your ISP to request that data.

Once you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Gateway. If you want to use a computer with an Ethernet adapter to configure the Gateway, continue to "Wired Connection to a computer." If you want to use a computer with a wireless adapter to configure the Gateway, continue to "Wireless Connection to a Computer." Chapter 4: Connecting the Wireless-G Broadband Gateway Overview 10 Wireless-G ADSL Gateway Wired Connection to a Computer 1. Before you begin, make sure that all of your network's hardware is powered off, including the Gateway and all computers.

2. Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the Gateway (see Figure 4-1), and the other end to an Ethernet port on a computer. 3. Repeat this step to connect more computers, a switch, or other network devices to the Gateway. IMPORTANT: If using microfilters, make sure to only place the microfilters between the phone and the wall jack and not between the Gateway and the wall jack or your ADSL will not connect.

4. Connect a phone cable from the ADSL port on the Gateway's back panel (see Figure 4-2) to the wall jack of the ADSL line. A small device called a microfilter may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions. 5. Connect the power adapter to the Gateway's Power port (see Figure 4-3), 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, then it will light up steady when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting." 6.

Power on one of your computers that is connected to the Gateway. Figure 4-2: ADSL Connection Figure 4-1: LAN Connection NOTE: You should always plug the Gateway's power adapter into a power strip with surge protection. Wireless Connection to a Computer If you want to use a wireless connection to access the Gateway, follow these instructions: 1. Before you begin, make sure that all of your network's hardware is powered off, including the Gateway and all computers. Figure 4-3: Power Connection Chapter 4: Connecting the Wireless-G Broadband Gateway Wired Connection to a Computer 11 Wireless-G ADSL Gateway IMPORTANT: If using microfilters, make sure to only place the microfilters between the phone and the wall jack and not between the Gateway and the wall jack or your ADSL will not connect. 2. Connect a phone cable from the ADSL port on the Gateway's back panel (see Figure 4-2) to the wall jack of the ADSL line. A small device called a microfilter may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions. 3.

Connect the power adapter to the Power port (see Figure 4-3), 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, then light up steady when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting." 4.

Power on one of the computers on your wireless network(s). 5. For initial access to the Gateway through a wireless connection, make sure the computer's wireless adapter has its SSID set to linksys (the Gateway's default setting), and its WEP encryption is disabled. After you have accessed the Gateway, you can change the Gateway and this computer's adapter settings to match the your usual network settings. NOTE: You should always change the SSID from its default, linksys, and enable WEP encryption.

The Gateway's hardware installation is now complete. Go to "Chapter 5: Configuring the Gateway." Chapter 4: Connecting the Wireless-G Broadband Gateway Wireless Connection to a Computer 12 Wireless-G ADSL Gateway Chapter 5: Configuring the Gateway Overview Follow the steps in this chapter and use the Gateway's web-based utility to configure the Gateway. 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 Gateway. 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 Gateway's default username and password is admin.

To secure the Gateway, change the Password from its default. There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs. Note: For added security, you should change the password through the Administration tab. Have You: Enabled TCP/IP on your computers? computers communicate over the network with this protocol. Refer to Appendix D: Windows Help for more information on TCP/IP. Setup · Basic Setup. Enter the Internet connection and network settings on this screen. · DDNS. To enable the Gateway's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.

· Advanced Routing. On this screen, you can alter Dynamic Routing, and Static Routing configurations. Wireless · Basic Wireless Settings. You can choose your Wireless Network Mode and Wireless Security on this screen. · Wireless Network Access.

This screen displays your wireless network access list. · Advanced Wireless Settings. On this screen you can access the Advanced Wireless features. Security · Firewall. This screen contains Filters and Block WAN Requests.

Filters block specific internal users from accessing the Internet and block anonymous Internet requests. Chapter 5: Configuring the Gateway Overview 13 Wireless-G ADSL Gateway · VPN. To enable or disable IPSec and/or PPTP Pass-through, and set up VPN tunnels, use this screen. Access Restrictions · Internet Access. This screen allows you to prevent or permit only certain users from attaching to your network. Applications & Gaming · Single Port Forwarding. Use this screen to set up common services or applications on your network. · Port Range 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. To allow one local user to be exposed to the Internet for use of special-purpose services, use this screen.

Administration · Management. On this screen, alter Gateway access privileges, SNMP, and UPnP settings. · Reporting. If you want to view or save activity logs, click this tab. · Diagnostics. Use this screen to do a Ping Test. · Factory Defaults.
If you want to restore the Gateway's factory defaults, use this screen. · Firmware Upgrade. Click this tab if you want to upgrade the Gateway's firmware. Status · Gateway. This screen provides status information about the Gateway.
· Local Network. This provides status information about the local network. · Wireless. This screen provides status information about the wireless network. · DSL Connection.
This screen provides status information about the DSL connection. Chapter 5: Configuring the Gateway Overview 14 Wireless-G ADSL Gateway How to Access the Web-based Utility To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Gateway's default IP address, 192.168.1.1, in the Address field. Then press Enter. A password request page, shown in Figure 5-1 will appear. (non-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 button.

The Setup Tab The Basic Setup Tab The first screen that appears is the Basic Setup tab. (See Figure 5-2.) This tab allows you to change the Gateway's general settings. Change these settings as described here and click the Save Settings button to save your changes or Cancel Changes to cancel your changes. Figure 5-1: Password Screen Internet Setup · VC Settings. Virtual Circuit (VPI and VCI): These fields consist of two items: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields. Multiplexing: Select LLC or VC , depending on your ISP. · ADSL Settings. The Gateway supports five Encapsulations: RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA, and Bridged Mode Only. Each Basic Setup screen and available features will differ depending on what kind of encapsulation you select. RFC 1483 Bridged Dynamic IP IP Settings. Select Obtain an IP Address Automatically if your ISP says you are connecting through a dynamic IP address. (See Figure 5-3.) Figure 5-2: Basic Setup Tab Chapter 5: Configuring the Gateway How to Access the Web-based Utility 15 Wireless-G ADSL Gateway Static IP If you are required to use a permanent IP address to connect to the Internet, then select Use the following IP Address.
(See Figure 5-4.) · IP Address. This is the Gateway'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 Gateway's Subnet Mask. 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 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 5-3: Dynamic IP Figure 5-4: Static IP Chapter 5: Configuring the Gateway The Setup Tab 16 Wireless-G ADSL Gateway RFC 1483 Routed If you are required to use RFC 1483 Routed, then select RFC 1483 Routed. (See Figure 5-5.

) · IP Address. This is the Gateway'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 Gateway's Subnet Mask. 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. RFC 2516 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. (See Figure 5-6.
) · Service Name. Enter the Service Name, if required by your ISP. · User Name and Password. Enter the User Name and Password provided by your ISP. · Connect on Demand: Max Idle Time.
You can configure the Gateway to disconnect 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 Gateway 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: Redial Period. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway 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 Gateway to check the Internet connection. The default Redial Period is 30 seconds.

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 5-6: RFC 2516 PPPoE Chapter 5: Configuring the Gateway The Setup Tab Figure 5-5: RFC 1483 Routed 17 Wireless-G ADSL Gateway RFC 2364 PPPoA Some DSL-based ISPs use PPPoA (Point-to-Point Protocol over ATM) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoA. If they do, you will have to enable PPPoA. (See Figure 5-7.) · User Name and Password. Enter the User Name and Password provided by your ISP. · Connect on Demand: Max Idle Time. You can configure the Gateway 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 Gateway 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 Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway 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 Gateway to check the Internet connection. The default Redial Period is 30 seconds. 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 5-7: RFC 2364 PPPoA Bridged Mode Only If you are using your Gateway as a bridge, which makes the Gateway act like a standalone modem, select Bridged Mode Only.

(see Figure 5-8). All NAT and routing is disabled in this mode. 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 5-8: Bridged Mode Only Optional Settings (Required by some ISPs) (See Figure 5-9.) · Host Name and Domain Name. These fields allow you to supply a host and domain name for the Gateway. 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. Chapter 5: Configuring the Gateway The Setup Tab 18 Wireless-G ADSL Gateway · MTU.

The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select Manual and enter the value desired. It is recommended that you leave this value in the 1200 to 1500 range. By default, MTU is configured automatically. Network Setup · Router IP. The values for the Gateway's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work. · 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). A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each computer on your network for you. Unless you already have one, it is highly recommended that you leave the Gateway 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 Gateway's DHCP option to Disable. · Starting 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, because the default IP address for the Gateway is 192.168.

1.1. · Number of Address. Enter the maximum number of computers that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. By default, as shown in Figure 5-9, the range is 192.168.1.100 to 192.168.

1.149. · DHCP Address Range. The range of DHCP addresses is displayed here. · Client Lease Time.

Enter the minutes in the field. · Time Setting. This is where you set the time zone for your Gateway. 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 5-9: Optional Settings Chapter 5: Configuring the Gateway The Setup Tab 19 Wireless-G ADSL Gateway The DDNS Tab The Gateway 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 Gateway. Before you can use this feature, you need to sign up for DDNS service at DynDNS.org. DDNS DDNS Service. If your DDNS service is provided by DynDNS.org, then select DynDNS.org in the drop-down menu. (See Figure 5-10.) To disable DDNS Service, select Disabled.

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 Gateway'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. Figure 5-10: DynDNS.

org 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. Chapter 5: Configuring the Gateway The Setup Tab 20 Wireless-G ADSL Gateway Advanced Routing Tab The Advanced Routing screen allows you to configure the dynamic routing and static routing settings. (See Figure 5-11.) Advanced Routing · Dynamic Routing. With Dynamic Routing you can enable the Gateway to automatically adjust to physical changes in the network's layout.

The Gateway, 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 Gateways on the network. To enable RIP, click Enabled. To disable RIP, click Disabled. · Receive RIP Version.

To receive RIP messages, select the protocol you want: RIP1 or RIP2. If you don't want to receive RIP messages, select None. · Transmit RIP Version. To transmit RIP messages, select the protocol you want: RIP1, RIP1-Compatible, or RIP2. If you don't want to transmit RIP messages, select None. Figure 5-11: Advanced Routing Static Routing If the Gateway is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To create a static route, change the following settings: · Select Entry. Select the number of the static route from the drop-down menu. The Gateway supports up to 20 static route entries.

If you need to delete a route, after selecting the entry, click the Delete Entry button. · Destination IP Address. The Destination 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 building a route to an entire network, be sure that the network portion of the IP address is set to 0. · 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. · Gateway. This IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host. · Hop Count.

This determines the maximum number of steps between network nodes that data packets will travel. A node is any router in the path to the remote network. Chapter 5: Configuring the Gateway The Setup Tab 21 Wireless-G ADSL Gateway · 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 (see Figure 5-12) displaying how data is routed through your LAN.

For each route, the Destination IP address, Subnet Mask, Gateway, and Interface are displayed. Click the Refresh button to update the information. 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 5-12: Routing Table Chapter 5: Configuring the Gateway The Setup Tab 22 Wireless-G ADSL Gateway The Wireless Tab Basic Wireless Settings (See Figure 5-13.

) This screen allows you to choose your wireless network mode and wireless security. Wireless Network · Wireless Network Mode. If you have 802.11g and 802.11b devices in your network, then keep the default setting, Mixed. If you have only 802.11g devices, select 802.11g. If you have only 802.11b devices, select 802.

11b. If you want to disable wireless networking, select Disabled. · Wireless Network Name (SSID). Enter the name for your wireless network into the field. The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Linksys recommends that you change the default SSID (linksys) to a unique name of your choice. · Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 13 (most of Europe).

All devices in your wireless network must use the same channel in order to function correctly. Linksys wireless clients will automatically detect the wireless channel of the Gateway. Figure 5-13: 64-Bit WEP Encryption Wireless Security · Wireless SSID Broadcast. When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Gateway. To broadcast the Gateway's SSID, keep the default setting, Enabled. If you do not want to broadcast the Gateway's SSID, then select Disabled. · WEP Encryption Level. An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode data transmissions, all devices in a network must use an identical WEP key.

Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance. To enable WEP, select 64 bits (10 hex digits) (see Figure 5-13) or 128 bits (26 hex digits) (see Figure 5-14). To disable WEP encryption, keep the default setting, No Encryption. · Passphrase for keys. 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 and cannot be used Chapter 5: Configuring the Gateway The Wireless Tab Figure 5-14: 128-Bit WEP Encryption 23 Wireless-G ADSL Gateway with Windows XP Zero Configuration. If you want to communicate with non-Linksys wireless products or Windows XP Zero Configuration, make a note of the WEP key generated in the Key 1 field, and enter it manually in the wireless client.) After you enter the Passphrase, click the Generate button to create WEP keys.

· Default Key Select which WEP key (1-4) will be used when the Gateway sends data. Make sure that the receiving device (wireless client) is using the same key. · WEP Keys 1-4. WEP keys enable you to create an encryption scheme for wireless network transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes; they are not valid key values.) If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F". When finished making your changes on this tab, click the Save Settings button to save these changes, or click the Cancel Changes button to undo your changes.

Wireless Network Access (See Figure 5-15.) Wireless Network Access. If you select Allow All, all computers will be allowed access to the wireless network. To restrict access to the network, select Restrict Access to Computers below. Click the Select MAC Address From Networked Computers button, and the screen in Figure 5-16 will appear.

Select the MAC Address from the list and click the Select box, then click the Select button. Click the Refresh button if you want to refresh the screen. Click the Close button to return to the previous screen. 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 5-15: Wireless Network Access Figure 5-16: Networked Computers Chapter 5: Configuring the Gateway The Wireless Tab 24 Wireless-G ADSL Gateway Advanced Wireless Settings (See Figure 5-17.

) On this screen you can access the Advanced Wireless features, including Authentication Type, Basic Data Rates, Control Tx Rates, Beacon Interval, DTIM Interval, RTS Threshold, and Fragmentation Threshold. · Control Tx Rates. The default transmission rate is Auto. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, Auto, to have the Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Gateway and a wireless client. · Beacon Interval. The default value is 100. Enter a value between 1 and 65,535 milliseconds.

The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Gateway to synchronize the wireless network. Figure 5-17: Advanced Wireless Settings · DTIM Interval. The default value is 3. This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Gateway has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. · Fragmentation Threshold. This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold.

Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.
· RTS Threshold. This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled.
The Gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. · Authentication Type. The default is set to Auto (default), which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do not use a WEP key for authentication but can use WEP for data encryption. If you want to allow on Open System authentication, then select Open System. For Shared Key authentication, the sender and recipient use a WEP key for both authentication and data encryption. If you want to use only Shared Key authentication, then select Shared Key. It is recommended that this option be left in the default (Auto) mode, because some clients cannot be configured for Shared Key.
Chapter 5: Configuring the Gateway The Wireless Tab 25 Wireless-G ADSL Gateway The Security Tab Firewall When you click the Security tab, you will see the Firewall screen (see Figure 5-18).

This screen contains Filters and the option to Block WAN Requests. Filters block specific Internet data types and block anonymous Internet requests. · Firewall. To add Firewall Protection, click Enabled. If you do not want Firewall Protection, click Disabled. Additional Filters · Filter Proxy. Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click Enabled. · Filter Cookies.
A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click Enabled. · Filter Java Applets. Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language.
To enable Java Applet filtering, click Enabled. · Filter ActiveX. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click Enabled.
Block WAN requests · Block Anonymous Internet Requests. This keeps your network from being "pinged" or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to discover your network. Select Block Anonymous Internet Requests to block anonymous Internet requests or deselect it to allow anonymous Internet requests. Click View Logs to view a log of any firewall events. 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 5-18: Firewall Chapter 5: Configuring the Gateway The Security Tab 26 Wireless-G ADSL Gateway VPN Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. The VPN screen, shown in Figure 5-19, 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 Passthrough. 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. IPSec VPN Tunnel The VPN Gateway 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 five simultaneous tunnels. Then click Enabled to enable the IPSec VPN 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.
These computers can be specified by a Subnet, specific IP address, or range. · Remote Security Gateway. The Remote Security Gateway is the VPN device, such as a second VPN Gateway, on the remote end of the VPN tunnel. Enter the IP Address or Domain of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Gateway, a VPN Server, or a computer with VPN client software that supports IPSec.
The IP Address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Gateway, but the IP Address of the remote VPN Gateway or device with which you wish to communicate. If you enter an IP address, only the specific IP Address will be able to acess the tunnel. If you select Any, any IP Address can access the tunnel. Figure 5-19: VPN Chapter 5: Configuring the Gateway The Security Tab 27 Wireless-G ADSL Gateway · 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 5-19, 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, if 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 5-19, MD5 (the default) has been selected. · Key Management. Select Auto (IKE) or Manual from the drop-down menu. 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. 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 select to have the key expire at the end of a time period.

Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely. Check the box next to PFS (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. Manual (See Figure 5-20.) Select Manual, then select the Encryption Algorithm from the drop-down menu. Enter the Encryption Key in the field (if you chose DES for your Encryption Algorithm, 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 you chose MD5 for your Authentication Algorithm, enter 32 hexadecimal characters, if you chose SHA1, enter 40 hexadecimal characters). Enter the Inbound and Outbound SPIs in the respective fields. Figure 5-20: Manual Key Management · Status. The status of the connection is shown. Click the Connect button to connect your VPN tunnel. Click the View Logs button to view logs. Click the Advanced Setting button and the Advanced IPSec VPN Tunnel Setup screen will appear. See Figure 5-20. 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.

Chapter 5: Configuring the Gateway The Security Tab 28 Wireless-G ADSL Gateway Advanced VPN Tunnel Setup From the Advanced IPSec VPN Tunnel Setup screen, shown in Figure 5-21, 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 Gateway will accept both Main and Aggressive requests from the remote VPN device. Select Username, then enter the user name.

· 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. · PFS. The status of PFS 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. Figure 5-21: Advanced VPN Tunnel Setup Chapter 5: Configuring the Gateway The Security Tab 29 Wireless-G ADSL Gateway · Key Life Time. In the Key Lifetime field, you may select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed. Other Setting · NetBIOS broadcast. Check the box next to NetBIOS broadcast to enable NetBIOS traffic to pass through the VPN tunnel. · Anti-replay. Check the box next to Anti-replay to enable the Anti-replay protection.

This feature keeps track of sequence numbers as packets arrive, ensuring security at the IP packet-level. · Keep-Alive. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. · Check this box to block unauthorized IP addresses.

Enter in the 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 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. Chapter 5: Configuring the Gateway The Security Tab 30 Wireless-G ADSL Gateway The Access Restrictions Tab Internet Access The Access Restrictions tab, shown in Figure 5-22, allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific computers 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 5-23, 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. 2. Click the Edit List button. This will open the List of computers screen, shown in Figure 5-24. From this screen, you can enter the IP address or MAC address of any computer to which this policy will apply. You can even enter ranges of computers by IP address. Click the Apply button to save your settings, the Cancel button to undo any changes, and the Close button to return to the Filters tab.

3. If you wish to Deny or Allow Internet access for those computers you listed on the List of PCs screen, click the option. 4. You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting a service from the drop-down menus next to Blocked Services.

If a service isn't listed, you can click the Add/ Edit Service button to open the Port Service screen, shown in Figure 5-25, and add a service to the list. You will need to enter a Service name, as well as the Protocol and Port Range used by the service. 5. By selecting the appropriate setting next to Days and Time, choose when Internet access will be filtered. 6. Click the Save Settings button to activate the policy.

Figure 5-22: Access Restriction Figure 5-23: Internet Policy Summary Chapter 5: Configuring the Gateway The Access Restrictions Tab 31 Wireless-G ADSL Gateway 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. 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 5-24: List of PCs Figure 5-25: Port Services Chapter 5: Configuring the Gateway The Access Restrictions Tab 32 Wireless-G ADSL Gateway The Applications and Gaming Tab Single Port Forwarding The Single Port Forwarding screen provides options for customization of port services for common applications. (See Figure 5-26.) When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function. Choose or 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 or UDP.

Enter the IP Address in the field. Click Enabled to enable UPnP Forwarding for the chosen application. When finished making your changes on this tab, click the Save Settings button to save these changes, or click the Cancel Changes button to undo your changes. Figure 5-26: Single Port Forwarding Chapter 5: Configuring the Gateway The Applications and Gaming Tab 33 Wireless-G ADSL Gateway 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 5-27.) When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should 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. · TCP UDP. Select the type of protocol you wish to use for each application: TCP, UDP, or Both.

· IP Address. Enter the IP Address and Click Enabled. When finished making your changes on this tab, click the Save Settings button to save these changes, or click the Cancel Changes button to undo your changes. Figure 5-27: Port Range Forwarding Port Triggering Port Triggering is used for special applications that can request a port to be opened on demand. For this feature, the Gateway will watch outgoing data for specific port numbers.

(See Figure 5-28.) The Gateway will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Gateway, 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 Outgoing Triggered Range numbers and the Incoming Forwarded Range numbers of the port you wish to forward. 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 5-28: Port Triggering Chapter 5: Configuring the Gateway The Applications and Gaming Tab 34 Wireless-G ADSL Gateway DMZ The DMZ screen (see Figure 5-29) allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing through DMZ Hosting. DMZ hosting forwards all the ports for one computer at the same time, which differs from Port Range Forwarding, which can only forward a maximum of 10 ranges of ports. · DMZ Hosting.

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 computer, 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." 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 5-29: DMZ Chapter 5: Configuring the Gateway The Applications and Gaming Tab 35 Wireless-G ADSL Gateway The Administration Tab Management The Management screen, shown in Figure 5-30, allows you to change the Gateway's access settings as well as configure the SNMP (Simple Network Management Protocol) and UPnP (Universal Plug and Play) features. Gateway Access Local Gateway Access. To ensure the Gateway's security, you will be asked for your password when you access the Gateway's Web-based Utility.

The default username and password is admin. · Gateway Username. Enter the default admin. It is recommended that you change the default username to one of your choice. · Gateway Password.

It is recommended that you change the default password to one of your choice. · Re-enter to confirm. Re-enter the Gateway's new Password to confirm it. Remote Gateway Access. This feature allows you to access the Gateway from a remote location, via the Internet.

IMPORTANT: Enabling remote Administration allows anyone with access to your password to configure the Gateway from somewhere else on the Internet. Figure 5-30: Management · Remote Administration. This feature allows you to manage the Gateway from a remote location via the Internet. To enable Remote Administration, click Enabled. · Administration Port. Enter the port number you will use to remotely access the Gateway.