LINKSYS®
A Division of Cisco Systems, Inc.

ADSL2 Gateway

with 4-Port Switch

WIRED

User Guide

Model No. AG241

CISCO SYSTEMS

Manual abstract:

and/or its affiliates in the U.S. and certain other countries. Copyright © 2004 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 Gateway ties it all together and lets your whole network share that high-speed Internet connection.

To protect your data and privacy, the ADSL2 Gateway with 4-Port Switch features an advanced firewall to keep Internet intruders and attackers out. 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 ADSL2 Gateway with 4-Port Switch at the heart of your home network, you're connected to the future. Chapter 1: Introduction Welcome 1 ADSL2 Gateway with 4-Port Switch What's in this Guide? This user guide covers the steps for setting up and using the ADSL2 Gateway with 4-Port Switch.

· Chapter 1: Introduction This chapter describes the ADSL2 Gateway with 4-Port Switch ADSL2 Gateway with 4-Port Switch applications and this User Guide. · Chapter 2: Planning Your Network This chapter describes the basics of networking. · Chapter 3: Getting to Know the ADSL2 Gateway with 4-Port Switch This chapter describes the physical features of the Gateway. · Chapter 4: Connecting the ADSL2 Gateway with 4-Port Switch 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 ADSL2 Gateway with 4-Port Switch. · Appendix B: 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 C: Upgrading Firmware This appendix instructs you on how to upgrade the firmware on your Gateway if you should need to do so. · Appendix D: Finding the MAC Address and IP Address for your Ethernet Adapter. This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Gateway. · Appendix E: Glossary This appendix gives a brief glossary of terms frequently used in networking. · Appendix F: Specifications This appendix provides the technical specifications for the Gateway. Chapter 1: Introduction What's in this Guide? 2 ADSL2 Gateway with 4-Port Switch · Appendix G: Warranty Information This appendix supplies the warranty information for the Gateway. · Appendix H: Regulatory Information This appendix supplies the regulatory information regarding the Gateway. · Appendix I: 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 ADSL2 Gateway with 4-Port Switch 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 ADSL2 Gateway with 4-Port Switch 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 are called "dynamic" because they are only temporarily assigned to the computer or device. After a certain time period, they expire and may change.

If a computer logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will automatically assign it a new dynamic IP address. DHCP (Dynamic Host Configuration Protocol) Servers Computers and other network devices using dynamic IP addressing are assigned a new IP address by a DHCP server.

The computer or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network. A DHCP server can either be a designated computer on the network or another network device, such as the Gateway. By default, the Gateway's DHCP Server function is enabled. If you already have a DHCP server running on 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 ADSL2 Gateway with 4-Port Switch 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 ADSL2 Gateway with 4-Port Switch Chapter 3: Getting to Know the ADSL2 Gateway with 4Port Switch The Back Panel Figure 3-1: Back Panel The Gateway's ports, where a network cable is connected, are located on the back panel. The Gateway's buttons are also located on the back panel.

Important: Resetting the Gateway to factory defaults will erase all of your settings and replace them with the factory defaults. Do not reset the Gateway if you want to retain these settings. LINE Ethernet (1-4) Reset Button The LINE port connects to the ADSL line. The Ethernet ports connect to your computer and other network devices. 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. The Power port is where you will connect the power adapter. This switch is used to turn the Gateway on or off. Power On/Off Switch With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys international website at www.

linksys.com/international for more information about products that work with the Gateway. Chapter 3: Getting to Know the ADSL2 Gateway with 4-Port Switch The Back Panel 8 ADSL2 Gateway with 4-Port Switch 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 Ethernet (1-4) Green. The Power LED lights up when the Gateway is powered on.

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 DSL LED lights up whenever there is a successful DSL connection. The LED blinks while establishing the ADSL connection. Green. The Internet LED lights up green when an Internet connection to the Internet Service Provider (ISP) session is established. The Internet LED lights up red when the connection to the ISP fails. DSL Internet Chapter 3: Getting to Know the ADSL2 Gateway with 4-Port Switch The Front Panel 9 ADSL2 Gateway with 4-Port Switch Chapter 4: Connecting the ADSL2 Gateway with 4-Port Switch 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. After you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Gateway.

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 Ethernet 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. Figure 4-1: Ethernet Connection NOTE: A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions. Chapter 4: Connecting the ADSL2 Gateway with 4-Port Switch Overview 10 ADSL2 Gateway with 4-Port Switch IMPORTANT: For countries that have phone jacks with RJ-11 connectors, make sure to only place the microfilters between the phone and the wall jack and not between the Modem and the wall jack or your ADSL will not connect. For countries that do not have phone jacks with RJ-11 connectors (e.

g. France, Sweden, Switzerland, United Kingdom, etc.), except for ISDN users, the microfilter has to be used between the modem and the wall jack, because the microfilter will have the RJ-11 connector. Annex B users (E1 and DE versions of the Gateway) must use the included special cable to connect the gateway to the wall jack (RJ-45 to RJ-12). If you require splitters or special jacks, please contact your service provider.

Figure 4-2: ADSL Connection 4. Connect a phone cable from the Line 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. Turn the On/Off switch to On. · The Power LED on the front panel will light up green as soon as the power adapter is connected properly and the switch is turned on. 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. NOTE: You should always plug the Gateway's power adapter into a power strip with surge protection. Figure 4-3: Power Connection The Gateway's hardware installation is now complete. Go to "Chapter 5: Configuring the Gateway.

" NOTE: You should always change the SSID from its default, linksys, and enable WEP encryption. Chapter 4: Connecting the ADSL2 Gateway with 4-Port Switch Connection to a Computer 11 ADSL2 Gateway with 4-Port Switch 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 six main tabs: Setup, 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 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. Security · Firewall. This screen contains Filters and Block WAN Requests. Filters block specific internal users from accessing the Internet and block anonymous Internet requests. · 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. Chapter 5: Configuring the Gateway Overview 13 ADSL2 Gateway with 4-Port Switch 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. · QoS. QoS ensures better service to high-priority types of network traffic, which may involve demanding, realtime applications, such as Internet phone calls or videoconferencing. Administration · Management. On this screen, alter Gateway access privileges, SNMP, UPnP, and WT-82 settings.

· Reporting. If you want to view or save activity logs, click this tab. · Diagnostics. Use this screen to do a Ping Test. · Backup&Restore.

The Backup&Restore tab allows you to back up and restore the Gateway's configuration file. · 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.

· Reboot. This tab allows you to do a soft or hard reboot of your Gateway. Status · Gateway. This screen provides status information about the Gateway. · Local Network. This provides status information about the local network. · DSL Connection. This screen provides status information about the DSL connection. Chapter 5: Configuring the Gateway Overview 14 ADSL2 Gateway with 4-Port Switch 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.

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 · PVC Connection. Select a PVC connection number from the drop-down menu. Then, select the Enable Now to enable the connection. · VC Settings. Virtual Circuits (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. · QOS Type: Select from the drop-down menu: CBR, Continuous Bit Rate to specify fixed bandwidth for voice or data traffic; UBR, Unspecific Bit Rate for application that are none-time sensitive, such as email; or VBR, Variable Bite Rate for Bursty traffic and bandwidth sharing with other application. · Pcr Rate: Peak Cell Rate, divide the DSL line rate by 424 to find the PCR to get the maximum rate the sender can send cells. Enter the rate in the field (if required by your service provider).

· Scr Rate: Sustain Cell Rate, sets the average cell rate that can be transmitted. SCR normally less than PCR. Enter the rate in the field (if required by your service provider). · Autodetect: Select Enable to have the settings automatically entered or Disable to enter the values manually. Figure 5-2: Basic Setup Tab · Virtual Circuit: Enter the VPI and VCi ranges in the fields. Chapter 5: Configuring the Gateway How to Access the Web-based Utility 15 ADSL2 Gateway with 4-Port Switch · Internet Connection Type. 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 type 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.

Static IP If you are required to use a permanent (static) IP address to connect to the Internet, then select Use the following IP Address. · Internet 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. · 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 ADSL2 Gateway with 4-Port Switch IPoA If you are required to use RFC 1577 IPoA (Classical IP over ATM), then select IPoA. · 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. · Service Name. Enter the name of your PPPoE service in the field.

· 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: IPoA 17 ADSL2 Gateway with 4-Port Switch 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. · 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.

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 Chapter 5: Configuring the Gateway The Setup Tab 18 ADSL2 Gateway with 4-Port Switch Optional Settings (Required by some ISPs) · 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. · MTU.

The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select Manual and enter the value desired in the Size field. 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.

· DHCP Relay Server. If you enable the Local DHCP Server or DHCP Relay for the Local DHCP server, enter the IP address for the DHCP server in the fields. · AutoDetect LAN DHCP Server. · 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. · Maximum Number of DHCP Users. Enter the maximum number of users/clients that can obtain an IP address. The number will vary depending on the starting IP address entered.

· Client Lease Time. The Client Lease Time is the amount of time a network user will be allowed connection to the Gateway with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. · Static DNS 1-3. The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs.

Your ISP will provide you with at least one DNS Server IP Address. You Chapter 5: Configuring the Gateway The Setup Tab Figure 5-9: Optional Settings 19 ADSL2 Gateway with 4-Port Switch can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers. · WINS. The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank. · Time Setting. This is where you set the time zone for your Gateway. Select your time zone from the dropdown menu.

If desired, check the Automatically adjust clock for daylight saving changes. When finished making your changes on this tab, click the Save Settings button to save these changes, or click the Cancel Changes button to undo your changes. 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 Figure 5-10: DynDNS.org 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. TZO.com · Email Address, Password, and Domain Name. Enter the Email Address, TZO Password Key, and Domain Name of the service you set up with TZO. Figure 5-11: TZO.com Chapter 5: Configuring the Gateway The Setup Tab 20 ADSL2 Gateway with 4-Port Switch · Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, this will change.

· Status. The status of the DDNS service connection is displayed here. When finished making your changes on this tab, click the Save Settings button to save these changes, or click the Cancel Changes button to undo your changes. Advanced Routing Tab The Advanced Routing screen allows you to configure the dynamic routing and static routing settings. Advanced Routing · Operating Mode. NAT is a security feature that is enabled by default. It enables the Gateway to translate IP addresses of your local area network to a different IP address for the Internet. To disable NAT, click the Disabled radio button. · 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. · Transmit RIP Version.

To transmit RIP messages, select the protocol you want: RIP1, RIP1-Compatible, or RIP2. · Receive RIP Version. To receive RIP messages, select the protocol you want: RIP1 or RIP2. · 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 set number. 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 This 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. Chapter 5: Configuring the Gateway The Setup Tab Figure 5-12: Advanced Routing 21 ADSL2 Gateway with 4-Port Switch · 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. Hop Count is the number of hops to each node until the destination is reached (16 hops maximum). Enter the Hop Count in the field. · Show Routing Table. Click the Show Routing Table button to open a screen 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.

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 5-13: Routing Table List The Security Tab Firewall When you click the Security tab, you will see the Firewall screen. This screen contains Filters and the option to Block WAN Requests. Filters block specific Internet data types and block anonymous Internet requests.

To add Firewall Protection, click Enable. If you do not want Firewall Protection, click Disable. 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. Chapter 5: Configuring the Gateway The Security Tab 22 ADSL2 Gateway with 4-Port Switch 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. 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. VPN Figure 5-14: Firewall Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. The VPN screen 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 Enable button. To disable IPSec Passthrough, click the Disable 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 Enable button. To disable PPTP Passthrough, click the Disable button. · L2TP Passthrough. Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used to enable the operation of a VPN over the Internet.To allow L2TP Passthrough, click the Enable button.

To disable L2TP Passthrough, click the Disable 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 Chapter 5: Configuring the Gateway The Security Tab 23 ADSL2 Gateway with 4-Port Switch multiple tunnels and does not have to match the name used at the other end of the tunnel. To delete a tunnel entry, select the tunnel, then click Delete. To view a summary of the settings, click Summary. · 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. · Local Security Gateway. · 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. · 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 the Manual Key Management screen, 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. Chapter 5: Configuring the Gateway The Security Tab Figure 5-15: VPN Figure 5-16: VPN Settings Summary 24 ADSL2 Gateway with 4-Port Switch Manual 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.

· Status. The status of the connection is shown. Click the Connect button to connect your VPN tunnel. Click View Logs to view system, UPnP, VPN, firewall, access, or all logs.Click the Advanced Settings button and the Advanced IPSec VPN Tunnel Setup screen will appear.

When finished making your changes on this tab, click the Save Settings button to save these changes, or click the Cancel Changes button to undo your changes. Advanced VPN Tunnel Setup From the Advanced IPSec VPN Tunnel Setup screen 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. · 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. Figure 5-18: System Log Chapter 5: Configuring the Gateway The Security Tab Figure 5-17: Manual Key Management 25 ADSL2 Gateway with 4-Port Switch · 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. · 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. Figure 5-19: Advanced VPN Tunnel Setup Chapter 5: Configuring the Gateway The Security Tab 26 ADSL2 Gateway with 4-Port Switch The Access Restrictions Tab Internet Access The Access Restrictions tab 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 with their name and settings. To return to the Filters tab, click the Close button. · Enter Policy Name.

Policies are created from the fields presented here. To create an Internet Access policy: 1. Enter a Policy Name in the field provided. Select Internet Access as the Policy Type. Figure 5-20: Internet Access 2.

Click the Edit List of PCs button. This will open the List of PCs screen. 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 Save Settings button to save your settings, the Cancel Changes button to undo any changes and return to the Filters tab. Figure 5-21: Internet Policy Summary Chapter 5: Configuring the Gateway The Access Restrictions Tab 27 ADSL2 Gateway with 4-Port Switch 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 Services screen 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. Figure 5-22: List of PCs 6. Click the Save Settings button to activate the policy. 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 5-23: Port Services Chapter 5: Configuring the Gateway The Access Restrictions Tab 28 ADSL2 Gateway with 4-Port Switch The Applications and Gaming Tab Single Port Forwarding The Single Port Forwarding screen provides options for customization of port services for common applications. 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 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. 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.) 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 5-25: Port Range Forwarding Chapter 5: Configuring the Gateway The Applications and Gaming Tab Figure 5-24: Single Port Forwarding 29 ADSL2 Gateway with 4-Port Switch 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. 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 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 5-26: Port Triggering DMZ The DMZ screen 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." Figure 5-27: DMZ 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 Applications and Gaming Tab 30 ADSL2 Gateway with 4-Port Switch QOS Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, realtime applications, such as Internet phone calls or videoconferencing.

Application-based QoS Application-based QoS manages information as it is transmitted and received. Depending on the settings of the QoS screen, this feature will assign information a high or low priority for the five preset applications and three additional applications that you specify. Enable/Disable. To use application-based QoS, select Enable. Otherwise, keep the default, Disable. High priority/Medium priority/Low priority. For each application, select High priority (traffic on this queue shares 60% of the total bandwidth), Medium priority (traffic on this queue shares 18% of the total bandwidth), or Low priority (traffic on this queue shares 1% of the total bandwidth). FTP (File Transfer Protocol). A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.).

For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP. HTTP (HyperText Transport Protocol). The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser. Telnet. A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program. SMTP (Simple Mail Transfer Protocol). The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

POP3 (Post Office Protocol 3). A standard mail server commonly used on the Internet.

It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time.

POP3 uses the SMTP messaging protocol. Specific Port#. You can add three additional applications by entering their respective port numbers in the Specific Port# fields. Figure 5-28: QOS Advanced QoS This setting allows you to specify traffic queue priority. Fragment packet's size of AF and BE traffic to be equal to the size of EF traffic.

Select this option to fragmentize the packet sizes for AF (Assured Forwarding) and BE (Best Effort) queues so that it will increase the efficiency for transporting EF (expedited forwarding) queues. Enter a range between 68~1492 bytes. Chapter 5: Configuring the Gateway The Applications and Gaming Tab 31 ADSL2 Gateway with 4-Port Switch Enable 802.1p P bits scheduling. VLAN's VID. Select this option to enable 802.1p P bits classification scheduling in the appropriate VLAN based on IEEE 802.1Q VLAN identification. Enter the VLAN VID (VLAN Identifier) number in the field. When you have finished making changes to this screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes.

The Administration Tab Management The Management screen 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. · 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. Figure 5-29: Management SNMP SNMP is a popular network monitoring and management protocol.

Chapter 5: Configuring the Gateway The Administration Tab 32 ADSL2 Gateway with 4-Port Switch Identification. To enable SNMP, click Enabled. To disable SNMP, click Disabled. UPnP UPnP allows Windows XP to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing. UPnp. To enable UPnP, click Enabled. Please select a pvc connection to bind. Select a number from the drop-down menu.___________________ 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. Reporting The Reporting tab provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

It also provides logs for VPN and firewall events. · Log. To enable log reporting, click Enabled. · Logviewer IP Address. Enter the IP Address that will receive logs into the field. Email Alerts E-Mail Alerts. To enable E-Mail Alerts, click Enabled. · Denial of Service Thresholds. Enter the thresholds of events you want to receive. · SMTP Mail Server.

Enter the IP Address of the SMTP server in the field. · E-Mail Address for Alert Logs. Enter the e-mail address for alert logs in the field. · Return E-Mail address. Enter the address for the return e-mail.

To view the logs, click the View Logs button. 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 5-30: Reporting Figure 5-31: System Log Chapter 5: Configuring the Gateway The Administration Tab 33 ADSL2 Gateway with 4-Port Switch Diagnostics Ping Test Ping Test Parameters · Ping Target IP. Enter the IP Address that you want to ping in the field. This can be either a local (LAN) IP or an Internet (WAN) IP address.

· Ping Size. Enter the size of the ping packets. · Number of Pings. Enter the number of times that you want to ping. · Ping Interval. Enter the ping interval in milliseconds. · Ping Timeout. Enter the time in milliseconds. · Ping Result. The results of the ping test will be shown here.

Click the Start Test button to start the Ping Test. Figure 5-32: Ping Test Backup&Restore The Backup&Restore tab allows you to back up and restore the Gateway's configuration file. To back up the Router's configuration file, click the Backup button. Then follow the on-screen instructions. To restore the Router's configuration file, click the Browse button to locate the file, and follow the on-screen instructions. After you have selected the file, click the Restore button. Figure 5-33: Backup&Restore Chapter 5: Configuring the Gateway The Administration Tab 34 ADSL2 Gateway with 4-Port Switch Factory Defaults Restore Factory Defaults. If you wish to restore the Gateway to its factory default settings and lose all your settings, click Yes. To begin the restore process, click the Save Settings button to save these changes, or click the Cancel Changes button to undo your changes. Figure 5-34: Factory Defaults Firmware Upgrade The ADSL Gateway allows you to upgrade firmware for the LAN (network) side of the Gateway.

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

Figure 5-35: Firmware Upgrade Chapter 5: Configuring the Gateway The Administration Tab 35 ADSL2 Gateway with 4-Port Switch Reboot This tab allows you to do a soft or hard reboot of your Gateway. Reboot Mode. To reboot your Gateway, select Hard or Soft. Choose hard to power cycle the Gateway or soft to restart it without a power cycle. To begin the reboot process, click the Save Settings button.

When a screen appears asking you if you really want to reboot the device. Click OK. Click the Cancel Changes button if you want to undo your changes. Figure 5-36: Reboot Chapter 5: Configuring the Gateway The Administration Tab 36 ADSL2 Gateway with 4-Port Switch The Status Tab Gateway This screen displays information about your Gateway and its WAN (Internet) Connections.