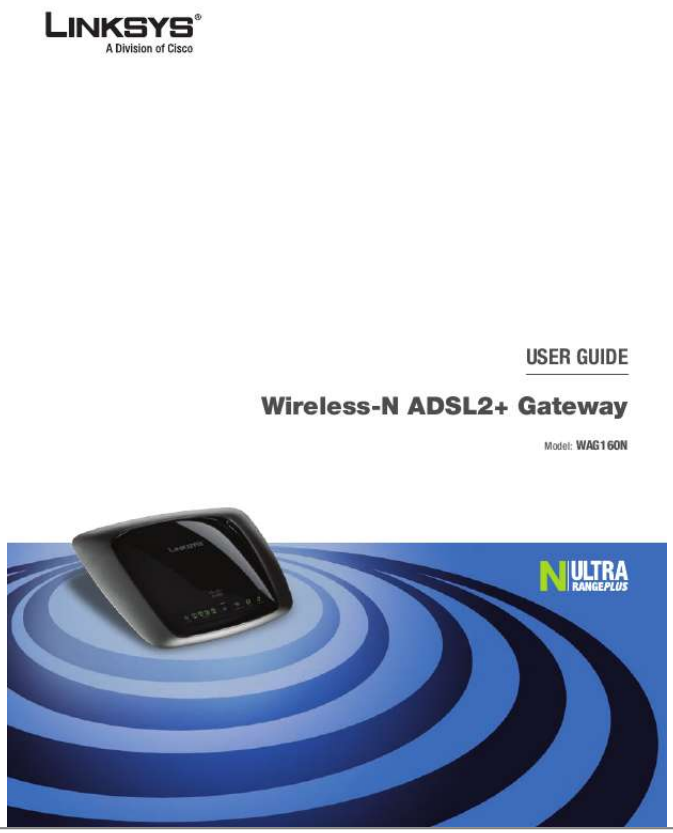

Manual abstract:

S. and certain other countries. Copyright © 2007 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders. Wreless-N ADSL2+ Gateway Table of Contents Chapter 1: Product Overview 1 Front Panel. . . . .

. . . . .

. . . . .

. . . . . 1 Back Panel . . . . .

1 Chapter 2: Wireless Security Checklist 2 General Network Security Guidelines . . . . .

. . . 2 Additional Security Tips . .

. . . . . 2 Chapter 3: Installation 3 Connection .

. . . 3 Setup . .

. 3 Chapter 4: Advanced Configuration 4 Setup > Basic Setup . . . .

. . . . . 4 Setup > DDNS. . . . .

. . . 8 Setup > MAC Address Clone. .

. . . . . .
. . . . .
. . . . .
. . 9 Setup > Advanced Routing . . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. 9 Wireless > Basic Wireless Settings . . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .10 Wireless > Wireless Security . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
11 Wireless > Wireless MAC Filter. . . . .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . .13 Wireless > Advanced Wireless Settings . . . . . .

. . . . . .
. . . . .
. . . . .
. . . . .14 Security > Firewall . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
15 Security > VPN Passthrough . . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
. . . .15 Access Restrictions > Internet Access Policy.
. . . . . .

. . . . . .
. . . . .
. . .16 Applications and Gaming > Single Port Forwarding. .
. . . . . .

. . . . . .
. .17 Applications and Gaming > Port Range Forwarding . . .
. . . . .
. . . . . .

. . . . .17 Applications & Gaming > Port Range Triggering . . . . .
. . . . .
. . . . .
. . . . . .

.18 Applications and Gaming > DMZ . . . . . .

. . . . .
. . . . .
. . . . . .

. . . . . .18 Applications and Gaming > QoS . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
. .18 Administration > Management. . .
. . . . .
. . . . . .

. . . . . .
. . . . .
. . . .20 Administration > Reporting .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .21 Administration > Diagnostics . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .22 Administration > Back Up & Restore. . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
22 Administration > Factory Defaults . . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
22 Administration > Firmware Upgrade . . . . .
. . . . . .

. . . . . .
. . . . .
. . .23 Status > Gateway. .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. . . .23 Status > Local Network . . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
.23 Status > Wireless Network . . . .
. . . . . .

. . . . . .
. . . . .
. . . . .

. . . . . .24 Status > DSL Connection . . . .

. . . . . .25 Appendix A: Troubleshooting Appendix B: Specifications Appendix C: Warranty Information Wreless-N ADSL2+ Gateway 26 27 28 Table of Contents Appendix D: Regulatory Information 29 FCC Statement . . .

. . . .29 Safety Notices. . . . . .

. .29 Industry Canada Statement . . .

.29 Avis d'Industrie Canada. . . . . .

. . .29 Wireless Disclaimer . . . . . .

. @@. . . .

. . @@.31 CE Marking . . . . . .

. .32 National Restrictions . . . . . .

. . . . .32 Product Usage Restrictions . . . . .

. . . . . .
. . . .33 Technical Documents on www.
linksys.com/international . . . .
. . . . . .

. . . . . @@. . . . .
. . . . .
. . . . .
. . . . . .

. . . @@It flashes to indicate network activity over the Internet port. Chapter : Product Overvew Thank you for choosing the Linksys Wireless-N ADSL2+ Gateway. The Gateway lets you access the Internet via a wireless connection or through one of its four switched ports. You can also use the Gateway to share resources such as computers, printers and files. A variety of security features help to protect your data and your privacy while online. Security features include WPA2 security, a Stateful Packet Inspection (SPI) firewall and NAT technology. Configuring the Gateway is easy using the provided browser-based utility.

Back Panel DSL The DSL port connects to the ADSL line. Ethernet , 2, 3, 4 These Ethernet ports (1, 2, 3, 4) connect the Gateway to wired computers and other Ethernet network devices. Reset There are two ways to reset the Gateway's factory defaults. Either press and hold the Reset button for approximately five seconds, or restore the defaults from the Administration > Factory Defaults screen of the Gateway's web-based utility. Power The Power port is where you will connect the power adapter.

Front Panel Power (Green) The Power LED lights up and stays on while the Gateway is powered on. Ethernet -4 (Green) These numbered LEDs, corresponding with the numbered ports on the Gateway's back panel, serve two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through that port. It flashes to indicate network activity over that port. W-F Protected Setup Button Press this button to cause Wi-Fi Protected Setup to search for your Wi-Fi Protected Setup-supported wireless device.

NOTE: Wi-Fi Protected Setup is a feature that makes it easy to configure your wireless network and its security settings. For more information, refer to "Wireless > Basic Wireless Settings" in the "Advanced Configuration" chapter. Wreless (Green) The Wireless LED lights up when the wireless feature is enabled. It flashes when the Gateway is actively sending or receiving data over the network. DSL (Green) The DSL LED lights up whenever there is a successful DSL connection. The LED flashes while the Gateway is establishing the ADSL connection. Wreless-N ADSL2+ Gateway Chapter2 Wireless Security Checklist Chapter 2: Wreless Securty Checklst Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.

4. Enable encrypton Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication. A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment. WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

. Change the default wreless network name or SSID Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use lnksys as the default wireless network name.

You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks. General Network Security Guidelines Wireless network security is useless if the underlying network is not secure. · · · · Password protect all computers on the network and individually password protect sensitive files. Change passwords on a regular basis. Install anti-virus software and personal firewall software.

Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge. 2. Change the default password For wireless products such as access points, routers, and gateways, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory.

The Linksys default password is admn. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess. Additional Security Tips · · Keep wireless routers, access points, or gateways away from exterior walls and windows. Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations). Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary. · 3. Enable MAC address flterng Linksys routers and gateways give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device.

With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network. Wreless-N ADSL2+ Gateway WEB: For more information on wireless security, visit www.lnksys.com/securty ield. Then, press Enter. A login screen appears. Use the default user name and password, admn, unless you have changed them during the Setup Wizard. (You can set a new user name and password from the Administration tab's Management screen.) Click OK to continue.

Setup > Basic Setup Internet Setup The Internet Setup section configures the Gateway to your Internet connection. Most of this information can be obtained through your ISP. Internet Connection Type Encapsulaton Select the appropriate encapsulation method from the drop-down menu. Each Basic Setup screen and available features will differ depending on which encapsulation method you select. These are the available methods: · · · · · · RFC 2364 PPPoA RFC 2516 PPPoE RFC 1483 Routed IPoA RFC 1483 Bridged Bridged Mode Only Gateway Login If you are unable to log in, press the Reset button on the back panel for at least 5 seconds, then wait for the device to reset and try again.

VC Settings Configure your Virtual Circuit (VC) settings in this section. Multplexng Select LLC or VC, depending on your ISP. net connection terminates. The default Max Idle Time is minutes. Keep Alve - Redal Perod 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, select Keep Alve. 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. Internet Connection Type > IPoA IP Settings Your ISP provides these settings. Internet IP Address Enter the Gateway's IP address, as seen from the Internet. Subnet Mask Enter the Gateway's Subnet Mask, as seen from the Internet (including your ISP). Default Gateway Enter the IP address of the ISP server. Prmary (Requred) and Secondary (Optonal) DNS Enter the DNS (Domain Name System) server IP address(es) provided by your ISP. At least one is required.

RFC 1483 Routed If you are required to use RFC 1483 Routed, then select RFC 483 Routed. RFC 1483 Bridged If you are required to use RFC 1483 Bridged, then select RFC 483 Brdged. Internet Connection Type > RFC 1483 Routed IP Settings Your ISP provides these settings. Internet IP Address Enter the Gateway's IP address, as seen from the Internet. Subnet Mask Enter the Gateway's Subnet Mask, as seen from the Internet (including your ISP). Default Gateway Enter the IP address of the ISP server. Prmary (Requred) and Secondary (Optonal) DNS Enter the DNS (Domain Name System) server IP address(es) provided by your ISP. At least one is required. Internet Connection Type > RFC 1483 Bridged IP Settings Select Automatcally obtan an IP address if your ISP says you are connecting through a dynamic IP address. If you are required to use a permanent (static) IP address to connect to the Internet, then select Use the followng IP Address.

Your ISP provides the settings needed for the following fields: 6 IPoA If you are required to use IPoA (IP over ATM), then select IPoA. Wreless-N ADSL2+ Gateway Chapter4 Advanced Configuration Network Setup The Network Setup section changes the settings on the network connected to the Gateway's Ethernet ports. Wireless setup is performed through the Wireless tab. Internet IP Address Enter the Gateway's IP address, as seen from the Internet. Subnet Mask Enter the Gateway's Subnet Mask, as seen from the Internet (including your ISP).

Default Gateway Enter the IP address of the ISP server. Prmary (Requred) and Secondary (Optonal) DNS Enter the DNS (Domain Name System) server IP address(es) provided by your ISP. At least one is required. Gateway 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.

Bridged Mode Only If you are using your Gateway as a bridge, which makes the Gateway act like a stand-alone modem, select Brdge Mode Only. All NAT and routing settings are disabled in this mode. Gateway IP Local IP Address The default value is 92.68... Subnet Mask The default value is 2.2.2.0.

Network Address Server Settings (DHCP) The settings allow you to configure the Gateway's Dynamic Host Configuration Protocol (DHCP) server function. The Gateway can be used as a DHCP server for your network.

A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Gateway's DHCP server option, make sure there is no other DHCP server on your network. Internet Connection Type > Bridged Mode Only Optional Settings Some of these settings may be required by your ISP. Verify with your ISP before making any changes. Optional Settings Host Name and Doman Name These fields allow you to supply a host and domain name for the Gateway. Some ISPs, usually cable 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 MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the Gateway select the best MTU for your Internet connection, keep the default, Auto. Sze When Manual is selected in the MTU field, this option is enabled.
Leave this value in the 1200 to 1500 range. The default, MTU is configured automatically. Network Address Server Settings (DHCP) DHCP Server 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, Linksys recommends that you keep the default, Enable. You can also use the Gateway in DHCP Relay mode.
(This setting is not available for all encapsulation types.) DHCP Relay Server IP Enter the DHCP server IP address to relay DHCP requests from the local network when the Gateway is in DHCP Relay mode. Startng IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Gateway's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.

168.1.253. The default is 92.68..00. Maxmum Number of DHCP Users Enter the maximum number of users (network devices) that can obtain an IP address. The number will vary depending on the starting Wreless-N ADSL2+ Gateway Chapter4 Advanced Configuration DDNS DDNS Service If your DDNS service is provided by DynDNS.org, then select DynDNS.
org from the drop-down menu. If your DDNS service is provided by TZO, then select TZO.com. The features available on the DDNS screen will vary, depending on which DDNS service provider you use. IP address entered and cannot be greater than 253.
The default is 0. Clent Lease Tme The Client Lease Time is the amount of time a network device will be allowed connection to the Gateway with its current dynamic IP address. Enter the number of minutes that the device will be "leased" this dynamic IP address. After the time is up, the device will be automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day.
Statc DNS -3 The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. At least one DNS server IP address is provided by your ISP. You can enter up to three DNS server IP addresses here. The Gateway 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. DynDNS.org Time Settings Tme Zone Select the time zone in which your network functions. Automatcally adjust clock for daylght savng tme Select this option if you want the Gateway to automatically adjust for daylight saving time.

Setup > DDNS > DynDNS User Name Enter the User Name for your account. Password Enter the Password for your account. Host Name Enter the DDNS URL assigned by the service. Status Displays the status of the DDNS service connection. Connect To manually trigger an update, click this button. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Time Settings and Language Language Language To use a different language, select one from the drop-down menu. The language of the web-based utility will change five seconds after you select another language. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. TZO.
com Setup > DDNS 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 with a DDNS service provider, www.dyndns.
org or www.TZO.com. If you do not want to use this feature, keep the default, Dsabled. Setup > DDNS > TZO E-Mal Address Enter the E-mail Address for your account.
TZO Password Enter the Password for your account. Doman Name Enter the DDNS URL assigned by the service. Status Displays the status of the DDNS service connection. Connect To manually trigger an update, click this button. Wreless-N ADSL2+ Gateway 8 Chapter4 Advanced Configuration Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Setup > MAC Address Clone A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Gateway with the MAC Address Clone feature. Setup > Advanced Routing Advanced Routing Operating Mode NAT If this Gateway is hosting your network's connection to the Internet, keep the default, Enable. If another gateway or router exists on your network, select Dsable.

Dynamic Routing Setup > MAC Address Clone Enable/Dsable To have the MAC Address cloned, click the radio button beside Enable. MAC Address Enter the MAC Address registered with your ISP here. Clone My Computer's MAC Clicking this button will clone the MAC address. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. RIP This allows the Gateway to automatically adjust to physical changes in the network's layout and exchange routing tables with other router(s). The Gateway determines the packets' route based on the fewest number of hops between source and destination. Select Enable to use Dynamic Routing. Otherwise, keep the default, Dsable. RIP Send Packet Verson, and RIP Receved Packet Verson Select the appropriate protocol version, RIP v or RIP v2. This should match the version supported by other routers on your LAN.
Setup > Advanced Routing The Advanced Routing screen is used to set up the Gateway's advanced routing functions. It contains three sections: Operating Mode, Dynamic Routing, and Static Routing.

Static Routing A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the following information to set up a new static route. Select Set Number To set up a static route between the Gateway and another network, select a number from the drop-down list.

The Gateway supports up to 20 static route entries. Click Delete Ths Entry to delete a static route. Destnaton IP Address The Destination IP Address is the IP 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 determines which portion of a Destination IP Address is the network portion, and which portion is the host portion. Wreless-N ADSL2+ Gateway 9 Chapter4 Advanced Configuration Network Mode Select the wireless standards running on your network. If you have Wireless-G and Wireless-B devices in your network, keep the default, Mxed. If you do not have any wireless devices, select Dsable. Network Name (SSID) The network name is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Linksys recommends that you change the default, lnksys, to a unique name of your choice. Rado Band For best performance in a network using Wireless-N, Wireless-G and Wireless-B devices, keep the default, Wde - 40MHz Channel. For Wireless-G and Wireless-B networking only, select Standard - 20MHz Channel. NOTE: If you select Wde - 40MHz Channel for the Radio Band setting, then Wireless-N can use two channels: a primary one (Wide Channel) and a secondary on (Standard Channel). This will enhance Wireless-N performance.

Advanced Routing > Routing Table Gateway The IP address of the gateway device that allows contact between the Gateway and remote network or host. Hop Count This is the number of hops to each node until the destination is reached (16 hops maximum). Enter the appropriate Hop Count. Click Show Routng Table to view the static routes you have already set up. Routing Table For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click Refresh to update the information. Click Close to exit this screen. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Wde Channel If you selected Wde - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu.

Standard Channel Select the channel for Wireless-N, Wireless-G, and Wireless-B networking. If you selected Wde 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. If you are not sure which channel to select, do not make any changes. SSID Broadcast When wireless devices survey the local area for wireless networks to associate with, they will detect the wireless network name or SSID broadcast by the Gateway. If you want to broadcast the Gateway's SSID, keep the default, Enable.

Otherwise, select Dsable. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Wireless > Basic Wireless Settings The basic settings for wireless networking are set on this screen. This screen allows you to choose your wireless network mode and wireless security. Wi-Fi Protected Setup If you set the Wireless Configuration to W-F Protected Setup, the Basic Wireless Settings screen displays the fields shown below. Wireless > Basic Wireless Settings Basic Wireless Settings Wreless Confguraton Keep the default selection, Manual, to configure your wireless network manually. Select W-F Protected Setup to set up your wireless network using Wi-Fi Protected Setup. Manual If you set the Wireless Configuration to Manual, the Basic Wireless Settings screen displays the following fields. Wreless-N ADSL2+ Gateway Wireless > Basic Wireless Settings - Wi-Fi Protected Setup 0 Chapter4 Advanced Configuration Encrypton The method is TKIP or AES. Pre-Shared Key Enter a key of 8 to 63 characters. Key Renewal Enter how often the Gateway should change encryption keys. The default is 3600 seconds. Configure your wireless network by adding your Wi-Fi Protected Setup-supported devices one at a time, using the appropriate method listed below: · The devce has a W-F Protected Setup button Press the Wi-Fi Protected Setup button, then click the Wi-Fi Protected Setup button on the screen. Searching..

. is displayed while the Gateway searches for your device. The devce has a W-F Protected Setup PIN number Enter the PIN number in the field provided on the screen. The devce asks for the Gateway's PIN number Enter the PIN number displayed on the screen. WPA-Personal (WPA2-Personal recommended) · · Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Wireless > Wireless Security The Wireless Security screen configures the security of your wireless network(s). The supported wireless security modes are WPA2-Personal, WPA-Personal, WPA2-Mixed, WPA2-Enterprise, WPA-Enterprise, RADIUS, and WEP. WPA (Wi-Fi Protected Access), is a security standard stronger than WEP (Wired Equivalent Privacy) encryption. WPA2 is a more advanced, more secure version of WPA. WPAEnterprise, WPA2-Enterprise, and RADIUS use a RADIUS (Remote Authentication Dial-In User Service) server for authentication.

For detailed instructions on configuring wireless security on the Gateway, refer to "Chapter 2: Wireless Security". Security Mode > WPA-Personal Encrypton The method is TKIP or AES. Pre-Shared Key Enter a key of 8 to 63 characters. Key Renewal Enter a Key Renewal period, which instructs the Gateway how often it should change the encryption keys. The default is 3600 seconds.

WPA2-Mixed This option allows clients to use EITHER WPA-Personal OR WPA2-Personal. Wireless Security Securty Mode Select the security method for your wireless network. Proceed to the appropriate instructions. If you do not want to use wireless security, keep the default, Dsabled. NOTE: If you use wireless security, remember that each device in your wireless network MUST use the same security method and settings, or else the wireless devices cannot communicate.

Security Mode > WPA2-Mixed WPA2-Personal (Recommended) Encrypton The method is TKIP or AES. Pre-Shared Key Enter a key of 8 to 63 characters. Key Renewal Enter a Key Renewal period, which instructs the Gateway how often it should change the encryption keys. The default is 3600 seconds.

WPA2-Enterprise WPA2-Enterprise features WPA2 used with a RADIUS server. (This method should only be used when the device is connected to a RADIUS server.) Security Mode > WPA2-Personal Wreless-N ADSL2+ Gateway Chapter4 Advanced Configuration RADIUS (WPA2-Enterprise recommended) Security Mode > WPA2-Enterprise Encrypton The method is TKIP or AES.

RADIUS Server Enter the IP address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. Shared Key Enter the key shared between the device and its RADIUS server.

Key Renewal Enter the Key Renewal period, which tells the device how often it should change the dynamic encryption keys. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Security Mode > RADIUS This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the device.) RADIUS Server Enter the IP address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. Shared Key Enter the key shared between the device and its RADIUS server. Encrypton Select the appropriate level of encryption, 40/64-bt (0 hex dgts) or 04/28-bt (26 hex dgts). A higher level of encryption is more secure. Passphrase Instead of manually entering WEP keys, you can enter a Passphrase.

It is case-sensitive and should not be longer than 32 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only and cannot be used 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 keys generated, and enter the appropriate one manually in the wireless computer or client.) If you want to use a Passphrase, then enter it in the Passphrase field and click the Generate button. Keys -4 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 40/64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 104/128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F". TX Key To indicate which WEP key to use, select a default Transmit (TX) Key number.

Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. 2 WPA-Enterprise (WPA2-Enterprise recommended) WPA-Enterprise features WPA used with a RADIUS server. (This method should only be used when the device is connected to a RADIUS server.) Security Mode > WPA-Enterprise Encrypton. The method is TKIP or AES. RADIUS Server Enter the RADIUS server's IP address. RADIUS Port Enter the RADIUS server's port number. Shared Key Enter the key shared between the device and its RADIUS server. Key Renewal Enter the Key Renewal period, which tells the device how often it should change the dynamic encryption keys. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes.

Wreless-N ADSL2+ Gateway Chapter4 Advanced Configuration Wireless > Wireless MAC Filter Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius. WEP (WPA2-Personal recommended) Security Mode > WEP Encrypton Select a level of WEP encryption, 64-bt or 28-bt. Passphrase Enter a Passphrase to automatically generate WEP keys. Then click Generate. NOTE: The WEP Passphrase is compatible with Linksys wireless products only. If you are use nonLinksys products, manually enter the appropriate WEP key on those devices. Key -4 If you did not enter a Passphrase, enter the WEP key(s) manually. TX Key Select which TX (Transmit) Key to use. The default is . Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes.

Wireless > Wireless MAC Filter Wireless MAC Filter To filter wireless users by MAC Address, either permitting or blocking access, click Enable. If you do not wish to filter users by MAC Address, select Dsable. Access Restrictions Block Click this button to block wireless access from the devices listed on this screen. Permt Click this button to allow wireless access by the devices listed on this screen. MAC Address Filter List Click Wreless Clent Lst to display the Wireless Client List screen.

This screen lists the computers and other devices on the wireless network sorted by IP address. You can also sort the list by Client Name, Interface, MAC Address, or Status, by using the To Sort By drop-down menu. Wreless-N ADSL2+ Gateway 3 Chapter4 Advanced Configuration use a WEP key for authentication. Select Shared Key to only use Shared Key authentication. Basc Rate The Basic Rate setting is not actually one rate of transmission but a series of rates at which the device can transmit.

The device will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The device will also advertise that it will automatically select the best rate for transmission. The default setting is Default, when the device can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are -2Mbps, for use with older wireless technology, and All, when the device can transmit at all wireless rates. Transmsson Rate 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 you can select Auto to have the device automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the device and a wireless client. The default setting is Auto. N Transmsson Rate The rate of data transmission should be set depending on the speed of your Wireless-N networking.

You can select from a range of transmission speeds, or you can select Auto to have the device automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the device and a wireless client. The default setting is Auto. CTS Protecton Mode CTS (Clear-To-Send) Protection Mode's default setting is Dsable. Select Auto so the device will automatically use CTS Protection Mode when your Wireless-N and Wireless-G products are experiencing severe problems and are not able to transmit to the device in an environment with heavy 802.11b traffic. This function boosts the device's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance. Beacon Interval 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(s).

The default value is 00. DTIM Interval 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.
The default value is . Fragmentaton Threshold This value specifies the maximum size for a packet before data is fragmented 4 Wireless Client List To add a device to the MAC Address Filter List, click the device's Add to MAC Flter Lst checkbox, then click Add. To retrieve the most up-to-date information, click Refresh. To exit this screen and return to the Wireless MAC Filter screen, click Close. MAC 0-0 Enter the MAC addresses of the devices whose wireless access you want to block or allow.
Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Wireless > Advanced Wireless Settings The Advanced Wireless Settings screen is used to set up the Gateway's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance. Wireless > Advanced Wireless Settings Advanced Wireless AP Isolaton This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Gateway but not with each other. To use this function, click Enable. AP Isolation is disabled by default. Authentcaton Type The default is Auto, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient Wreless-N ADSL2+ Gateway Chapter4 Advanced Configuration Flter Cookes A cookie is data stored on your computer and used by Internet sites when you interact with them.

Select Flter Cookes to filter cookies. Deselect the feature to allow cookie usage. Flter ActveX 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. Select Flter ActveX to enable ActiveX filtering. Deselect the feature to allow ActiveX usage. 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 reduction of the default value is recommended. In most cases, it should remain at its default value of 2346. RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default, 2346, is 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.
The RTS Threshold value should remain at its default value of 2346. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Block WAN Requests Block Anonymous Internet Requests This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature to allow anonymous Internet requests.
Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Security > Firewall The Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the Gateway's local network. Security > VPN Passthrough The VPN Passthrough screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Gateway's firewall. Security > VPN Passthrough Security > Firewall Firewall SPI Frewall Protecton To use firewall protection, keep the default selection, Enable. To turn off firewall protection, select Dsable. 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 tunnels to pass through the Gateway, keep the default, Enable. PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Gateway, keep the default, Enable. L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level.

To allow L2TP tunnels to pass through the Gateway, keep the default, Enable. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Filters Flter Proxy Use of WAN proxy servers may compromise the Gateway's security. Denying Proxy will disable access to any WAN proxy servers. Select Flter Proxy to enable proxy filtering. Deselect the feature to allow proxy access. Flter Java Applets Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. Select Flter Java Applets to enable Java filtering. Deselect the feature to allow Java usage.
Wreless-N ADSL2+ Gateway Chapter4 Advanced Configuration Status Policies are disabled by default. To enable a policy, select its number from the drop-down menu, and select Enable. To create a policy, follow steps 1-10. Repeat these steps to create additional policies, one at a time. 1.
Select a number from the Internet Access Policy dropdown menu. 2. To enable this policy, select Enable. 3. Enter a Policy Name in the field provided.
4. Click Edt Lst of Computers to select which computers will be affected by the policy. The Internet Access PC List screen appears. You can select a computer by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of computers. After making your changes, click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Then click Close. Access Restrictions > Internet Access Policy The Internet Access Policy screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times. Access Restrictions > Internet Access Policy Internet Access Policy Internet Access Polcy Access can be managed by a policy. Use the settings on this screen to establish an access policy (after Save Settngs is clicked).

Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click Delete. To view all the policies, click Summary. Internet Access PC List 5. @@@@6. Specify when this policy will be in effect. Select the days: individual days of the week, or Every Day. @@7. @@8. @@9.
@@@@@@To delete a policy, select Delete. @@Click Save Settngs to save the policy's settings. @@@@Some Internet applications may not require any forwarding.) Applications and Gaming > Single Port Forwarding The Single Port Forwarding screen allows you to customize port services for common applications.

Applications and Gaming > Single Port Forwarding When users send these types of requests to your network via the Internet, the Gateway will forward those requests to the appropriate servers (computers).
Applications and Gaming > Port Range Forwarding Single Port Forwarding To forward a port, enter the information on each line for the criteria required. Applcaton Enter the name you wish to give the application. Each name can be up to 12 characters. @@@@@@Enable For each application, select Enable to enable port forwarding. @@@@@@@@Each name can be up to 12 characters.
@@@@@@@@@@@@@@To expose one PC, select Enable. @@@@Applcaton Name Enter the application name of the trigger.
@@@@@@@@@@@@@DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding feature is more secure Wreless-N ADSL2+ Gateway Applications and Gaming > QoS 8 Chapter4 Advanced Configuration Click the Add button to save your changes. Your new entry will appear in the Summary list. Wireless Network The Gateway features Wi-Fi Multimedia (WMMTM) Support. The No Acknowledgement feature is available only when the WMM Support feature is enabled. WMM Support Wi-Fi Multimedia is a QoS feature defined by WiFi Alliance before IEEE 802.11e was finalized. Now it is part of IEEE 802.

11e. When it is enabled, it provides four priority queues for different types of traffic. It automatically maps the incoming packets to the appropriate queues based on QoS settings (in IP or layer 2 header). WMM provides the capability to prioritize traffic in your environment. If you have other devices on your network that support WMM, keep the default, Enable. Otherwise, select Dsable. No ACK If you want to disable the Gateway's Acknowledgement feature, so the Gateway will not resend data if an error occurs, then keep the default, Enable. Otherwise, select Dsable. Add a New Application or Game Add a New Application Internet Access Priority Enable/Dsable To use the QoS policies you have set, select Enable. Otherwise, select Dsable.
Set Internet Bandwdth This is used to set your Internet connection's bandwidth. Select Auto (default) to set the bandwidth automatically. To set the bandwidth manually, select Manual, then enter the bandwidth in kbps. Add a New Game Enter a Name Enter any name to indicate the name of the entry. Port Range Enter the port range used by the application or game.
For example, to allocate bandwidth for FTP, enter 21-21. If you need services for an application or game that uses ports 1000 to 1250, enter 1000-1250. You can have up to three ranges per bandwidth allocation. Port numbers range from 1 to 65535. Check the application's or game's documentation for details on service ports used.
In the drop-down menu, select the protocol TCP or UDP, or select Both. Prorty Select the appropriate priority: Hgh, Medum, Normal, or Low. The default is Medum. Click the Add button to save your changes. Your new entry will appear in the Summary list. Category Select one of these categories: Applcatons, Onlne Games, MAC Address, Ethernet Port, or Voce Devce. Then proceed to the instructions below for your selection. For each category, you can set the bandwidth priority to one of four levels: Hgh, Medum, Normal, or Low. Be careful not to set all your applications to High priority, as this will defeat the purpose of allocating the available bandwidth. For below-normal bandwidth, select Low.

Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority. Online Games Applications Applcatons Select the appropriate application: MSN Messenger, Skype, or Yahoo Messenger. For any other application, select Add a New Applcaton, then fill in the Enter a Name and Port Range fields as detailed below in "Add a New Application or Game". @@@@Prorty Select the appropriate priority: Hgh, Medum, Normal, or Low. @@@@@@@@@@MAC Address Enter the MAC address of your device. Prorty Select the appropriate priority: Hgh, Medum, Normal, or Low. The default is Medum. Click the Add button to save your changes. @@Prorty Select the appropriate priority: Hgh, Medum, Normal, or Low. The default is Medum.
Click the Add button to save your changes. @@MAC Address Enter the MAC address of your voice device. Prorty Select the appropriate priority: Hgh, Medum, Normal, or Low. The default is Medum. Click the Add button to save your changes.
@@The default User Name and password are admn. User Lst Select the number of the user. The default is user . Gateway User Name Enter the default Gateway User Name, admn. @@Re-Enter to Confrm Enter the Gateway Password again to confirm.
For non-admin users, select a different user number, and then configure the Gateway User Name and Password settings. Summary This lists the QoS entries you have created for your applications and devices. Prorty This displays the bandwidth priority of Hgh, Medum, Normal, or Low. Name This displays the application, device, or port name. Wreless-N ADSL2+ Gateway 20 Chapter4 Advanced Configuration Remote Access Remote Management To permit remote access to the Gateway from outside the local network, select Enable. Otherwise, keep the default, Dsable. Management Port Enter the port number that will be open to outside access. NOTE: To manage the Gateway remotely, enter https://<Internet_IP_address>:port substituting the Gateway's Internet IP address for <Internet_IP_address>, and the Management Port number for port. Administration > Reporting UPnP Universal Plug and Play (UPnP) allows Windows XP and Vista to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing. UPnP If you want to use UPnP, keep the default, Enable.

Otherwise, select Dsable. Reporting Log To disable the Log function, keep the default, Dsable. To monitor traffic between the network and the Internet, select Enable. With logging enabled, you can choose to view temporary logs. E-Mal Alerts To enable E-Mail Alerts, select Enable. Denal of Servce Thresholds Enter the number of Denial of Service attacks that will trigger an e-mail alert. SMTP Mal Server Enter the IP address of the SMTP server. E-Mal Address for Alert Logs Enter the e-mail address that will receive alert logs. Return E-Mal address Enter the return address for the e-mail alerts. (This can be a dummy address.) Vew Log To view the logs, click Vew Log. WLAN If you are using the Gateway in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Gateway's web-based utility. Management va WLAN This feature allows the Gateway to be managed by a wireless computer on the local network when it logs into the Gateway's web-based utility. You will only be able to access the utility via a wired connection if you disable this feature. To allow wireless access to the utility, keep the default, Enable.
Otherwise, select Dsable. IGMP IGMP Proxy Internet Group Membership Protocol (IGMP) is a system to improve multicasting for wireless clients.

This should be set to Enable if your clients support it; otherwise, select Dsable. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. View Log Administration > Reporting The Gateway can keep logs of traffic and events for your Internet connection.
Log Type Select from the following: ALL, System Log, Access Log, Frewall Log, or VPN Log. Click Refresh to update the log. Click Clear to clear all the information that is displayed. Click Prevous Page to view the previous page of information. Click Next Page to view the next page of information. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Wreless-N ADSL2+ Gateway 2 Chapter4 Advanced Configuration Administration > Back Up & Restore The Back Up & Restore screen allows you to back up or restore the Gateway's settings using a configuration file. Administration > Diagnostics The ping test allows you to check the connections of your network devices, including connection to the Internet. Administration > Diagnostics Administration > Back Up & Restore Ping Test Ping Test Parameters The ping test checks the status of a connection. Png Target IP Enter the IP address that you want to ping.

This can be either a local (LAN) or Internet (WAN) IP address. Png Sze Enter the packet size you want to use. The default is 60 bytes. Number of Pngs Enter how many times you want to ping. The default is . Png Interval Enter the number of milliseconds between pings. The default is 000 milliseconds. Png Tmeout Enter the number of milliseconds before the ping test will time out. The default is 000 milliseconds. Start Test To run the test, click this button.
The Ping Test screen will show if the test was successful. Click Close to return to the Diagnostics screen. Back Up Configuration Back Up To save the Gateway's settings in a configuration file, click Back Up and follow the on-screen instructions. Restore Configuration To use this option, you must have previously backed up its configuration settings. Select a fle to restore Click the Browse button and select the Gateway's configuration file.
Restore To restore the Gateway's configuration settings, click this button and follow the on-screen instructions. Administration > Factory Defaults This screen allows you to restore the Gateway's configuration to its factory default settings. Administration > Factory Defaults Diagnostics > Ping Png Result The results of the ping test are displayed. Click Save Settngs to apply your changes, or click Cancel Changes to cancel your changes. Wreless-N ADSL2+ Gateway NOTE: Restoring factory defaults deletes all custom settings.
To retain your custom settings, use the Administration > Backup & Restore screen to back up the settings before you restore the factory defaults. 22 Chapter4 Advanced Configuration Status > Gateway The Gateway screen displays information about the Gateway and its current settings. Factory Defaults Restore Factory Defaults To reset settings to the default values, click this button and follow the on-screen instructions. Any custom Gateway settings you have saved will be lost when the default settings are restored. Administration > Firmware Upgrade Status > Gateway Administration > Firmware Upgrade Gateway Information Frmware Verson The version number of the Gateway's current firmware is displayed. MAC Address The Gateway's MAC address, as seen by your ISP, is displayed. Current Tme The time set on the Gateway is displayed. The Firmware Upgrade screen allows you to upgrade the Gateway's firmware. Do not upgrade the firmware unless you are experiencing problems with the Gateway or the new firmware has a feature you want to use. Firmware Upgrade Before upgrading the firmware, download the Gateway's firmware upgrade file from the Linksys website, www.

linksys.com/international. Then extract the file. Select a Fle to Upgrade Click Browse and select the extracted firmware upgrade file. Upgrade After you have selected the appropriate file, click this button, and follow the on-screen instructions. Language To use a different language, select one from the drop-down menu. The web-based utility will switch to the new language five seconds after your selection is made. Internet Connection This section shows the current network information stored in the Gateway. The information varies depending on the Internet connection type selected on the Basic Setup screen. Click Refresh to update the on-screen information.
Status > Local Network The Local Network screen displays information about the local wired network. Status > Local Network Wreless-N ADSL2+ Gateway 23 Chapter4 Advanced Configuration ARP/RARP Table An ARP request is a request sent by the Gateway asking local network devices with IP addresses for their MAC addresses, so the Gateway can map IP addresses to MAC addresses. RARP is the reverse of ARP. (This data is stored in temporary memory and changes periodically.) To retrieve the most up-to-date information, click Refresh.
To exit this screen and return to the Local Network screen, click Close. Local Network MAC Address The MAC address of the Gateway's local, wired interface is displayed. IP Address The Gateway's IP address, as it appears on your local network, is displayed. Subnet Mask The Subnet Mask of the Gateway is displayed. DHCP Server DHCP Server The status of the Gateway's DHCP server function is displayed.
Start IP Address For the range of IP addresses used by devices on your local network, the starting IP address is displayed. End IP Address For the range of IP addresses used by devices on your local network, the ending IP address is displayed. DHCP Clent Table Click this button to view a list of devices that are using the Gateway as a DHCP server. Status > Wireless Network The Wireless Network screen displays information about your wireless network. Status > Wireless Network Wireless Network DHCP Client Table MAC Address The wireless MAC address of the Gateway's local, wireless interface is displayed. Mode The wireless network mode of the Gateway is displayed. Network Name (SSID) The wireless network name, which is also called the SSID, is displayed. Rado Band The channel bandwidth setting selected on the Basic Wireless Settings screen is displayed. Wde Channel The wide channel of the wireless network is displayed. Standard Channel The standard channel of the wireless network is displayed.

Securty The wireless security method is displayed. SSID Broadcast displayed. The status of SSID Broadcast is DHCP Client Table The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Gateway. The list displays Client Host Name, IP Address, MAC Address, and Expires time (how much time is left for the current IP address). To remove a DHCP client, click Delete.

To retrieve the most up-to-date information, click Refresh. To exit this screen and return to the Local Network screen, click Close. ARP/RARP Table Click this button to view the current IP and MAC addresses of the Gateway's local network clients. ARP/RARP Table Wreless-N ADSL2+ Gateway 24 Chapter4 Advanced Configuration Enable The number of Permanent Virtual Circuits (PVC) is displayed. PVC Status The status of the PVC is displayed. Status > DSL Connection The DSL screen displays information about your DSL connection. Status > DSL Connection DSL Connection Status The status of the DSL connection is displayed. Downstream Rate The download speed of traffic from the Internet to the Gateway is displayed. Upstream Rate The upload speed of traffic from the Gateway to the Internet is displayed. For ADSL connection, the Upstream Rate is typically 25% of the Downstream Rate. NOTE: The Downstream and Upstream Rates are affected by distance from and configuration of the DSL central office. PVC Connection Encapsulaton The Encapsulation setting selected on the Basic Setup screen is displayed. Multplexng The Multiplexing setting selected on the Basic Setup screen is displayed. QoS The QoS method selected on the Basic Setup screen is displayed. PCR The PCR value entered on the Basic Setup screen is displayed. SCR The SCR value entered on the Basic Setup screen is displayed. Autodetect The Autodetect setting selected on the Basic Setup screen is displayed. VPI The VPI value entered on the Basic Setup screen is displayed. VCI The VCI value entered on the Basic Setup screen is displayed. Wreless-N ADSL2+ Gateway 2 AppendixA Troubleshooting You need to modify the basic settings on the Gateway. Run the Setup Wizard on the Setup CD-ROM. You need to modify the advanced settings on the Gateway. Open the web browser (for example, Internet Explorer or Firefox), and enter the Gateway's IP address in the address field (the default IP address is 92.68..

). When prompted, complete the User name and Password fields (the default user name and password is admn). Click the appropriate tab to change the settings Appendx A: Troubleshootng Your computer cannot connect to the Internet. Follow the instructions until your computer can connect to the Internet: · · Make sure that the Gateway is powered on. The Power LED should be green and not flashing. If the Power LED is flashing, then power off all of your network devices, including the Gateway and computers. Then power on each device in the following order: 1. 2. Gateway Computer WEB: If your questions are not addressed here, refer to the Linksys www.lnksys. com/nternatonal website, · Check the LEDs on the front panel of the Gateway. Make sure the Power, DSL, and at least one of the numbered LEDs are lit. If they are not, then check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Gateway, and the Line port of the Gateway must be connected to the ADSL line. When you double-click the web browser, you are prompted for a username and password. If you want to get rid of the prompt, follow these instructions. Launch the web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers): 1. 2. 3. 4. Select Tools > Internet Optons. Click the Connectons tab. Select Never dal a connecton. Click OK. You are using a static IP address and cannot connect. Refer to Windows Help and change your Internet Protocol (TCP/IP) Properties to Obtain an IP address automatically. The computer cannot connect wirelessly to the network. Make sure the wireless network name or SSID is the same on both the computer and the Gateway. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Gateway. Wreless-N ADSL2+ Gateway 26 AppendixB Specifications Appendx B: Specfcatons Model Number Standards WAG160N Draft 802.

11N, IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, g.992.1 (g.dmt), g.992.2 (g.lite), g. 992.3, g.992.5, T1.413i2 Issue 2, U-R2 for Annex B Power, DSL, Ethernet (1-4) Reset, Wi-Fi Protected Setup CAT5 UTP, RJ-45, RJ-11 Power, Wireless, Ethernet (1-4), DSL, Internet 2 internal 17 dBm 2 dBi Ports Buttons Cabling Type LEDs Antennas Transmit Power Antenna Gain Security Features Password-Protected Configuration for Web Access PAP and CHAP Authentication Denial of Service (DoS) Prevention SPI Firewall AP Isolation URL Filtering, and Keyword, Java, ActiveX, Proxy, Cookie Blocking ToD Filter (Blocks Access by Time) VPN Passthrough for IPSec, PPTP, and L2TP Protocols WPA, WPA2 Personal and Enterprise 128, 64 Bits WEP with Passphrase WEP Key Generation SSID Broadcast Disable Access Restriction by MAC and IP Addresses Envronmental Dimensions Weight Power Certification Operating Temp. Storage Temp. Operating Humidity 202 x 34 x 160 mm (8.0" x 1.3" x 6.3") 362 g (12. 8 oz) 12VDC, 1A FCC, CE, IC-03, Wi-Fi, A-Tick, Telepermit, IDA 0 to 40°C (32 to 104°F) -20 to 70°C (-4 to 158°F) 10 to 85% Noncondensing Storage Humidity 5 to 90% Noncondensing Wreless-N ADSL2+ Gateway 2 AppendixC Warranty Information TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You. Ths Warranty s vald and may be processed only n the country of purchase. Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623. Appendx C: Warranty Informaton Linksys warrants to You that, for a period of two years (the "Warranty Period"), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates.

This limited warranty extends only to the original purchaser. If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase.