LINKSYS®
A Division of Cisco Systems, Inc.

2,4GHz 802.11g

Wireless-G

WIRELESS

ADSL Gateway with SRX200

User Guide

Model No. **WAG54GX2 (EU)**

CISCO SYSTEMS

Copyright and Trademarks

How to Use this Guide

Your Guide to the Wireless-G ADSL Gateway with SRX200 has been designed to make understanding networking with the Gateway easier than ever. Look for the following items when reading this User Guide:

This checkmark means there is a Note of interest and is something you should pay special attention to while using the Gateway.

This exclamation point means there is a Caution or Warning and is something that could damage your property or the Gateway.

This question mark provides you with a reminder about something you might need to do while using the Gateway.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G ADSL Gateway with SRX200. This Gateway will provide your computers with a high-speed Internet connection as well as resources, including files and printers.

How does the Gateway do all of this? By connecting the Internet, as well as your computers and peripherals, to the Gateway, then the Gateway can direct and control communications for your network. Plus, since the Gateway is wireless, Internet access can be shared over the wireless broadcast as well as the wired network.

The Wireless-G ADSL Gateway with SRX200 combines smart antenna technology with standards-based, Wireless-G (802.11g) networking. By overlaying the signals of two Wireless-G compatible radios, the "Multiple In, Multiple Out" (MIMO) technology effectively doubles the data rate. Unlike ordinary wireless networking technologies that are confused by signal reflections, MIMO actually uses these reflections to increase the range and reduce "dead spots" in the wireless coverage area. The robust signal travels farther, maintaining wireless connections up to two times farther than standard Wireless-G. And the farther away you are, the more advantage you get—the higher data rate and reflection-friendly technology can yield up to six times more throughput than Wireless-G in some situations. The Gateway avoids interference by dynamically switching to the clearest channel available. Even your standard Wireless-G and -B equipment will work better when communicating with SRX-enabled devices.

To protect your data and privacy, WPA encryption provides greater wireless security opportunities while the whole network is protected through a Stateful Packet Inspection (SPI) firewall and NAT technology. In addition, you can safeguard your family with parental control features such as Internet access restrictions and keyword blocking. These security features, as well as the Gateway's other settings, are accessed through the easy-to-use, browser-based utility.

But what does all of this mean?

Networks are useful tools for sharing Internet access and computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks not only are useful in homes and offices, but also can be fun.

PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired". PCs equipped with wireless cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wireless Local Area Network. Since the Gateway has wireless capabilities, it can bridge your wired and wireless networks, letting them communicate with each other.

***802.11b**: an IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.*

***802.11g**: an IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.*

***wpa** (wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.*

***spi** (stateful packet inspection) **firewall**: a technology that inspects incoming packets of information before allowing them to enter the network.*

***firewall**: Security measures that protect the resources of a local network from intruders.*

***nat** (network address translation): NAT technology translates IP addresses of a local area network to a different IP address for the Internet.*

***network**: a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users*

***lan** (local area network): The computers and networking products that make up the network in your home or office.*

With your networks all connected, wired, wireless, and the Internet, you can now share files and Internet access—and even play games. All the while, the Wireless-G ADSL Gateway with SRX200 protects your networks from unauthorized and unwelcome users.

Linksys recommends using the Setup CD-ROM for first-time installation of the Gateway. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then use the instructions in this Guide to help you connect the Gateway, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Wireless-G ADSL Gateway with SRX200.

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G ADSL Gateway with SRX200.

- Chapter 1: Introduction
  This chapter describes applications of the Wireless-G ADSL Gateway with SRX200 and this User Guide.
- Chapter 2: Planning Your Network
  This chapter describes the basics of networking.
- Chapter 3: Getting to Know the Wireless-G ADSL Gateway with SRX200
  This chapter describes the physical features of the Gateway.
- Chapter 4: Connecting the Wireless-G ADSL Gateway with SRX200
  This chapter instructs you on how to connect the Gateway to your network.
- Chapter 5: Setting up the Wireless-G ADSL Gateway with SRX200
  This chapter explains how to set up the Gateway using its Setup Wizard.
- Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200
  This chapter explains how to configure the Gateway's settings using its Web-based Utility.
- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G ADSL Gateway with SRX200.
- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- Appendix C: 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 D: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on the Gateway if you should need to do so.

- 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.

- 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 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.

Figure 2-1: Network

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.

ip *(internet protocol): a protocol used to send data over a 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 Security - Firewall tab in "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200."

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 your network, you must disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Gateway, see the DHCP section in "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200."

Chapter 3: Getting to Know the Wireless-G ADSL Gateway with SRX200

Ports and Reset Button on Side Panel

The Gateway's ports and Reset button are located on a side panel.

Figure 3-1: Ports and Reset Button on Side Panel

Line The **Line** port connects to the ADSL line.

Ethernet (1-4) The **Ethernet** ports connect to your computers and other network devices.

Reset Button There are two ways to reset the Gateway's factory defaults. Either press the **Reset Button**, for approximately five seconds, or restore the defaults from the *Factory Defaults* screen of the Administration tab in the Gateway's Web-based Utility.

Power The **Power** port is where you will connect the power adapter.

IMPORTANT: Resetting the Gateway to factory defaults will erase all of your settings (including Internet connection, wireless, and other settings) and replace them with the factory defaults. Do not reset the Gateway if you want to retain these settings.

LEDs on Side Panel

The Gateway's LEDs, which indicate network activity, are located on the other side panel.

Figure 3-2: LEDs on Side Panel

(POWER) button When you want to power the Gateway on or off, push this button.

POWER Green. The **POWER** LED lights up when the Gateway is powered on.

WIRELESS Green. The **WIRELESS** LED lights up whenever there is a successful wireless connection. If the LED is flashing, the Gateway is actively sending or receiving data to or from one of the devices on the network.

ETHERNET (1-4) Green. The **ETHERNET** LED serves two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through the Ethernet port. If the LED is flashing, it is an indication of any network activity.

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.

INTERNET Green. The **INTERNET** LED lights up green when an Internet connection to the Internet Service Provider (ISP) is established. The INTERNET LED lights up red when the connection to the ISP fails.

Chapter 4: Connecting the Wireless-G ADSL Gateway with SRX200

Overview

The installation technician from your ISP should have left the setup information for the 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.

If you want to use a computer with an Ethernet adapter to configure the Gateway, continue to "Wired Connection to a Computer." If you want to use a computer with a wireless adapter to configure the Gateway, continue to "Wireless Connection to a Computer."

Wired Connection to a Computer

1. Make sure that all of your network's hardware is powered off, including the Gateway and all computers.

2. Connect a phone cable from the Line port on the Gateway's side panel to the wall jack of the ADSL line. 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.

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.

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 Gateway 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 Gateway 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 network cable to connect the Gateway to the wall jack or NTBA device. If you require splitters or special jacks, please contact your service provider.

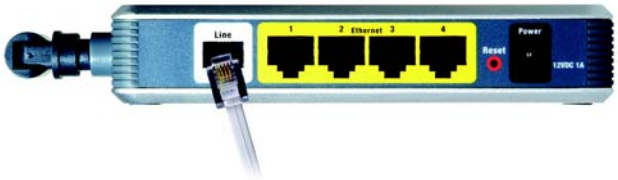


Figure 4-1: Connect the ADSL Line

3. Connect one end of an Ethernet network cable to one of the Ethernet ports (labeled 1-4) on the back of the Gateway, and the other end to an Ethernet port on a computer.

   Repeat this step to connect more computers, a switch, or other network devices to the Gateway.

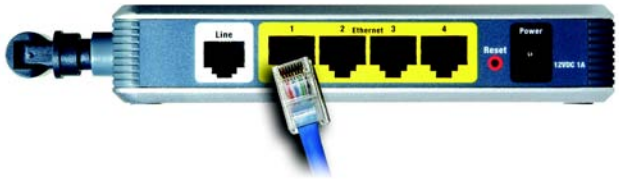


Figure 4-2: Connect a PC

4. Connect the power adapter to the Gateway's Power port, and then plug the power adapter into a power outlet.

NOTE: You should always plug the Gateway's power adapter into a power strip with surge protection.

   The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."

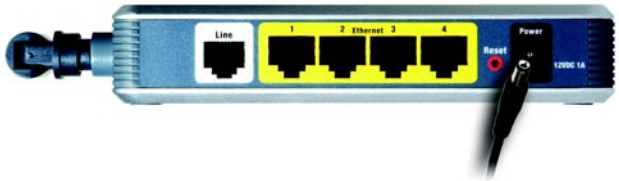


Figure 4-3: Connect the Power

5. Power on one of your computers that is connected to the Gateway.

Go to "Chapter 5: Setting up the Wireless-G ADSL Gateway with SRX200."

Wireless Connection to a Computer

If you want to use a wireless connection to access the Gateway, follow these instructions:

1. Make sure that all of your network's hardware is powered off, including the Gateway and all computers.

2. Connect a phone cable from the Line port on the Gateway's back panel to the wall jack of the ADSL line. 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.

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.

IMPORTANT: For countries that have phone jacks with RJ-11 connectors, make sure you only place the microfilters between the phone and the wall jack and **not** between the Gateway and the wall jack or your ADSL will not connect.

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 Gateway 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 network cable to connect the Gateway to the wall jack or NTBA device. If you require splitters or special jacks, please contact your service provider.

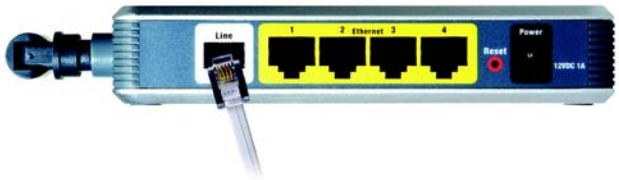


Figure 4-4: Connect the ADSL Line

3. Connect the power adapter to the Power port, and then plug the power adapter into a power outlet.

NOTE: You should always plug the Gateway's power adapter into a power strip with surge protection.

The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."

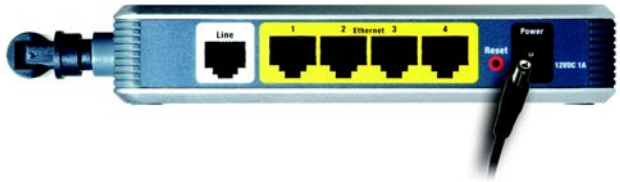


Figure 4-5: Connect the Power

4. Power on one of the computers on your wireless network(s).

5. For initial access to the Gateway through a wireless connection, make sure the computer's wireless adapter has its SSID set to **linksys** (the Gateway's default setting), and its wireless security is disabled. After you have accessed the Gateway, you can change the Gateway and this computer's adapter settings to match your usual network settings.

NOTE: You should always change the SSID from its default, **linksys**, and enable wireless security.

Go to "Chapter 5: Setting up the Wireless-G ADSL Gateway with SRX200."

Chapter 5: Setting up the Wireless-G ADSL Gateway with SRX200

Overview

The Wireless-G ADSL Gateway with SRX200 Setup Wizard will guide you through the installation procedure. It will go through the instructions for configuring the Gateway's network and wireless settings.

Using the Setup Wizard

1. Insert the **Setup Wizard CD-ROM** into your CD-ROM drive. The Setup Wizard should run automatically, and the *Welcome* screen should appear. If it does not, click the **Start** button and choose **Run**. In the field that appears, enter **D:\setup.exe** (if "D" is the letter of your CD-ROM drive).

2. The Setup Wizard will automatically detect the language setting of your PC; if it does not, select one of the available languages from the *Language* drop-down menu. On the initial *Welcome* screen, click the **Next** button if you want to proceed with the Setup Wizard using the current language. If you want to use a different language, select the appropriate language, and then click the **Next** button.

Figure 5-1: Setup Wizard's Welcome - Language Selection Screen

3. On the following *Welcome* screen, click the **Click Here to Start** button. These are your other choices:

   Norton Internet Security - Click the **Norton Internet Security** button to install the Norton Internet Security software program.

   User Guide - Click the **User Guide** button to open the PDF file of this User Guide.

   Exit - Click the **Exit** button to exit the Setup Wizard.

Figure 5-2: Setup Wizard's Welcome - Start Wizard Screen

4. After reading the License Agreement, click the **Next** button if you accept, or click the **Exit** button to end the installation. Click the **Back** button go back to the previous screen.

Figure 5-3: Setup Wizard's License Agreement Screen

5. The Setup Wizard will ask you to disconnect your broadband modem from your PC and the ADSL wall jack. After you have done so, click the **Next** button.

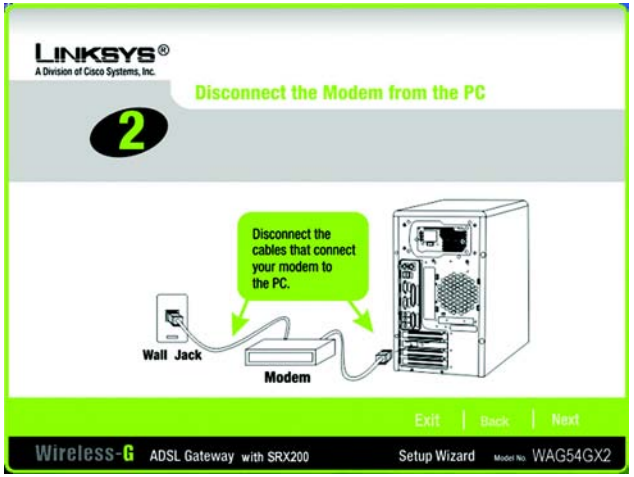


Figure 5-4: Setup Wizard's Disconnect the Modem from the PC and ADSL Wall Jack Screen

6. The Setup Wizard will ask you to connect the Gateway to the ADSL wall jack. After you have done so, click the **Next** button.

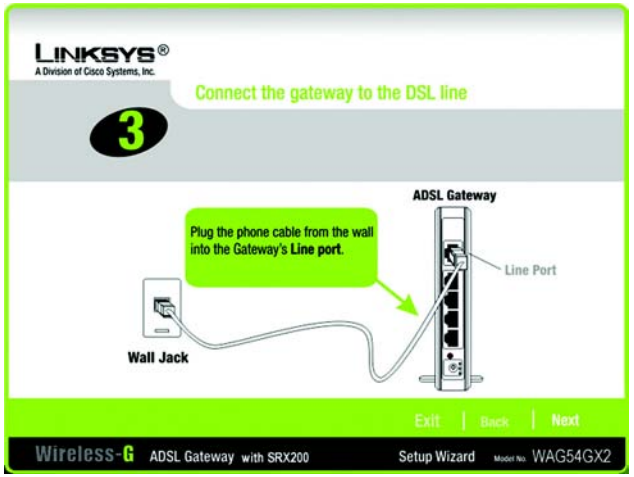


Figure 5-5: Setup Wizard's Connect the Gateway to the ADSL Wall Jack Screen

7. The Setup Wizard will ask you to connect a network cable to your PC. After you have done so, click the **Next** button.

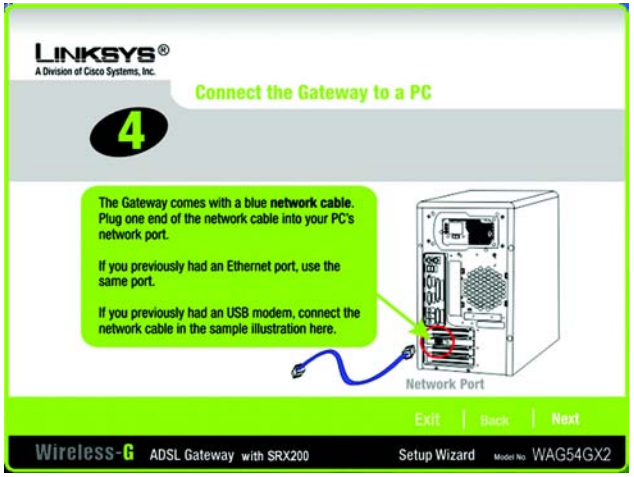


Figure 5-6: Setup Wizard's Connect a Network Cable to a PC Screen

8. The Setup Wizard will ask you to connect the other end of the network cable to the Gateway.

   Then you can also connect additional PCs to the Gateway.

   After you have done so, click the **Next** button.

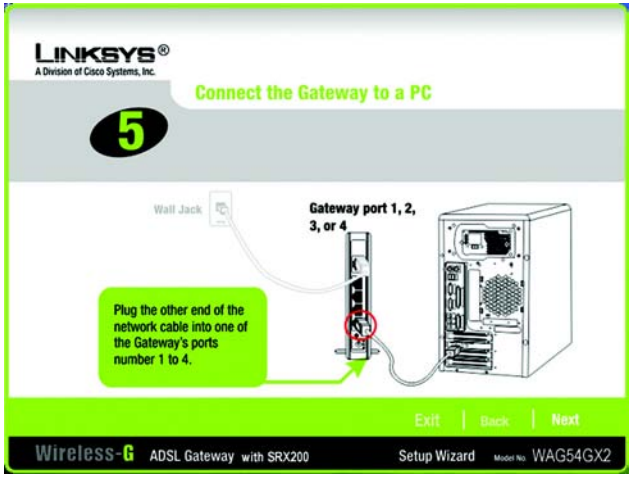


Figure 5-7: Setup Wizard's Connect the Network Cable to the Gateway Screen

9. The Setup Wizard will ask you to power on the Gateway. After you have done so, click the **Next** button.

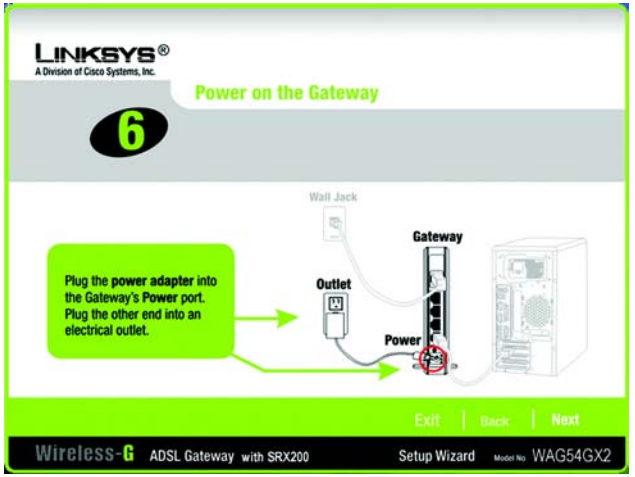


Figure 5-8: Setup Wizard's Power on the Gateway Screen

10. Make sure the Gateway's Power, DSL, and numbered LEDs (depending on the number of PCs connected) are lit on its front panel. After you have done so, click the **Next** button.

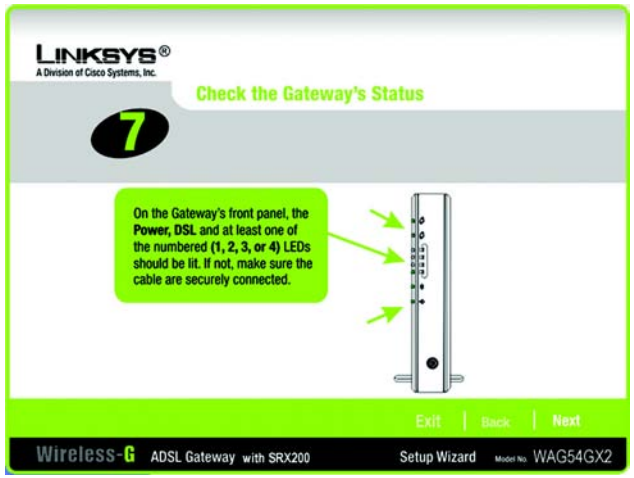


Figure 5-9: Setup Wizard's Check the Gateway's Status Screen

11. You will be asked where you reside. Select the appropriate country from the drop-down menu. Then click the **Next** button.

NOTE: If your country is not listed, then use the Gateway's Web-based Utility to configure your settings. Refer to "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200" for instructions.

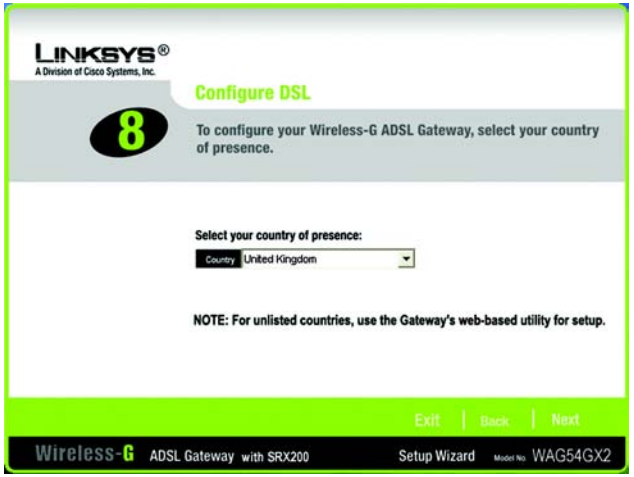


Figure 5-10: Setup Wizard's Select Your Country Screen

12. The Internet Service Providers (ISPs) for your country will be listed. (The on-screen options will vary depending on which country you selected on the previous screen.) Click the button for your ISP.

    If your ISP is not listed, click the **Next** button to manually enter your settings.

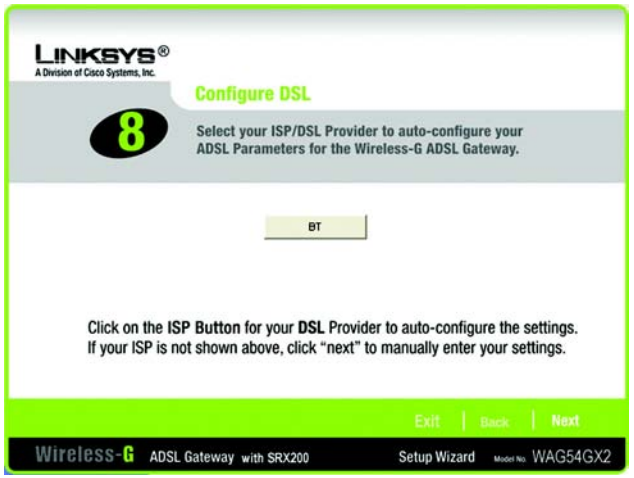


Figure 5-11: Setup Wizard's Select Your Internet Service Provider Screen (UK)

13. If applicable, the Setup Wizard will automatically detect the Encapsulation type you use: 1483 Bridged, 1483 Routed, PPPoA, or PPPoE. To manually enter your settings, select your Encapsulation type: **1483 Bridged**, **1483 Routed**, **PPPoA**, or **PPPoE**.

    NOTE: If your Encapsulation type is IPoA or Bridged Mode Only, you will have to use the Gateway's Web-based Utility to configure it. Refer to "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200" for instructions.

    Proceed to the appropriate section for your Encapsulation type.

1483 Bridged

If you selected your ISP, then the Setup Wizard will automatically select the Encapsulation, VPI, VCI, and Multiplexing settings. Then select the appropriate IP setting for your DSL connection.

If you need to manually enter your settings, use this screen.

VPI/VCI - If you need to manually enter your settings, enter the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) settings provided by your ISP.

Multiplexing - If you need to manually enter your settings, select **LLC** or **VC**, depending on your ISP.

Auto IP - If you are using a dynamic IP address, then click the **Auto IP** radio button.

Static IP - If you are using a static IP address, then click the **Static IP** radio button. Complete the *IP Address*, *Subnet Mask*, *Default Gateway*, *Primary DNS* (Domain Name System), and *Secondary DNS* fields. (You need to enter at least one DNS server IP address.)

Click the **Next** button to continue or the **Back** button to return to the previous screen.

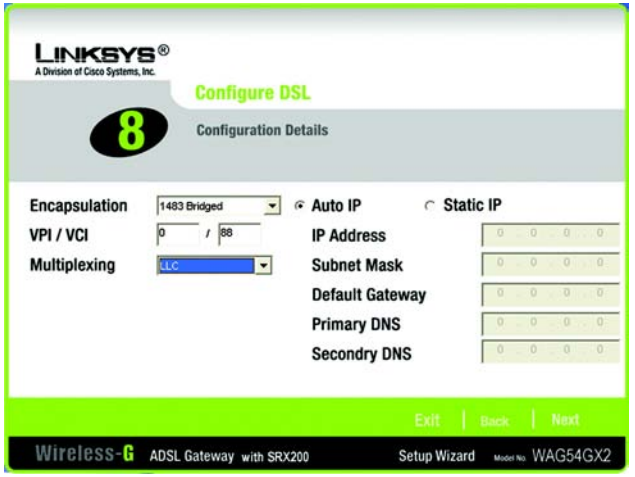


Figure 5-12: Setup Wizard's Configure DSL - 1483 Bridged Screen

1483 Routed

If you selected your ISP, then the Setup Wizard will automatically select the Encapsulation, VPI, VCI, and Multiplexing settings. Then enter the appropriate IP settings for your DSL connection.

If you need to manually enter your settings, use this screen.

VPI/VCI - If you need to manually enter your settings, enter the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) settings provided by your ISP.

Multiplexing - If you need to manually enter your settings, select **LLC** or **VC**, depending on your ISP.

Static IP - Complete the *IP Address*, *Subnet Mask*, *Default Gateway*, *Primary DNS* (Domain Name System), and *Secondary DNS* fields. (You need to enter at least one DNS server IP address.)

Click the **Next** button to continue or the **Back** button to return to the previous screen.

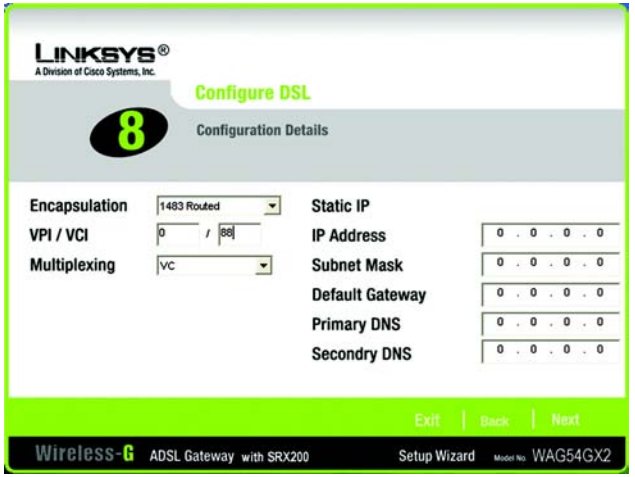


Figure 5-13: Setup Wizard's Configure DSL - 1483 Routed Screen

PPPoA

If you selected your ISP, then the Setup Wizard will automatically select the Encapsulation, VPI, VCI, and Multiplexing settings. Then enter the User ID and Password for your DSL connection.

If you need to manually enter your settings, use this screen.

VPI/VCI - If you need to manually enter your settings, enter the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) settings provided by your ISP.

Multiplexing - If you need to manually enter your settings, select **LLC** or **VC**, depending on your ISP.

User ID and **Password** - Enter the User ID and Password provided by your ISP.

Connection - Select **Keep Alive** if you always want to be connected to your ISP, or select **Connect on Demand** if you are charged for the time that you are connected to your ISP.

Keep Alive - For this option, the Gateway will keep the Internet connection active. In the *Redial Period* field, specify how often you want the Gateway to check the Internet connection (the default is **5** minutes).

Connect on Demand - If you select this option, the Gateway will terminate your Internet access after all online applications have been closed for a specified period of time, which you can specify in the *Max Idle Time* field (the default is **30** seconds).

Click the **Next** button to continue or the **Back** button to return to the previous screen.

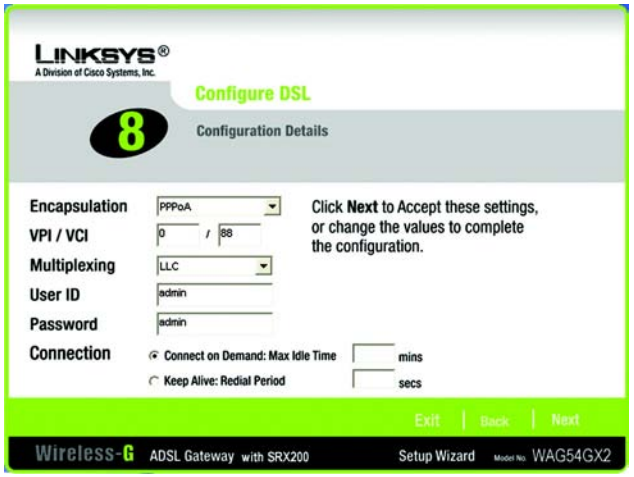


Figure 5-14: Setup Wizard's Configure DSL - PPPoA Screen

PPPoE

If you selected your ISP, then the Setup Wizard will automatically select the Encapsulation, VPI, VCI, and Multiplexing settings. Then enter the User ID and Password for your DSL connection.

If you need to manually enter your settings, use this screen.

VPI/VCI - If you need to manually enter your settings, enter the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) settings provided by your ISP.

Multiplexing - If you need to manually enter your settings, select **LLC** or **VC**, depending on your ISP.

User ID and **Password** - Enter the User ID and Password provided by your ISP.

Connection - Select **Keep Alive** if you always want to be connected to your ISP, or select **Connect on Demand** if you are charged for the time that you are connected to your ISP.

Keep Alive - For this option, the Gateway will keep the Internet connection active. In the *Redial Period* field, specify how often you want the Gateway to check the Internet connection (the default is **5** minutes).

Connect on Demand - If you select this option, the Gateway will terminate your Internet access after all online applications have been closed for a specified period of time, which you can specify in the *Max Idle Time* field (the default is **30** seconds).

Click the **Next** button to continue or the **Back** button to return to the previous screen.

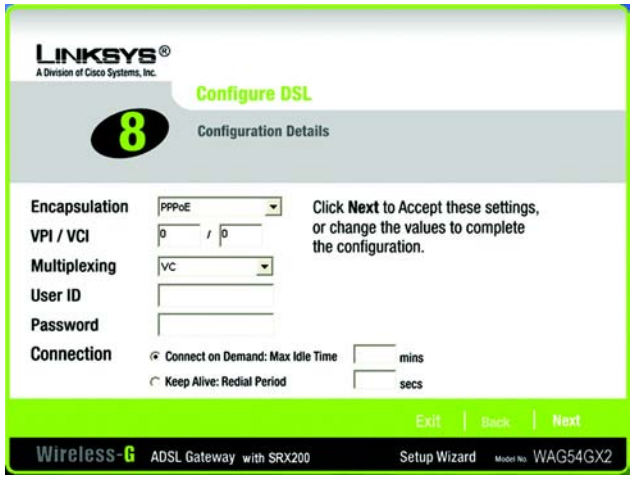


Figure 5-15: Setup Wizard's Configure DSL - PPPoE Screen

14. The Gateway provides a Web-based Utility you can use for configuring the Gateway from any networked PC. Access to the Utility is protected by a password.

Password - The default password is **admin**. Change it to a password of your choice.

Confirm - Enter the password again in the *Confirm* field.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

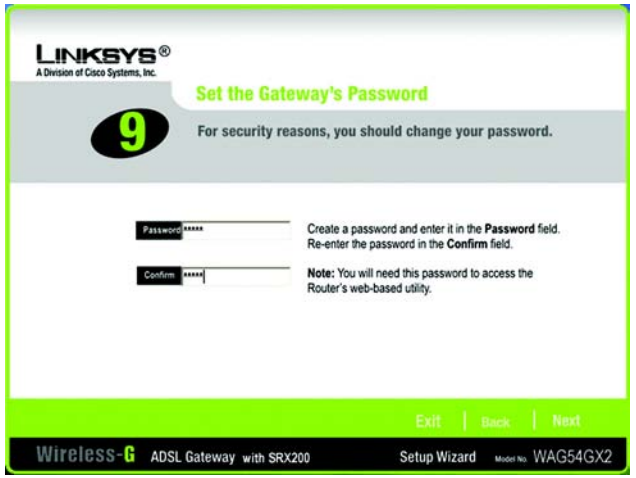


Figure 5-16: Setup Wizard's Set the Gateway's Password Screen

15. The Setup Wizard will ask you to enter the settings for your wireless network.

SSID - In the *SSID* field, enter the name of your wireless network. The SSID must be identical for all devices in the network. The default setting is **linksys** (all lowercase).

NOTE: An SSID is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network.

Channel - Select the operating channel for your wireless network. All of your wireless devices will use this channel to communicate.

Network Mode - From the *Network Mode* drop-down menu, select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed**. If you have only 802.11g devices, select **G-Only**. If you have only 802.11b devices, select **B-Only**. If you want to disable your wireless network, select **Disable**.

Device Name - Enter a name for the Gateway in the *Device Name* field.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

16. Select the method of security you want to use: **WPA Personal**, **WPA2 Personal**, **WPA2 Mixed Mode**, **WEP (64-Bit)**, or **WEP (128-Bit)**. WPA stands for Wi-Fi Protected Access, and WEP stands for Wired Equivalent Privacy. WPA is a stronger security method than WEP, and WPA2 is a stronger version of WPA. Proceed to the appropriate section for your security method.

If you do not want to use any wireless security method, select **Disabled** and then click the **Next** button. Proceed to step 17.

NOTE: If you want to use WPA Enterprise or WPA2 Enterprise security, select **Disabled** and then click the **Next** button. After you have finished the Setup Wizard, use the Gateway's Web-based Utility to configure your wireless security settings. Refer to "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200" for instructions.

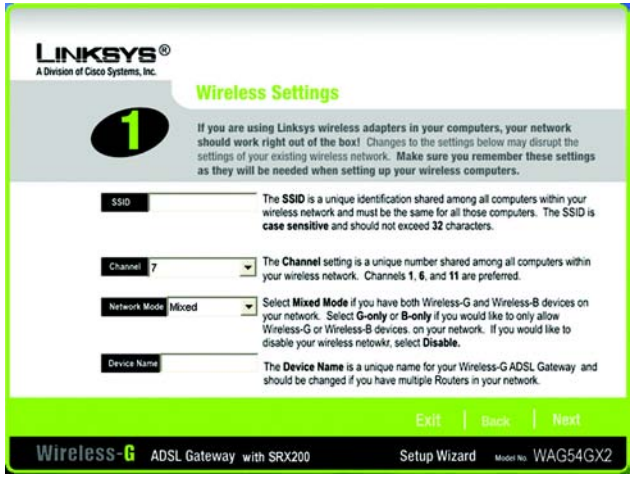


Figure 5-17: Setup Wizard's Wireless Settings Screen

wpa *(wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.*

wep *(wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.*

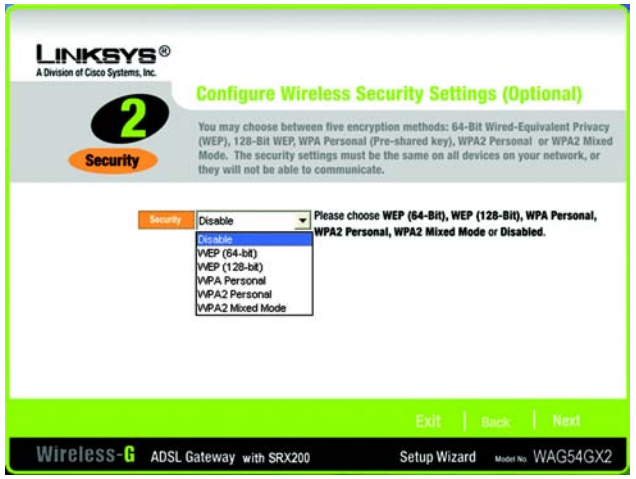


Figure 5-18: Setup Wizard's Configure Wireless Security Settings Screen

WPA Personal

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8 to 63 characters. The longer and more complex your Passphrase is, the more secure your network will be.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

encryption: *encoding data transmitted in a network.*

Figure 5-19: Setup Wizard's Wireless Security - WPA Personal Screen

WPA2 Personal

Encryption - AES is automatically selected for WPA2 Personal mode.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8 to 63 characters. The longer and more complex your Passphrase is, the more secure your network will be.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

Figure 5-20: Setup Wizard's Wireless Security - WPA2 Personal Screen

WPA2 Mixed Mode

Encryption - TKIP + AES is automatically selected so both methods can be used.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8 to 63 characters. The longer and more complex your Passphrase is, the more secure your network will be.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

Figure 5-21: Setup Wizard's Wireless Security - WPA2 Mixed Mode Screen

WEP (64-Bit)

Enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. The passphrase is case-sensitive and should not be longer than 16 alphanumeric characters. It must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

Key 1 - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Click the **Next** button to continue or the **Back** button to return to the previous screen.

Figure 5-22: Setup Wizard's Wireless Security - WEP (64-Bit) Screen

WEP (128-Bit)

Enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. The passphrase is case-sensitive and should not be longer than 16 alphanumeric characters. It must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

Key 1 - The WEP key you enter must match the WEP key of your wireless network. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Click the Next button to continue or the Back button to return to the previous screen.

Figure 5-23: Setup Wizard's Wireless Security - WEP (128-Bit) Screen

17. The Setup Wizard will ask you to review your settings before it saves them. Click the **Yes** button if you are satisfied with your settings, or click the **No** button if you do not want to save your new settings.

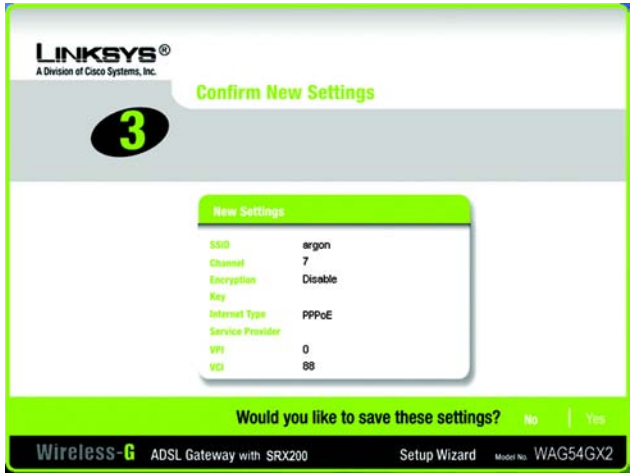


Figure 5-24: Setup Wizard's Confirm New Settings Screen

18. After the settings have been saved, the *Safe Surfing* screen will appear. Click the **Norton Internet Security Suite** button to install the special edition of Norton Internet Security on your computer, or click the **Finish** button to complete the Setup Wizard.

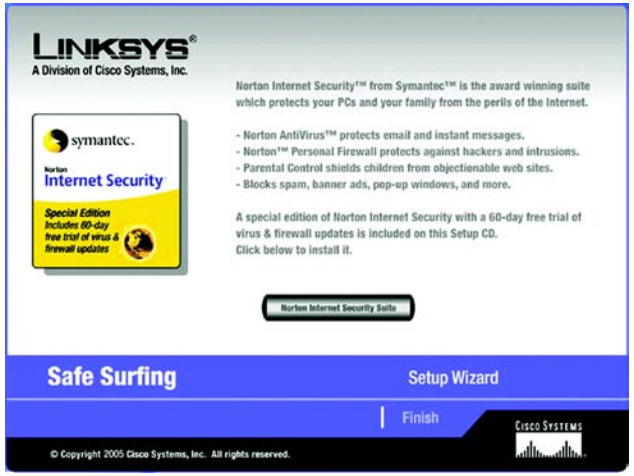


Figure 5-25: Setup Wizard's Safe Surfing Screen

19. The *Congratulations* screen will appear. Click the **Online Registration** button to register the Gateway, or click the **Exit** button to exit the Setup Wizard.

Congratulations! The installation of the Wireless-G ADSL Gateway with SRX200 is complete.

If you want to make advanced configuration changes, proceed to "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200."

Figure 5-26: Setup Wizard's Congratulations Screen

Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200

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 default username and password.

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs. Click **Help** for more information.

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 NAT and routing configurations.

Wireless

- Basic Wireless Settings. You can choose your wireless network settings on this screen.
- Wireless Security. Configure your wireless security settings on this screen.
- Wireless Access. This screen lets you control access to your wireless network.
- Advanced Wireless Settings. On this screen you can access the advanced wireless network settings.

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.

NOTE: For added security, you should change the username and password through the Administration tab.

Security

- Firewall. Use this screen to enable/disable the firewall, set up filters, and block anonymous Internet requests.
- VPN Passthrough. You can enable or disable Virtual Private Network (VPN) Passthrough on this screen.
- VPN. Use this screen to configure up to five VPN tunnels.

vpn *(virtual private network): a security measure to protect data as it leaves one network and goes to another over the Internet.*

Access Restrictions

- Internet Access Policy. This screen allows you to control the Internet usage and traffic on your local network.

Applications & Gaming

- Single Port Range Forwarding. Use this screen to set up common services or applications that require forwarding on a single port.
- Port Range Forwarding. To set up public services or other specialized Internet applications that require forwarding on a range of ports, use this screen.
- Port Triggering. To set up triggered ranges and forwarded ranges for Internet applications, click this tab.
- DMZ. To allow one local computer to be exposed to the Internet for use of special-purpose services, use this screen.
- QoS. Use Quality of Service (QoS) to assign different priority levels to different types of data transmissions.

Administration

- Management. On this screen, alter Gateway access, Simple Network Management Protocol (SNMP), Universal Plug and Play (UPnP), wireless management, and IGMP proxy settings.
- Reporting. If you want to view or save activity logs, click this tab.
- Diagnostics. Use this screen to run a Ping test.
- Backup&Restore. On this screen, you can back up or restore the Gateway's configuration.
- Factory Defaults. If you want to restore the Gateway's factory default settings, use this screen.
- Firmware Upgrade. Click this tab if you want to upgrade the Gateway's firmware.

Status

- Gateway. This screen provides status information about the Gateway.
- Local Network. This provides status information about the local network.
- Wireless. This screen provides status information about the wireless network.
- DSL Connection. This screen provides status information about the DSL connection.

Figure 6-1: Login Screen

How to Access the Web-based Utility

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Gateway's default IP address, **192.168.1.1**, in the *Address* field. Then press **Enter**.

A login screen will appear (Windows XP users will see a similar screen). Enter **admin** (the default user name) in the *User Name* field, and enter **admin** (the default password) in the *Password* field. Then click the **OK** 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 click the **Cancel Changes** button to cancel your changes. Click **Help** for more information.

Internet Setup

- Internet Connection Type. The Gateway supports six Encapsulation methods: RFC 1483 Bridged, RFC 1483 Routed, IPoA, RFC 2516 PPPoE, RFC 2364 PPPoA, and Bridged Mode Only. Select the appropriate type of encapsulation from the drop-down menu. Each *Basic Setup* screen and available features will differ depending on what type of encapsulation you select.
- VC Settings. You will configure your Virtual Circuit (VC) settings in this section.
  - 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 e-mail; or **VBR** (Variable Bite Rate) for bursty traffic and bandwidth-sharing with other applications.

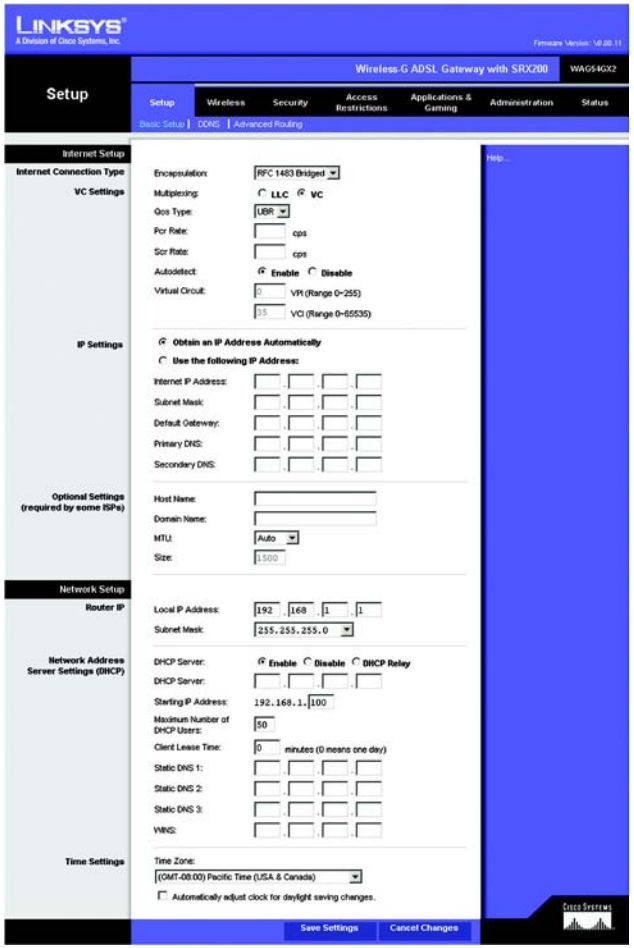


Figure 6-2: Basic Setup

- Pcr Rate: For the Peak Cell Rate, divide the DSL line rate by 424 to get the maximum rate the sender can send cells. Enter the rate in the field (if required by your service provider).
- Scr Rate: The Sustain Cell Rate sets the average cell rate that can be transmitted. The SCR value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
- Autodetect: Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
- Virtual Circuit: 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.

- IP Settings. Follow the instructions in the section for your type of encapsulation.

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.
- 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.

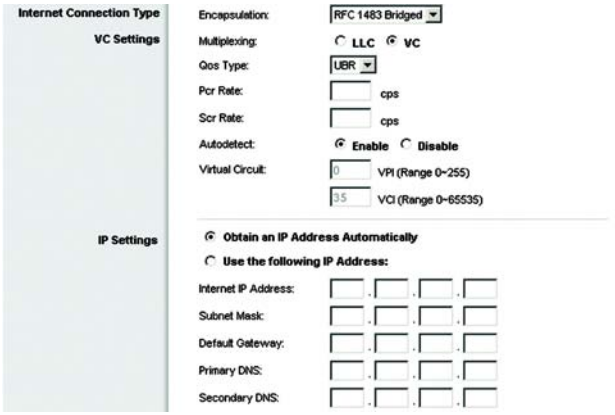


Figure 6-3: RFC 1483 Bridged

RFC 1483 Routed

If you are required to use RFC 1483 Routed, then select **RFC 1483 Routed**.

- 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.
- 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.

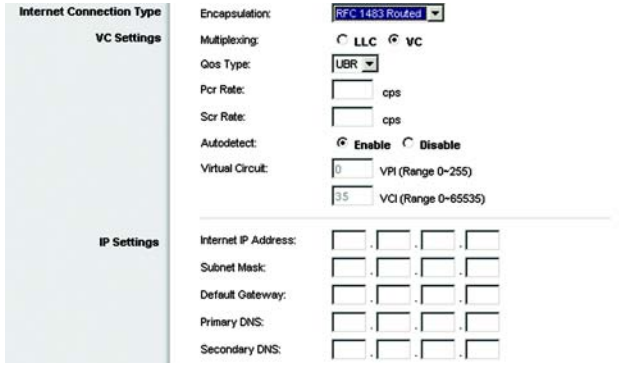


Figure 6-4: RFC 1483 Routed

IPoA

If you are required to use IPoA (IP over ATM), then select **IPoA**.

- 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.
- 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.

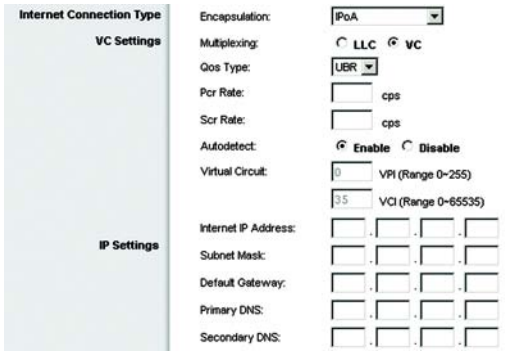


Figure 6-5: IPoA

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.

- 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. To use this option, click the **Connect on Demand** 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 **Keep Alive** radio button. In the *Redial Period* field, specify how often you want the Gateway to check the Internet connection. The default Redial Period is **30** seconds.

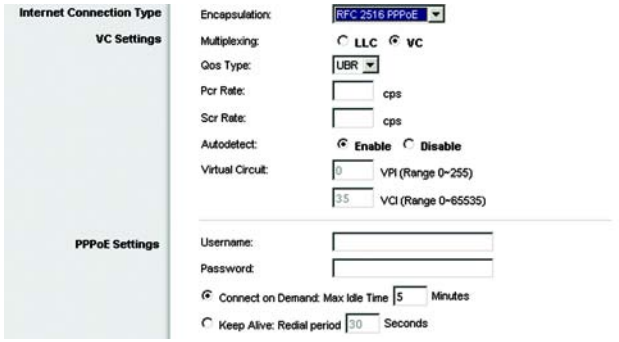


Figure 6-6: RFC 2516 PPPoE

IMPORTANT: For Connect on Demand to work correctly, close all Internet applications or the Gateway may not drop the connection depending on how often the application tries to get on the Internet (e.g., chat programs).

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 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. To use this option, click the **Connect on Demand** 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 **Keep Alive** radio button. In the *Redial Period* field, specify how often you want the Gateway to check the Internet connection. The default Redial Period is **30** seconds.

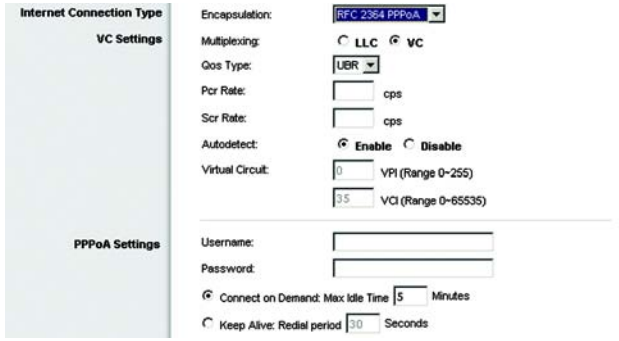


Figure 6-7: RFC 2364 PPPoA

Bridge Mode Only

If you are using your Gateway as a bridge, which makes the Gateway act like a stand-alone modem, select **Bridge Mode Only**. All NAT and routing settings are disabled in this mode.

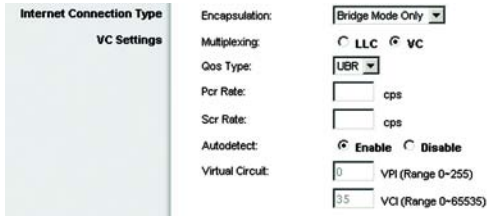


Figure 6-8: Bridged Mode Only

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, you can leave these fields blank.
- MTU and Size. 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). Configure the Gateway's Dynamic Host Configuration Protocol (DHCP) settings in this section.
  - 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, it is highly recommended that you leave the Gateway enabled as a DHCP server. You can also use the Gateway in DHCP Relay mode. (This setting is not available for all Encapsulation types.)
  - DHCP Server. If you enable the DHCP Relay mode for the *DHCP Server* setting, enter the IP address for the DHCP relay server in the fields provided. (This setting is not available for all Encapsulation types.)
  - 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.

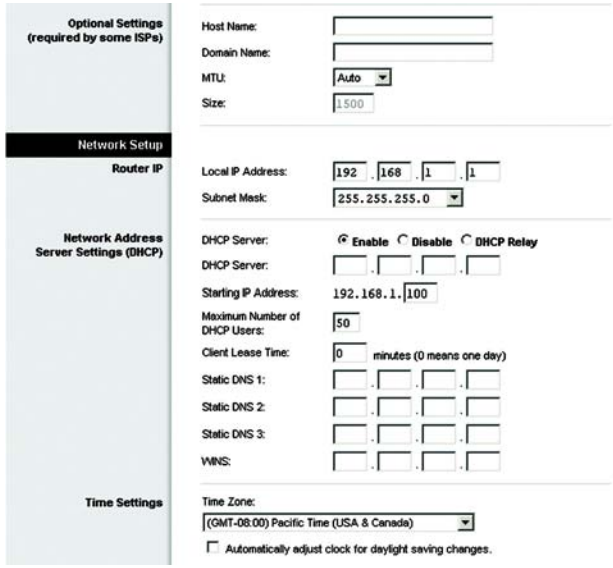


Figure 6-9: Optional Settings

- Client Lease Time. The Client Lease Time is the amount of time a computer will be allowed connection to the Gateway with its current dynamic IP address. Enter the amount of time, in minutes, that the computer 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 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.
- Time Setting. Select the appropriate time zone for the Gateway's location. If desired, check the **Automatically adjust clock for daylight saving changes** checkbox.

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. Click **Help** for more information.

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 or TZO.com.

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.com, then select **TZO.com** from the drop-down menu. 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.
- Status. The status of the DDNS service connection is displayed here.
- Connect. Click the **Connect** button to start the DDNS service connection.

TZO.com

- E-mail Address, Password, and Domain Name. Enter the E-mail Address, Password, and Domain Name of the account you set up with TZO.
- Status. The status of the DDNS service connection is displayed here.
- Connect. Click the **Connect** button to start the DDNS service connection.

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. Click **Help** for more information.

Figure 6-10: DDNS - DynDNS.org

Figure 6-11: DDNS - TZO.com

The Advanced Routing Tab

The *Advanced Routing* screen allows you to configure the NAT, dynamic routing, and static routing settings.

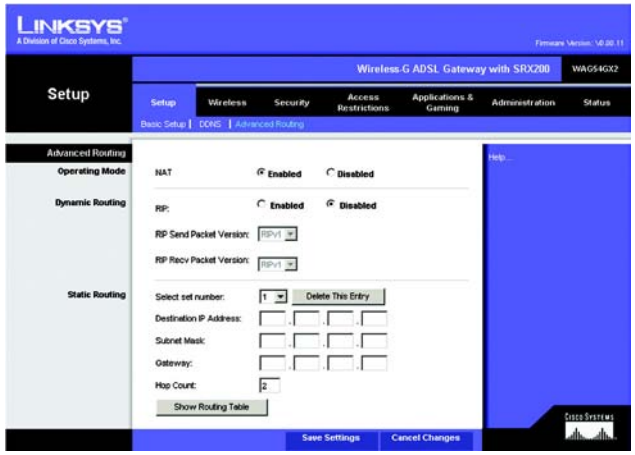


Figure 6-12: Advanced Routing

Advanced Routing

- Operating Mode. In this section, you will configure the Gateway's general routing settings.
  - NAT. 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. Using RIP, the Gateway 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.
  - RIP. If you have multiple routers, you may want to use the Routing Information Protocol (RIP) so the routers can exchange routing information with each other. To use RIP, select the **Enabled** radio button. Otherwise, keep the default, **Disabled**.
  - RIP Send Packet Version. Select the protocol version you want, **RIPv1** or **RIPv2**.
  - RIP Recv Packet Version. Select the protocol version you want, **RIPv1** or **RIPv2**.
- 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, then select the entry and 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.
  - Subnet Mask. Enter the Subnet Mask (also known as the Network Mask), which determines which portion of an IP address is the network portion, and which portion is the host portion.

- Gateway. Enter 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 provided.

- Show Routing Table. Click the **Show Routing Table** button to open a screen displaying how data is routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click the **Refresh** button to update the information. Click the **Close** button to 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. Click **Help** for more information.

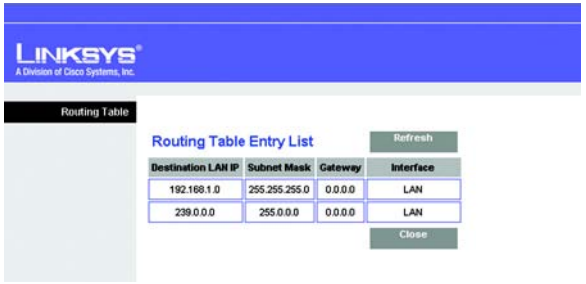


Figure 6-13: Routing Table

The Wireless Tab

The Basic Wireless Settings Tab

This screen allows you to choose your wireless network mode and wireless security.

Wireless Network

- Wireless Network Mode. If you have 802.11g and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only 802.11g devices, select **G-Only**. If you have only 802.11b devices, select **B-Only**. If you want to disable wireless networking, select **Disabled**.
- Wireless Network Name (SSID). Enter the name for your wireless network into the field. The SSID is the network name shared among all devices in a wireless network. It must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Linksys recommends that you change the default SSID (linksys) to a unique name of your choice.
- Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly. Wireless computers or clients will automatically detect the wireless channel of the Gateway.
- Wireless SSID Broadcast. When wireless computers or clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Gateway. To broadcast the Gateway's SSID, keep the default setting, **Enable**. If you do not want to broadcast the Gateway's SSID, then select **Disable**.

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. Click **Help** for more information.

Figure 6-14: Basic Wireless Settings

The Wireless Security Tab

The Wireless Security settings configure the security of your wireless network. There are six wireless security options supported by the Gateway: WPA-Personal, WPA2-Personal, WPA2-Mixed, WPA Enterprise, WPA2 Enterprise, and WEP. WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP (Wired Equivalent Privacy) encryption. WPA2 is a more advanced, more secure version of WPA. WPA Enterprise and WPA2 Enterprise use a RADIUS (Remote Authentication Dial-In User Service) server for authentication. These are briefly discussed here. For detailed instructions on configuring wireless security for the Gateway, turn to "Appendix B: Wireless Security."

If you want to disable wireless security, select **Disable** from the drop-down menu for Security Mode.

- Security Mode. Select the mode you want your network to use, **WPA-Personal**, **WPA2-Personal**, **WPA2-Mixed**, **WPA Enterprise**, **WPA2 Enterprise**, or **WEP**. If you have devices using WPA-Personal and WPA2-Personal, select **WPA2-Mixed**.

WPA-Personal

- Encryption. Select the method you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)
- Passphrase. Enter the key shared by the Gateway and your other network devices. It must have 8 to 63 characters.
- Key Renewal. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

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. Click **Help** for more information.

WPA2-Personal

- Encryption. AES is automatically selected.
- Passphrase. Enter the key shared by the Gateway and your other network devices. It must have 8 to 63 characters.
- Key Renewal. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

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. Click **Help** for more information.

Figure 6-15: Wireless Security - WPA-Personal

IMPORTANT: If you are using wireless security, always remember that each device in your wireless network MUST use the same wireless security method and shared key, or else the network will not function correctly. If you have devices using WPA-Personal and WPA2-Personal, you should use WPA2-Mixed. You may mix between WPA and WPA2 Enterprise, but not between Personal and Enterprise, Personal and WEP, or Enterprise and WEP.

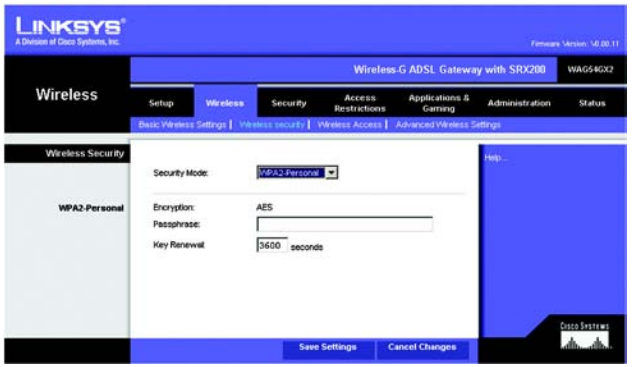


Figure 6-16: Wireless Security - WPA2-Personal

WPA2-Mixed

- Encryption. TKIP + AES is automatically selected so both methods are available.
- Passphrase. Enter the key shared by the Gateway and your other network devices. It must have 8 to 63 characters.
- Key Renewal. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

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. Click **Help** for more information.

Figure 6-17: Wireless Security - WPA2-Mixed

WPA Enterprise

WPA Enterprise features WPA used with a RADIUS server. (This method should only be used when the Gateway is connected to a RADIUS server.)

- RADIUS Server Address. 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 Gateway and its RADIUS server.
- Key Renewal Timeout. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

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. Click **Help** for more information.

Figure 6-18: Wireless Security - WPA Enterprise

WPA2 Enterprise

WPA2 Enterprise features WPA2 used with a RADIUS server. (This method should only be used when the Gateway is connected to a RADIUS server.)

- RADIUS Server Address. 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 Gateway and its RADIUS server.
- Key Renewal Timeout. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

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. Click **Help** for more information.

Figure 6-19: Wireless Security - WPA2 Enterprise

WEP

- Encryption. Select the appropriate level of encryption, **64-bit** or **128-bit**. 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.
- WEP Keys 1-4. 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 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.

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. Click **Help** for more information.

Figure 6-20: Wireless Security - WEP

The Wireless Access Tab

Wireless Network Access

Wireless Network Access. Select **Allow All** you want all computers to have access to the wireless network. To restrict access to the network, select **Restrict Access**, and then select **Prevent** to block access for the designated computers or **Permit only** to permit access for the designated computers. Click the **Update Filter List** button, and the *Mac Address Filter List* screen will appear.

Enter the MAC addresses of the computers you want to designate. To see a list of MAC addresses for wireless computers or clients, click the **Wireless Client MAC List** button.

The *Wireless Client List* screen will list MAC addresses for your wireless devices. Click the **Refresh** button to get the most up-to-date information. To add a specific computer to the Mac Address Filter List, click the **Enable MAC Filter** checkbox and then the **Update Filter List** button. Click the **Close** button to return to the *MAC Address Filter List* screen.

On the *MAC Address Filter List* screen, click the **Save Settings** button to save this list, or click the **Cancel Changes** button to remove your entries.

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. Click **Help** for more information.

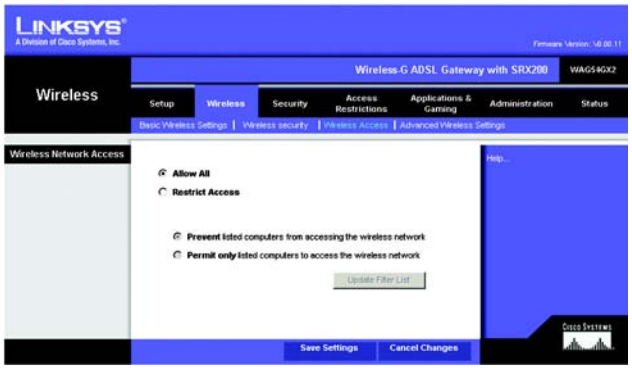


Figure 6-21: Wireless Access

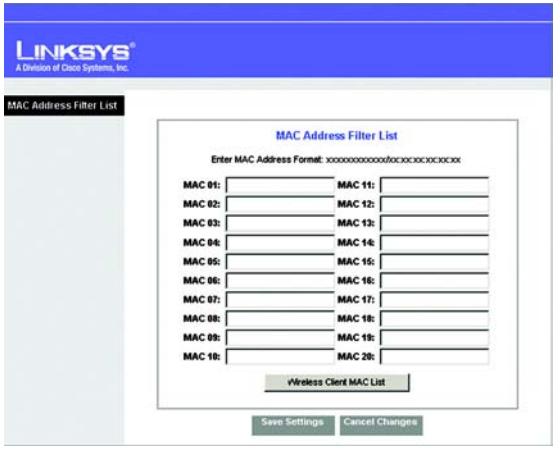


Figure 6-22: MAC Address Filter List

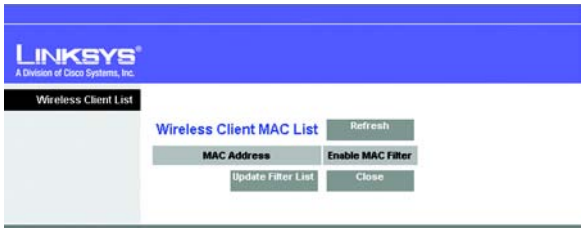


Figure 6-23: Wireless Client MAC List

The Advanced Wireless Settings Tab

You can access the advanced wireless features on this screen.

Advanced Wireless

Wireless-G Settings

This tab 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.

Figure 6-24: Advanced Wireless Settings

- Basic Rate Set. The Basic Rate Set is a series of rates at which the Gateway can transmit. (If you want to specify the Gateway's actual rate of data transmission, configure the Transmission Rate setting.) The Gateway will advertise its Basic Rate Set to the other wireless devices in your network, so they know which rates will be supported. The Gateway will also advertise that it will automatically select the best rate for transmission. In most cases, you should keep the default setting, **Default (1-2-5.5-11)**. Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Gateway can transmit at all wireless rates.

- Transmission 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 Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Gateway and a wireless client. The default is **Auto**.

- CTS Protection Mode. CTS (Clear-To-Send) Protection Mode should remain set to its default, **Auto**, so when your Wireless-G products are not able to transmit to the Gateway in an environment with heavy 802.11b traffic, the CTS Protection Mode will be used. This function boosts the Gateway's ability to catch all Wireless-G transmissions but will severely decrease performance.

- Beacon Interval. A beacon is a packet broadcast by the Gateway to synchronize the wireless network.Beacon Interval. The default value is **100**. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Gateway to synchronize the wireless network.

- 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 **1**.

- Fragmentation Threshold. This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation

Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

- RTS Threshold. If you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. This value should remain at its default setting of **2346**.

- Preamble Type. The preamble defines the length of the CRC block for communication between the Gateway and a roaming wireless client. (High network traffic areas should use the shorter preamble type.) Select the appropriate preamble type, **Long** (default) or **Short**.

- Network Density. This determines the Gateway's transmission and reception range. Select one of these settings, **Low** (greater range), **Medium** (mid-range), or **High** (lower range). The Low setting is recommended when you have few wireless networks in your area, while the High setting is recommended when you have a lot of wireless network traffic in your area. You can also use the Medium setting if you want a mid-range setting. The default setting is **Low**.

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. Click **Help** for more information.

The Security Tab

The Firewall Tab

You can enable or disable the firewall, select filters to block specific Internet data types, and block anonymous Internet requests. Use these features to enhance the security of your network.

Firewall

- SPI Firewall Protection. The Stateful Packet Inspection (SPI) firewall feature enhances the security of your network. To use this feature, click **Enable**. If you do not want to use the firewall, 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 the checkbox.
- 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 the checkbox.
- 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 the checkbox.
- 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 the checkbox.

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 de-select 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. Click **Help** for more information.

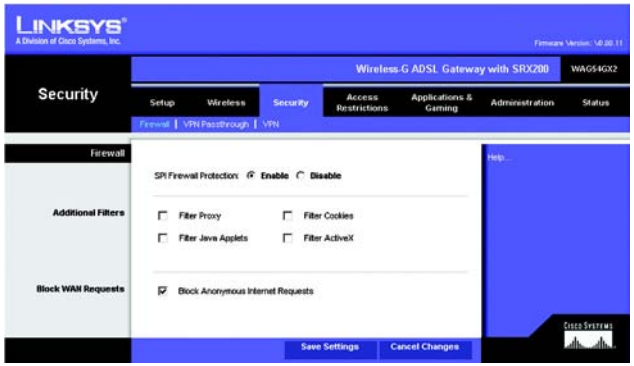


Figure 6-25: Firewall

The VPN Passthrough Tab

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. Configure these settings so the Gateway will permit VPN tunnels to pass through.

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.

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. Click **Help** for more information.

Figure 6-26: VPN Passthrough

The VPN Tab

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. Configure these settings so the Gateway will create VPN tunnels, up to a maximum of five.

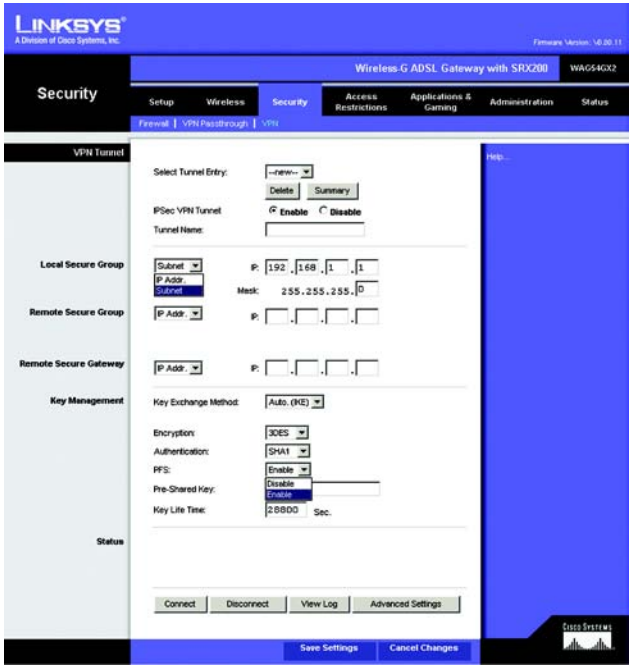


Figure 6-27: VPN

VPN Tunnel

- Select Tunnel Entry. To establish this tunnel, select **new**. To modify the settings for a tunnel, select the tunnel you wish to modify.
- Delete. To delete a tunnel, select it from the drop-down menu and click the **Delete** button.
- Summary. To see the settings for a tunnel, select it from the drop-down menu and click the **Summary** button.
- IPSec VPN Tunnel. Select **Enable** to activate the current VPN tunnel. Otherwise, select **Disable**.
- Tunnel Name. Once the tunnel is enabled, enter the name of the tunnel. Unique names allow you to identify multiple tunnels. The name you give on this end does not have to match the name used at the remote end of the tunnel.

Local Secure Group

The Local Secure Group is the computer(s) on your local network that can access the tunnel. From the drop-down menu, select **IP Addr.** or **Subnet**.

- IP Addr. Select **IP Addr.** if you want to designate a specific computer. Then enter the computer's IP address in the *IP* field.
- Subnet. Select **Subnet** if you want to include the entire network for the tunnel. Then enter the Gateway's IP address in the *IP* field and subnet mask in the *Mask* field.

Remote Secure Group

The Remote Secure Group is the computer(s) on the remote end of the tunnel; these are the computers that can access the tunnel. From the drop-down menu, select **IP Addr.**, **Subnet**, or **Any**.

- IP Addr. Select **IP Addr.** if you want to designate a specific computer. Then enter the computer's IP address in the *IP* field.
- Subnet. Select **Subnet** if you want to include the entire network for the tunnel. In the *IP* field, enter the IP address of the remote VPN device, such as a router, and enter its subnet mask in the *Mask* field.

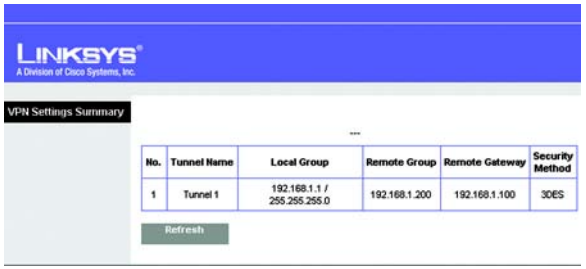


Figure 6-28: VPN Settings Summary

- Any. Select **Any** if you want the Gateway to accept requests from any IP address.

Remote Secure Gateway

The Remote Secure Gateway is the VPN device on the remote end of the VPN tunnel. The remote VPN device can be a VPN router, VPN server, or computer with VPN client software that supports IPSec. From the drop-down menu, select **IP Addr.** or **Any**.

- IP Addr. Select **IP Addr.** if you want to designate a static IP address. Then enter the VPN device's IP address in the *IP* field.

- Any. Select **Any** if you want the Gateway to accept requests from any IP address.

Key Management

- Key Exchange Method. Select **Auto (IKE)** or **Manual** for the Key Exchange Method. Both ends of a VPN tunnel must use the same mode of key management. The two methods are described below. After you have selected the method, the settings available on this screen may change, depending on the selection you have made.

  Auto (IKE)

  IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Pre-Shared Key to authenticate the remote IDE peer.

  - Encryption. When you select Auto (IKE), 3DES (168-bit) encryption is automatically selected. The same type of encryption must be used by the VPN device at the remote end of the tunnel.

  - Authentication. Select one of the two authentication methods available, **SHA1** or **MD5**. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.

  - PFS. PFS (Perfect Forward Secrecy) ensures that the initial key exchange and IKE proposals are secure. To use PFS, select **Enable**. Otherwise, select **Disable**.

  - Pre-Shared Key. 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, 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.

  - Key Life Time. 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 useful, or leave it blank for the key to last indefinitely.

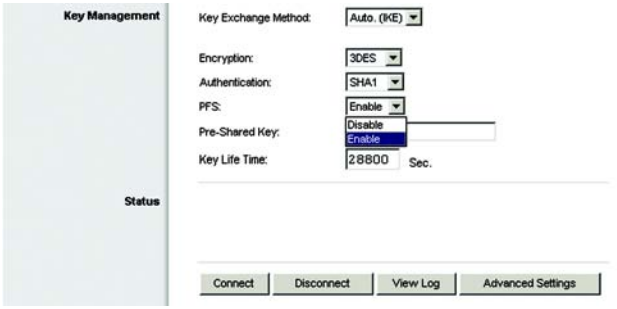


Figure 6-29: Key Exchange Method - Auto (IKE)

Manual

If you select Manual, you generate the key yourself, and no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purposes.

- Encryption Algorithm. When you select Manual, 3DES (168-bit) encryption is automatically selected. The same type of encryption must be used by the VPN device at the remote end of the tunnel.
- Encryption Key. This field specifies a key used to encrypt and decrypt IP traffic. The Encryption Key is 48-bit, so you should enter a key of 24 ASCII characters. Make sure both ends of the VPN tunnel use the same Encryption Key.
- Authentication Algorithm. Select a method of authentication, **MD5** or **SHA1**. This determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.
- Authentication Key. This field specifies a key used to authenticate IP traffic. Enter a key of hexadecimal values. If MD5 is selected, the Authentication Key is 32-bit, so you should enter 16 ASCII characters. If SHA is selected, the Authentication Key is 40-bit, so you should enter a key of 20 ASCII characters. Make sure both ends of the VPN tunnel use the same Authentication Key.
- Inbound and Outbound SPI (Security Parameter Index). SPI is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to select the SA, under which a packet should be processed. Hexadecimal values is acceptable, and the valid range is 100~ffffffff. Each tunnel must have a unique Inbound SPI and Outbound SPI. No two tunnels share the same SPI. The Incoming SPI here must match the Outgoing SPI value at the other end of the tunnel, and vice versa.

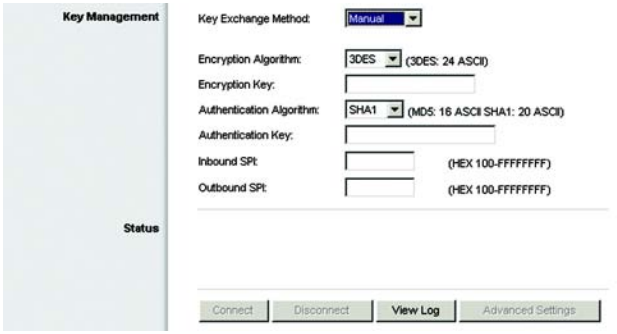


Figure 6-30: Key Exchange Method - Manual

Status

The status information for the Gateway's VPN tunnels is displayed here.

If you selected Manual, then you will have one button available. Click the **View Log** button to see the activity logs.

If you selected Auto (IKE), then you will have four buttons available. Click the **Connect** button to start the VPN connection.Click the **Disconnect** button to terminate the VPN connection. Click the **View Log** button to see the activity logs. Click the **Advanced Settings** button to configure the advanced settings of the VPN tunnel.

Figure 6-31: VPN Log

Advanced VPN Tunnel Setup

Click the **Advanced Settings** button, and the *Advanced VPN Tunnel Setup* screen will appear.

These advanced IPSec settings are for advanced users.

Phase 1

Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.

Operation Mode. There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Router will accept both Main and Aggressive requests from the remote VPN device.

Local Identity. Select the **Local IP address** or **Name** radio button. If you select Local IP address, then the Gateway's Internet IP address will be used. If you select Name, enter the Fully Qualified Domain Name (FQDN) of the Gateway in the field provided, so its current IP address can be located via DDNS.

Remote Identity. Select the **Remote IP address** or **Name** radio button. If you select Remote IP address, then the Internet IP address of the remote VPN device will be used. If you select Name, enter the Fully Qualified Domain Name (FQDN) of the remote VPN device in the field provided, so a current IP address can be located via DDNS.

Encryption. For encryption or decryption of ESP packets. 3DES (168-bit) encryption is automatically selected.

Authentication. Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA1. SHA1 is recommended because it is more secure.

Group. There are three Diffie-Hellman Groups to choose from: 768-bit, 1024-bit, and 1536-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Life Time. In the *Key Lifetime* field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Phase 2

Encryption. The encryption method selected in Phase 1 will be displayed.

Authentication. The authentication method selected in Phase 1 will be displayed.

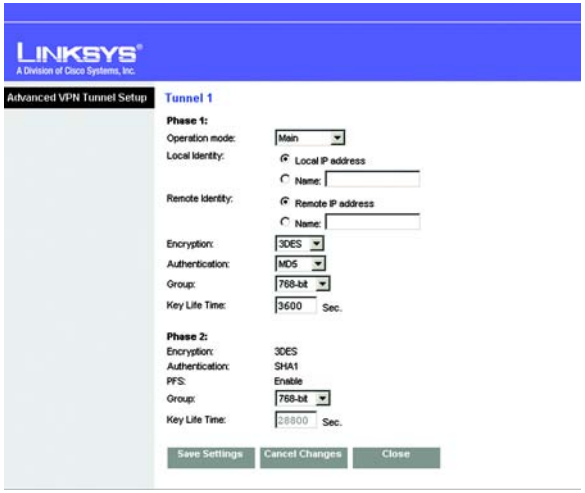


Figure 6-32: Advanced VPN Tunnel Setup

PFS. The status of the PFS (Perfect Forward Secrecy) feature will be displayed.

Group. There are three Diffie-Hellman Groups to choose from: 768-bit, 1024-bit, and 1536-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Life Time. In the *Key Lifetime* field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

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.

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. Click **Help** for more information.

The Access Restrictions Tab

The Internet Access Policy Tab

The *Internet Access Policy* screen allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific computers and block websites by URL address or keyword.

Internet Access Policy

Internet Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button 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 the **Delete** button. To view all the policies, click the **Summary** button. (Policies can be deleted from the *Summary* screen by selecting the policy or policies and clicking the **Delete** button. To return to the Internet Access screen, click the **Close** button.)

Status. Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and click the radio button beside *Enable*.

To create an Internet Access policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, click the radio button beside *Enable*.
3. Enter a Policy Name in the field provided.

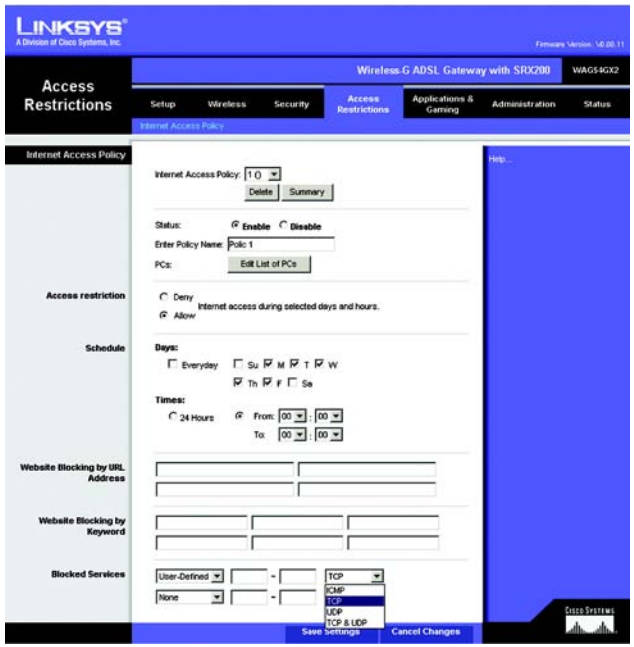


Figure 6-33: Internet Access Policy

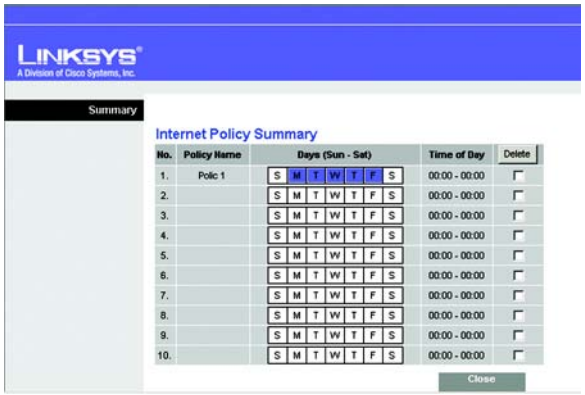


Figure 6-34: Internet Policy Summary

4. Click the **Edit List of PCs** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC 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 PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button to exit this screen.

5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.

6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

7. If you want to block websites with specific URL addresses, enter each URL in a separate field next to *Website Blocking by URL Address*.

8. If you want to block websites using specific keywords, enter each keyword in a separate field next to *Website Blocking by Keyword*.

9. You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. The port numbers and protocol for the selected service will be automatically displayed.

   If the service you want is not listed, select **User-Defined**. Enter its port numbers in the fields provided. Then select its protocol, **ICMP**, **TCP**, **UDP**, or **TCP & UDP** from the drop-down menu.

10. Click the **Save Settings** button to save the policy's settings. To undo the policy's settings, click the **Cancel Changes** button. Click **Help** for more information.

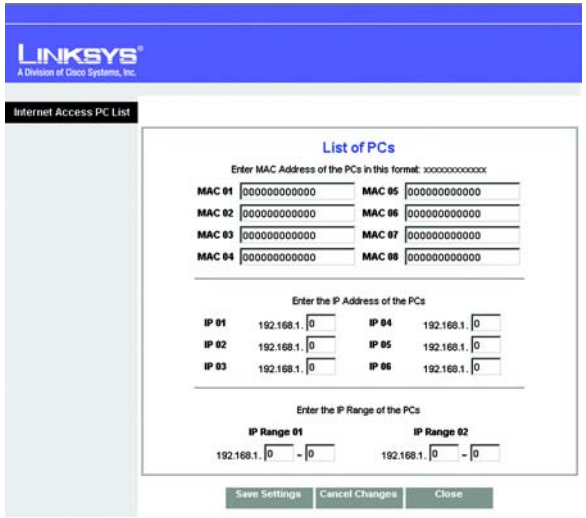


Figure 6-35: List of PCs

The Applications and Gaming Tab

The Single Port Range Forwarding Tab

Use the *Single Port Range Forwarding* screen when you want to open a specific port so users on the Internet can see the servers behind the Gateway (such servers may include FTP or e-mail servers). 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.

Single Port Forwarding

- Application. Enter the name of the application in the field provided.
- External Port and Internal Port. Enter the External and Internal Port numbers.
- Protocol. Select the protocol you wish to use for each application: **TCP** or **UDP**.
- IP Address. Enter the IP Address of the appropriate computer.
- Enabled. 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. Click **Help** for more information.

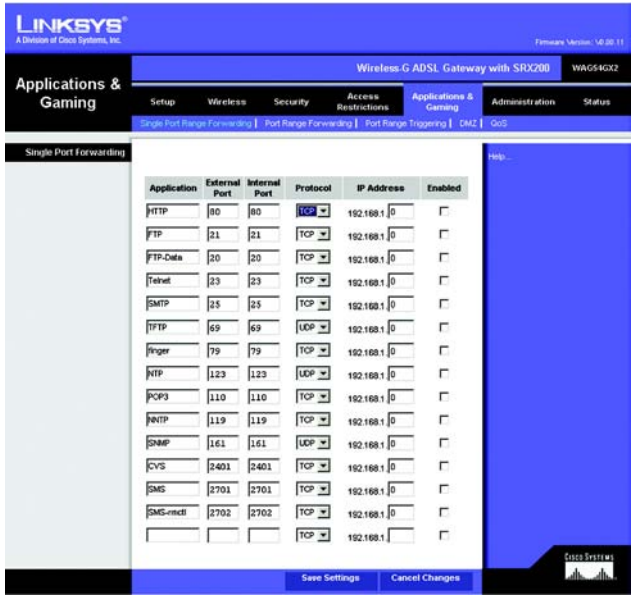


Figure 6-36: Single Port Forwarding

The Port Range Forwarding Tab

The *Port Range 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.

Port Range Forwarding

- Application. Enter the name of the application in the field provided.
- Start and End. Enter the starting and ending numbers of the port range you wish to forward.
- Protocol. Select the protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- IP Address. Enter the IP Address of the appropriate computer.
- Enable. Click the **Enable** checkbox 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. Click **Help** for more information.

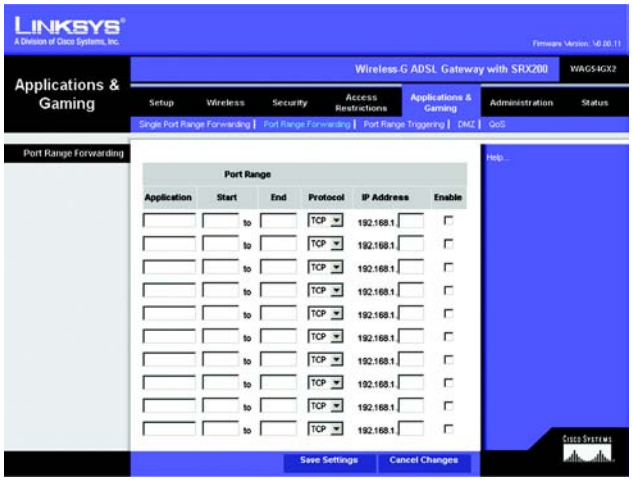


Figure 6-37: Port Range Forwarding

The Port Triggering Tab

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.

Port Range Triggering

- Application. Enter the name you wish to give each application.
- Triggered Range. Enter the starting and ending port numbers of the Triggered Range.
- Forwarded Range. Enter the starting and ending port numbers of the Forwarded Range.
- Enabled. Click the **Enabled** checkbox to enable port triggering 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. Click **Help** for more information.

Figure 6-38: Port Triggering

The DMZ Tab

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.

Figure 6-39: DMZ

DMZ

- 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 **Enable**. To disable DMZ, select **Disable**.
- 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 C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

The QoS Tab

QoS (Quality of Service)

QoS ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as Internet phone calls or videoconferencing.

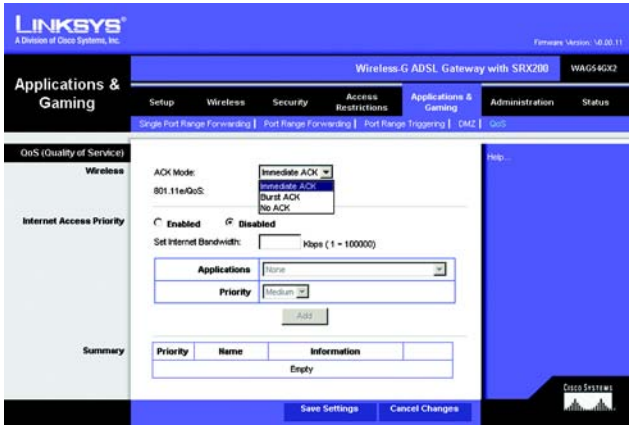


Figure 6-40: QoS

Wireless

- **ACK Mode**. This setting prioritizes QoS for users who also have ACK Mode enabled. Users with Immediate ACK (the default setting) will experience reliable connectivity for normal network use. Burst ACK is faster but less reliable and may also affect long-range wireless performance. The No ACK setting disables the ACK feature. Clients utilizing ACK must have their wireless adapter on the same setting as the Gateway. This is normally used in a multicast broadcast like video. Do not use this unless you are an advanced user.

- **802.11e/QoS**. QoS will be enabled by default to provide the best performance for your wireless connection. Select **Disable** to improve performance for a mixed wireless network.

Internet Access Priority

In this section, you can set priority based on Application, Port Range, or MAC Address. There are four priories you can set: High, Medium, Normal, or Low.

- Enabled/Disabled. To limit outgoing bandwidth for the QoS policies in use, select **Enabled**. Otherwise, select **Disabled**.

- Set Internet Bandwidth. This setting allows you to limit the outgoing bandwidth for the QoS policies in use, so you can control how much bandwidth a particular application is allowed to use. Enter the bandwidth in the field.

- Application. With this option you can select **None**, **Online Game**, **MSN Messenger**, **YAHOO Messenger**, **Skype**, **Voice Device, Add a New Application**, or select from the list of applications you want to set. To create a new entry, select **Add a New Application**, and refer to the *Add a New Application* section.

- Priority. Select **High**, **Medium**, **Normal**, or **Low** for the bandwidth priority you need for the application you selected. Don't set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select **Low**. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority. Once you have made your selection, click **Add** to add to the Summary list.

Online Game

Selecting Online Game will display the *Select a Game* drop-down menu, which will list a few common pre-configured games. Select the game from the list, and then select its priority.

MSN Messenger

Select its priority from the drop-down menu, and click **Add**.

YAHOO Messenger

Select its priority from the drop-down menu, and click **Add**.

Skype

Select its priority from the drop-down menu, and click **Add**.

Voice Device

Enter the name of your network device in the *Enter a Name* field, enter its MAC Address, select its priority from the drop-down menu, and click **Add**.

Add a New Application

Enter a Name — Enter any name to indicate the name of the entry.

Category — Select from **Port Range** or **MAC Address** for the Gateway to use to set the bandwidth priority.

Port Range — If you selected Port Range, then this category will be available. It allows you to enter the port range(s) that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

You can define up to three ranges for this bandwidth allocation. For each port range, designate the protocol type(s): **TCP**, **UDP**, or **Both**.

MAC Address — If you selected MAC Address, then this category will be available. Enter the 12 hexadecimal digit MAC Address to represent the device you want to set as a bandwidth priority. This is a unique identifier for your network device. When the Gateway identifies the device entered, the Gateway will allocate the priority set for that entry. Check the device's documentation to obtain the MAC Address.

Figure 6-41: QoS - Online Game

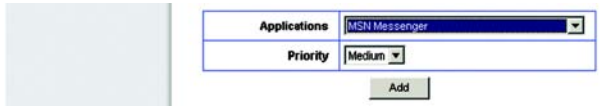


Figure 6-42: QoS - MSN Messenger

Figure 6-43: QoS - Voice Device

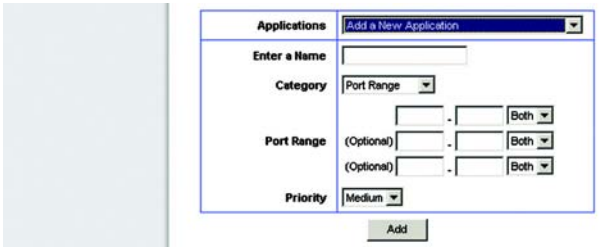


Figure 6-44: QoS - Add a New Application (Port Range)

Priority — Select the bandwidth priority for the application you selected. Select **High**, **Medium**, **Normal**, or **Low** for the bandwidth, but don't set all applications to High. Once you have made your selection, click **Add** to add to the Summary list.

Summary

Priority — This displays the bandwidth allocation priority of High, Medium, Normal, or Low, that you set for the application.

Name — This displays the application name or the entries you entered to be allocated.

Information — This displays the Port Range or MAC Address entered when you added a new application. If a pre-configured application was selected, there will be no valid entry shown in this section.

Remove — This button allows you to remove the application entry. To remove the entry, click the **Remove** button. To save the configuration, click the **Save Settings** button. Otherwise, to cancel, click the **Cancel Changes** 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. Click **Help** for more information.

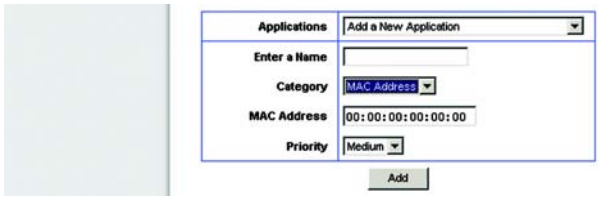


Figure 6-45: QoS - Add a New Application (MAC Address)

The Administration Tab

The Management Tab

The *Management* screen allows you to change the Gateway's access settings as well as configure the SNMP (Simple Network Management Protocol), UPnP (Universal Plug and Play), and WLAN management features.

Figure 6-46: Management

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 Userlist. Select the number of the user from the drop-down menu.
- Gateway Username. Enter the default username, **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, **admin**, 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.

- Remote Management. This feature allows you to manage the Gateway from a remote location via the Internet. To enable Remote Management, click **Enable**.

IMPORTANT: Enabling remote management allows anyone with your password to configure the Gateway from somewhere else on the Internet.

- Management Port. Enter the port number you will use to remotely access the Gateway.

SNMP

SNMP is a popular network monitoring and management protocol.

- Device Name. Enter the name of the Gateway.
- SNMP. To enable SNMP, click **Enable**. To disable SNMP, click **Disable**.
- Get Community. Enter the password that allows read-only access to the Gateway's SNMP information.

- Set Community. Enter the password that allows read/write access to the Gateway's SNMP information.
- Trap Management: Trap to. Enter the IP address of the remote host computer that will receive the trap messages.

UPnP

UPnP allows Windows Me and XP to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing.

- UPnP. To enable UPnP, click **Enable**. Otherwise, click **Disable**.

WLAN

- Management via 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. To enable this feature, click **Enable**. Otherwise, click **Disable**.

IGMP

- IGMP Proxy. If your multimedia application or device is not working properly behind the Gateway, then you can use the IGMP Proxy feature to allow multicast traffic through the Gateway. To use this feature, click **Enable**. Otherwise, click **Disable**.

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. Click **Help** for more information.

The Reporting Tab

The *Reporting* screen 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.

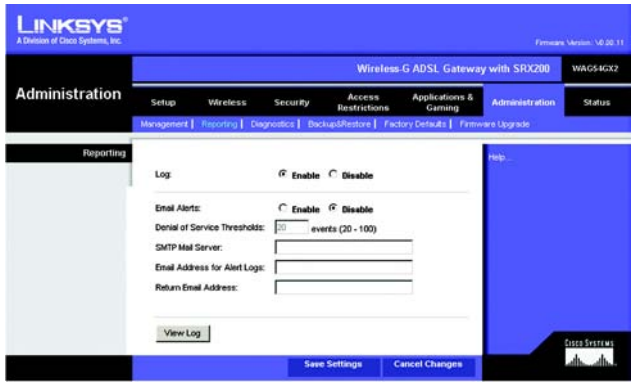


Figure 6-48: Reporting

Reporting

- Log. To enable log reporting, click **Enable**.

Email Alerts

- E-Mail Alerts. To enable E-Mail Alerts, click **Enable**.
- Denial of Service Thresholds. Enter the number of Denial of Service attacks that will trigger an e-mail alert.
- SMTP Mail Server. Enter the IP address of the SMTP server.
- E-Mail Address for Alert Logs. Enter the e-mail address that will receive alert logs.
- Return E-Mail address. Enter the return address for the e-mail alerts.

To view the logs, click the **View Logs** button. A new screen will appear. From the drop-down menu, select which log you want to view: **ALL**, **Access Log**, or **Firewall Log**. Click the **pageRefresh** button to refresh the information. Click the **Clear** button to clear the log information. Click the **Previous Page** button to go to the previous page of information. Click the **Next Page** button to move to the next page of information.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

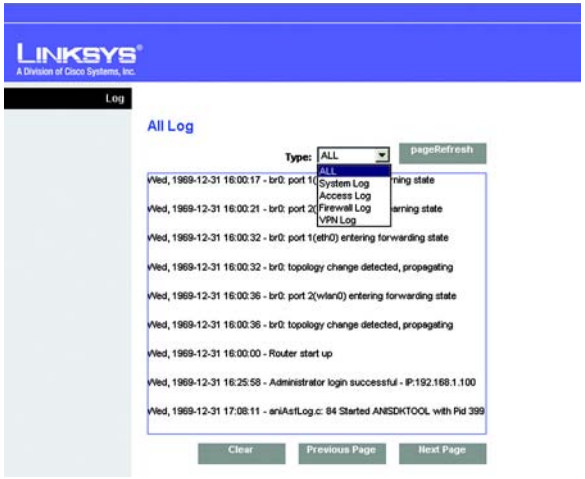


Figure 6-49: System Log

The Diagnostics Tab

Use this screen to run ping tests and display test results.

Ping Test

Ping Test Parameters

- Ping Target IP. Enter the IP address that you want to ping. This can be either a local (LAN) IP or an Internet (WAN) IP address.
- Ping Size. Enter the size of the packet.
- Number of Pings. Enter the number of times that you want to ping.
- Ping Interval. Enter the ping interval (how often the target IP address will be pinged) in milliseconds.
- Ping Timeout. Enter the ping timeout (how long before the ping test times out) in milliseconds.

Click the **Start Test** button to start the Ping Test.

- Ping Result. The results of the ping test will be shown 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. Click **Help** for more information.

Figure 6-50: Diagnostics

The Backup&Restore Tab

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

Backup Configuration

To back up the Gateway's configuration file, click the **Backup** button. Then follow the on-screen instructions.

Restore Configuration

To restore the Gateway's configuration file, click the **Browse** button. Then follow the on-screen instructions to locate the file. After you have selected the file, click the **Restore** button.

Click **Help** for more information.

Figure 6-51: Backup&Restore

The Factory Defaults Tab

If you want to restore the Gateway's factory default settings, then use this screen.

Factory Defaults

Restore Factory Defaults. If you wish to restore the Gateway to its factory default settings and lose all your settings, click **Restore Factory Defaults**. Then follow the on-screen instructions. Click **Help** for more information.

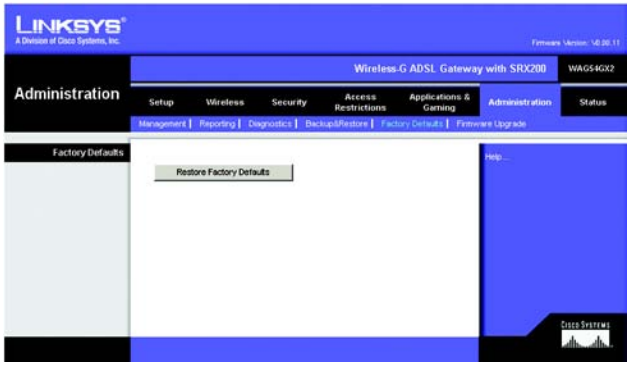


Figure 6-52: Factory Defaults

The Firmware Upgrade Tab

Use this screen to upgrade the Gateway's firmware.

Firmware Upgrade

To upgrade the Gateway's firmware:

1. Download the Gateway's firmware upgrade file from www.linksys.com/international.
2. Extract the file on your computer.
3. On the *Firmware Upgrade* screen, click the **Browse** button to find the firmware upgrade file.
4. Double-click the firmware file that you have downloaded and extracted.
5. Click the **Start to Upgrade** button, and follow the on-screen instructions.

Click **Help** for more information.

Figure 6-53: Firmware Upgrade

The Status Tab

The Gateway Tab

This screen displays information about the Gateway and its Internet connection.

Gateway Information

This section displays the Gateway's Firmware Version, MAC Address, and Current Time.

Internet Connection

This section shows the following information: Login Type, Interface, IP Address, Subnet Mask, Default Gateway, and DNS 1, 2, and 3 server IP addresses.

Figure 6-54: Gateway

DHCP Renew. If available, click the **DHCP Renew** button to replace the Gateway's current IP address with a new IP address.

DHCP Release. If available, click the **DHCP Release** button to delete the Gateway's current IP address.

Click the **Refresh** button if you want to refresh the displayed information. Click **Help** for more information.

The Local Network Tab

This screen displays information about the Gateway's local network.

Local Network

This screen displays the following: the local Mac Address, IP Address, Subnet Mask, DHCP Server, Start IP Address, and End IP Address.

To view the DHCP Client Table, click the **DHCP Client Table** button. To view the ARP/RARP Table, click the **ARP/RARP Table** button.

DHCP Clients Table. The DHCP Active IP Table shows the current DHCP Client data. You will see the computer name, IP address, MAC address, and expiration time of the dynamic IP address for the clients using the DHCP server. (This data is stored in temporary memory and changes periodically.) Click the **Refresh** button if you want to refresh the displayed information. To delete a client from the DHCP server, select the client, and then click the **Delete** button. Click the **Close** button to return to the *Local Network* screen.

ARP/RARP Table. An ARP request is a request sent by the Gateway asking clients with IP addresses for their MAC addresses, so the Gateway can map IP addresses to MAC addresses. RARP is the reverse of ARP. The ARP/RARP Table shows the current data for the local network clients of the Gateway. You will see their IP addresses and MAC addresses. (This data is stored in temporary memory and changes periodically.) Click the **Refresh** button if you want to refresh the displayed information. Click the **Close** button to return to the *Local Network* screen.

Click the **Refresh** button if you want to refresh the displayed information. Click **Help** for more information.

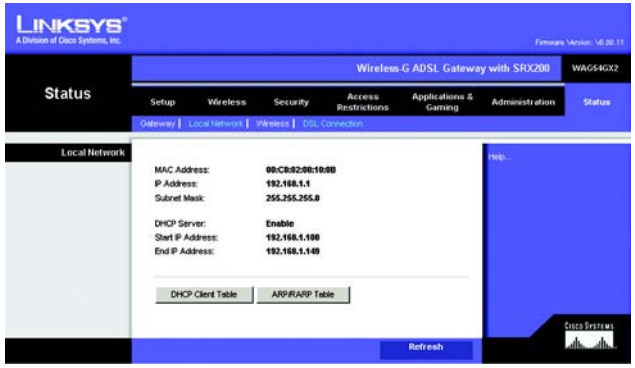


Figure 6-55: Local Network

Figure 6-56: DHCP Active IP Table

Figure 6-57: ARP/RARP Table

The Wireless Tab

This screen displays information about the Gateway's wireless network.

Wireless

This screen displays the following: the Wireless Firmware Version, MAC Address, Mode, SSID, Channel, and Encryption Function.

Click the **Wireless Clients Connected** button to view a list of the wireless clients connected to the Gateway, along with their computer names, IP addresses, and MAC addresses. Click the **Refresh** button if you want to refresh the displayed information. Click the **Close** button to return to the *Wireless* screen.

Click the **Refresh** button if you want to refresh the displayed information. Click **Help** for more information.

Figure 6-58: Wireless

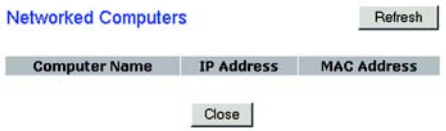


Figure 6-59: Networked Computers

The DSL Connection Tab

This screen shows information about the DSL connection.

DSL Status

This section shows the following: Status, Downstream Rate, and Upstream Rate.

PVC Connection

This section displays the following information: Encapsulation, Multiplexing, QoS, Pcr Rate, Scr Rate, Autodetect, VPI, VCI, Enable status, and PVC Status.

Click the **Refresh** button if you want to refresh the displayed information. Click **Help** for more information.

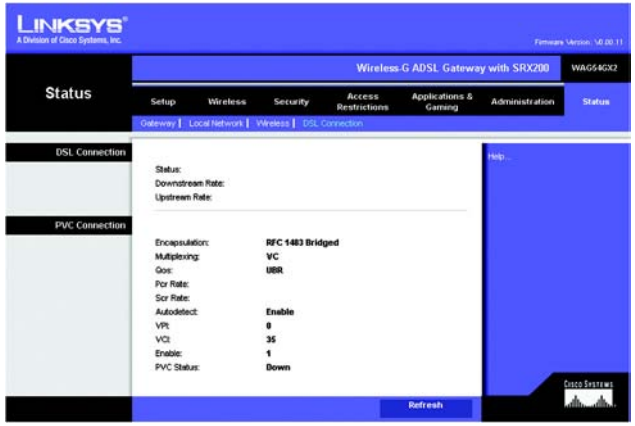


Figure 6-60: DSL Connection

Appendix A: Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems that may occur during the installation and operation of the Gateway. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the Linksys international website at www.linksys.com/international.

Common Problems and Solutions

1. I need to set a static IP address on a computer.

You can assign a static IP address to a computer by performing the following steps:

- For Windows 98 and Me:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
  2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
  3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway. Make sure that each IP address is unique for each computer or network device.
  4. Click the **Gateway** tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Gateway. Click the Add button to accept the entry.
  5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
  6. Click the **OK** button in the TCP/IP properties window, and click Close or the OK button for the Network window.
  7. Restart the computer when asked.
- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
  3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
  5. Enter the Subnet Mask, 255.255.255.0.
  6. Enter the Default Gateway, 192.168.1.1 (Gateway's default IP address).

7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
9. Restart the computer if asked.

- For Windows XP:

  The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

  1. Click **Start** and **Control Panel**.
  2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
  3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the Properties option.
  4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
  5. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
  6. Enter the Subnet Mask, 255.255.255.0.
  7. Enter the Default Gateway, 192.168.1.1 (Gateway's default IP address).
  8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

- Refer to Windows Help for details. Make sure Obtain IP address automatically is selected in the settings.

For Windows NT 4.0:

- Click **Start**, **Setting**s, and **Control Panel**. Double-click the **Network** icon.
- Click the Protocol tab, and double-click on TCP/IP Protocol.
- When the window appears, make sure you have selected the correct Adapter for your Ethernet adapter and set it for **Obtain an IP address** from a DHCP server.
- Click the **OK** button in the TCP/IP Protocol Properties window, and click the **Close** button in the Network window.
- Restart the computer if asked.

B. Open a command prompt.

For Windows 98 and Me:

- Click **Start** and **Run**. In the Open field, type in command. Press the **Enter** key or click the **OK** button.

For Windows NT, 2000, and XP:

- Click **Start** and **Run**. In the Open field, type cmd. Press the **Enter** key or click the **OK** button. In the command prompt, type ping 192.168.1.1 and press the Enter key.
- If you get a reply, the computer is communicating with the Gateway.
- If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

C. In the command prompt, type ping followed by your Internet or WAN IP address and press the **Enter** key. The Internet or WAN IP Address can be found on the Status screen of the Gateway's web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter ping 1.2.3.4 and press the Enter key.

- If you get a reply, the computer is connected to the Gateway.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

D. In the command prompt, type ping www.yahoo.com and press the **Enter** key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. I am not getting an IP address on the Internet with my Internet connection.

- Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
  1. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA, Bridged Mode Only, or IPoA. Please refer to the Setup section of "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200" for details on Internet connection settings.
  2. Make sure you have the right cable. Check to see if the Gateway column has a solidly lit ADSL LED.
  3. Make sure the cable connecting from your Gateway's ADSL port is connected to the wall jack of the ADSL service line. Verify that the Status page of the Gateway's web-based utility shows a valid IP address from your ISP.
  4. Turn off the computer and Gateway. Wait 30 seconds, and then turn on the Gateway, and computer. Check the Status tab of the Gateway's web-based utility to see if you get an IP address.

4. I am not able to access the Setup page of the Gateway's web-based utility.

- Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Gateway.
  1. Refer to "Appendix C: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
  2. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."

3. Refer to "Problem #10: I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window."

5. I can't get my Virtual Private Network (VPN) working through the Gateway.

Access the Gateway's web interface by going to http://192.168.1.1 or the IP address of the Gateway, and go to the Security tab. Make sure you have IPsec passthrough and/or PPTP pass-through enabled.

- VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Gateway; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.
- VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Gateway. AH has limitations due to occasional incompatibility with the NAT standard.
- Change the IP address for the Gateway to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Gateway will have difficulties routing information to the right location. If you change the Gateway's IP address to 192.168.2.1, that should solve the problem. Change the Gateway's IP address through the Setup tab of the web interface.
- If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.
- Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.
- Check the Linksys international website for more information at www.linksys.com/international.

6. I need to set up a server behind my Gateway and make it available to the public.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

- Follow these steps to set up port forwarding through the Gateway's web-based utility. We will be setting up web, ftp, and mail servers.
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
  2. Enter any name you want to use for the Customized Application.
  3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
  4. Check the protocol you will be using, TCP and/or UDP.
  5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the

field provided. Check "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

6. Check the Enable option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
Web server	80 to 80	X		192.168.1.100	X
FTP server	21 to 21	X		192.168.1.101	X
SMTP (outgoing)	25 to 25	X		192.168.1.102	X
POP3 (incoming)	110 to 110	X		192.168.1.102	X

When you have completed the configuration, click the **Save Settings** button.

7. I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Gateway to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Gateway's web interface by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
UT	7777 to 27900	X	X	192.168.1.100	X
Halflife	27015 to 27015	X	X	192.168.1.105	X
PC Anywhere	5631 to 5631		X	192.168.1.102	X
VPN IPSEC	500 to 500		X	192.168.1.100	X

When you have completed the configuration, click the **Save Settings** button.

8. I can't get the Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one computer to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Gateway will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Gateway will send the data to whichever computer or network device you set for DMZ hosting.)

- Follow these steps to set DMZ hosting:
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => DMZ tab. Click Enabled and enter the IP of the computer.
  2. Check the Port Forwarding pages and disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
- Once completed with the configuration, click the **Save Settings** button.

9. I forgot my password, or the password prompt always appears when I am saving settings to the Gateway.

- Reset the Gateway to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Enter the default username and password **admin**, and click the **Administrations** => **Management** tab.
  2. Enter a different password in the Gateway Password field, and enter the same password in the second field to confirm the password.
  3. Click the **Save Settings** button.

10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Gateway is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

- For Microsoft Internet Explorer 5.0 or higher:
  1. Click **Start, Settings**, and **Control Panel**. Double-click Internet Options.
  2. Click the **Connections** tab.
  3. Click the **LAN settings** button and remove anything that is checked.
  4. Click the **OK** button to go back to the previous screen.
  5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

- For Netscape 6 or higher:
  1. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
  2. Make sure you have Direct connection to the Internet selected on this screen.
  3. Close all the windows to finish.

11. To start over, I need to set the Gateway to factory default.

Hold the **Reset** button for 10 seconds and then release it. This will return the Internet settings, password, forwarding, and other settings on the Gateway to the factory default settings. In other words, the Gateway will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys international website and download the latest firmware at www.linksys.com/international.

- Follow these steps:
  1. Go to the Linksys international website at http://www.linksys.com/international and select your region or country.
  2. Click the **Products** tab and select the Gateway.
  3. On the Gateway's webpage, click **Firmware**, and then download the latest firmware for the Gateway.
  4. To upgrade the firmware, follow the steps in the Administration section found in "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200."

13. The firmware upgrade failed, and/or the Power LED is flashing.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Power LED stop flashing:

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the computer; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:
  IP Address: 192.168.1.50
  Subnet Mask: 255.255.255.0
  Gateway: 192.168.1.1
- Perform the upgrade using the TFTP program or the Gateway's web-based utility through its Administration tab.

14. My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet.

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

1. To connect to the Gateway, go to the web browser, and enter http://192.168.1.1 or the IP address of the Gateway.
2. Enter the username and password, if asked. (The default username and password is admin.)
3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 30 (seconds) (this will keep the connection to the ISP and will not disconnect.
4. Click the **Save Settings** button. Click the **Status** tab, and click the **Connect** button.
5. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
6. Click the **Save Settings** button to continue.

- If the connection is lost again, follow steps 1- 6 to re-establish connection.

15. I can't access my e-mail, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set automatically.

- If you are having some difficulties, perform the following steps:
  1. To connect to the Gateway, go to the web browser, and enter http://192.168.1.1 or the IP address of the Gateway.
  2. Enter the username and password, if asked. (The default username and password is admin.)
  3. Look for the MTU option, and select **Manual**. In the Size field, enter 1492.
  4. Click the **Save Settings** button to continue.
- If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
  1462
  1400
  1362
  1300

16. The Power LED flashes continuously.

The Power LED lights up when the device is first powered up. In the meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED remains steady to show that the system is working fine. If the LED continues to flash after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.

- Check if other computers work. If they do, ensure that your computer's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the computers are configured correctly, but still not working, check the Gateway. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)

- If the Gateway is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Gateway to verify a direct connection.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

18. I'm trying to access the Gateway's Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, "404 Forbidden."

If you are using Windows Explorer, perform the following steps until you see the Web-based Utility's login screen (Netscape Navigator will require similar steps):

1. Click **File**. Make sure *Work Offline* is NOT checked.
2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.

- Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

Frequently Asked Questions

What is the maximum number of IP addresses that the Gateway will support?
The Gateway will support up to 253 IP addresses.

Is IPSec Passthrough supported by the Gateway?
Yes, it is a built-in feature that is enabled by default.

Where is the Gateway installed on the network?
In a typical environment, the Gateway is installed between the ADSL wall jack and the LAN.

Does the Gateway support IPX or AppleTalk?
No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.

Does the LAN connection of the Gateway support 100Mbps Ethernet?
The Gateway supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Gateway.

What is Network Address Translation and what is it used for?
Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a computer connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Gateway to be used with low cost Internet accounts when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Gateway support any operating system other than Windows 98SE, Windows Millennium, Windows 2000, or Windows XP?
Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the Gateway support ICQ send file?
Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Gateway.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?
If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Gateway from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get Half-Life: Team Fortress to work with the Gateway?
The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?

Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.linksys.com/international for more information.

If all else fails in the installation, what can I do?

Reset the Gateway by holding down the reset button until the Power LED fully turns on and off. Reset your DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys international website, www.linksys.com/international.

How will I be notified of new Gateway firmware upgrades?

All Linksys firmware upgrades are posted on the Linksys international website at www.linksys.com/international, where they can be downloaded for free. To upgrade the Gateway's firmware, use the Administration tab of the Gateway's web-based utility. If the Gateway's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use.

Will the Gateway function in a Macintosh environment?

Yes, but the Gateway's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Gateway. What can I do?

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

What is DMZ Hosting?

Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

If DMZ Hosting is used, does the exposed user share the public IP with the Gateway?

No.

Does the Gateway pass PPTP packets or actively route PPTP sessions?

The Gateway allows PPTP packets to pass through.

Is the Gateway cross-platform compatible?
Any platform that supports Ethernet and TCP/IP is compatible with the Gateway.

How many ports can be simultaneously forwarded?
Theoretically, the Gateway can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

What are the advanced features of the Gateway?
The Gateway's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.

How can I check whether I have static or DHCP IP Addresses?
Consult your ISP to obtain this information.

How do I get mIRC to work with the Gateway?
Under the Port Forwarding tab, set port forwarding to 113 for the computer on which you are using mIRC.

Can the Gateway act as my DHCP server?
Yes. The Gateway has DHCP server software built-in.

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

What is the IEEE 802.11b standard?
It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11b and 802.11g features are supported?

The product supports the following IEEE 802.11b and IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

It also supports OFDM technology for 802.11g networking.

What is ad-hoc mode?

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other, peer-to-peer without the use of an access point.

What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a network through a wireless access point.

What is roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the computer must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is the ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Will the information be intercepted while it is being transmitted through the air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I reset the Gateway?
Press the Reset button on the back panel for about ten seconds. This will reset the Gateway to its default settings.

How do I resolve issues with signal loss?
There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Gateway and a wireless computer will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Gateway and your wireless computer in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.
Wireless security is probably enabled on the Gateway, but not on your wireless adapter (or vice versa). Verify that the same wireless security settings are being used on all devices of your wireless network.

How many channels/frequencies are available with the Gateway?
There are eleven available channels, ranging from 1 to 11, in most of North, Central, and South America. There are thirteen available channels, ranging from 1 to 13, in most of Europe. There may be additional channels available in other regions, subject to the regulations of your region and/or country.

If your questions are not addressed here, refer to the Linksys international website, www.linksys.com/international.

Appendix B: Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

For information on implementing these security features, refer to "Chapter 6: Configuring the Wireless-G ADSL Gateway with SRX200."

NOTE: Some of these security features are available only through the network gateway, router, or access point. Refer to the gateway, router, or access point's documentation for more information.

Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages". These messages can be easily decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier). Here are the steps you can take:

Change the administrator's password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

SSID. There are several things to keep in mind about the SSID:

1. Disable Broadcast
2. Make it unique
3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Use "Shared Key" authentication
3. Change your WEP key regularly

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. **WPA2** is the newer version of Wi-Fi Protected Access with stronger encryption than WPA. WPA gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. WPA Enterprise and WPA2 Enterprise use a RADIUS (Remote Authentication Dial-In User Service) server for authentication.

IMPORTANT: Always remember that each device in your wireless network MUST use the same encryption method and encryption key or your wireless network will not function properly.

WPA Personal. Select the type of algorithm, TKIP or AES, enter a password in the Passphrase field of 8-63 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Gateway or other device how often it should change the encryption keys.

WPA2 Personal. WPA2 gives you one encryption method, AES, with dynamic encryption keys. Enter a Passphrase of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Gateway how often it should change the encryption keys.

WPA2 Mixed Mode. WPA2 Mixed Mode gives you TKIP+AES encryption. Enter a Passphrase of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Gateway how often it should change the encryption keys.

WPA Enterprise. This method is WPA used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Gateway and its RADIUS server. Then enter a Key Renewal Timeout period, which instructs the Gateway how often it should change the encryption keys.

WPA2 Enterprise. This method is WPA2 used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Gateway and its RADIUS server. Then enter a Key Renewal Timeout period, which instructs the Gateway how often it should change the encryption keys.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering feature of the Gateway. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Gateway's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98 or Me Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.
2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Gateway via a CAT 5 Ethernet network cable. See Figure C-1.
3. Write down the Adapter Address as shown on your computer screen (see Figure C-2). This is the MAC address for your Ethernet adapter and is shown in hexadecimal as a series of numbers and letters.

   The MAC address/Adapter Address is what you will use for MAC filtering. The example in Figure D-2 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

   The example in Figure C-2 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

NOTE: The MAC address is also called the Adapter Address.

Figure C-1: IP Configuration Screen

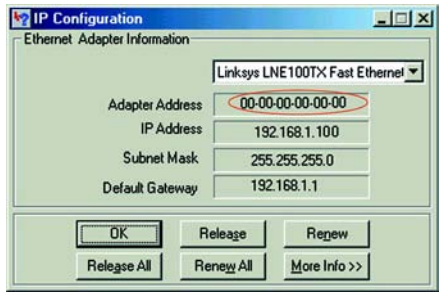


Figure C-2: MAC Address/Adapter Address

Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.

NOTE: The MAC address is also called the Physical Address.

2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.

3. Write down the Physical Address as shown on your computer screen (Figure C-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

   The MAC address/Physical Address is what you will use for MAC filtering. The example in Figure C-3 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

   The example in Figure C-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

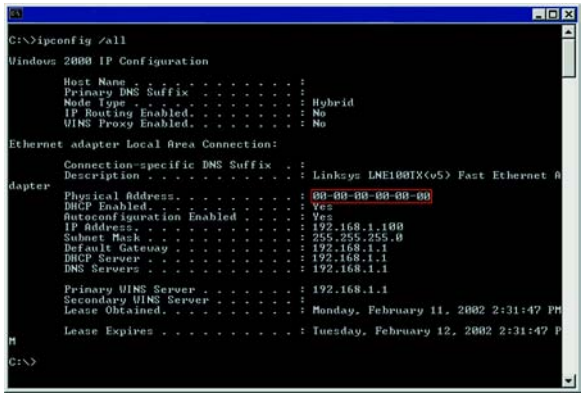


Figure C-3: MAC Address/Physical Address

Appendix D: Upgrading Firmware

To upgrade the Gateway's firmware:

1. Download the Gateway's firmware upgrade file from *www.linksys.com/international*.
2. Extract the file on your computer.
3. Open the Gateway's Web-based Utility and click the **Administration** tab.
4. Click the **Firmware Upgrade** tab.
5. Click the **Browse** button to find the extracted file, and then double-click it.
6. Click the **Upgrade** button, and follow the on-screen instructions.

Figure D-1: Firmware Upgrade

Appendix E: Glossary

802.11b - A wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - A wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - A device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (**A**dvanced **E**ncryption **S**tandard) - A security method that uses symmetric 128-bit block data encryption.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**De**militarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data transmitted in a network.

Ethernet - A networking protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a username and password system.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) - Frequency transmission that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel to prevent information from being lost in transit.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

PEAP (**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack**-45**) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (**U**ser **D**atagram **P**rotocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WEP (**W**ired **E**quivalent **P**rivacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Me utility that displays the IP address for a particular networking device.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix F: Specifications

Model Number	WAG54GX2
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, IEEE 802.3, g.992.1 (g.dmt), g.992.2 (g.lite) g.992.3, g.992.5, T1.413i2, Annex A (FR, EU, UK versions of the product)
Ports	Power, ADSL, Ethernet (1-4)
Button	Reset, Power
Cabling Type	CAT 5 UTP
LEDs	Power, Wireless, Ethernet (1-4), DSL, Internet
Number of Antennas	2
Antenna Connector Type	Fixed (not removable)
RF Pwr (EIRP) in dBm	802.11b: 18, 802.11g: 16, 802.11g MiMo: 17
Antenna Gain in dBi	3.3
UPnP able/cert	Able

Security Features	Password protected configuration for web access PAP and CHAP authentication Denial of Service (DoS) Prevention URL filtering, and keyword, Java, ActiveX, Proxy, Cookie blocking ToD filter (Blocks Access by Time VPN Passthrough for IPSec, PPTP, and L2TP Protocols 128, 64 bits WEP with Passphrase WEP key generation SSID Broadcast Disable Access restriction by MAC and IP addresses Support IPSec VPN Terminal, up to 5 tunnels Support WPA and WPA2
WEP Key Bits	64, 128
Dimensions	140 mm x 140 mm x 27 mm (5,51" x 5,51" x 1,06")
Unit Weight	0,27 kg (9,60 oz.)
Power	12VDC 1A
Certifications	CE
Operating Temp.	32º~104ºF (0º~40ºC)
Storage Temp.	-4º~158ºF (-20º~70ºC)
Operating Humidity	10~85% Non-Condensing
Storage Humidity	5~90% Non-Condensing

Appendix G: Warranty Information

Linksys warrants to You that, for a period of three 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. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

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.

This Warranty is valid and may be processed only in the country of purchase.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix H: Regulatory Information

FCC Statement

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Industry Canada (Canada)

This device complies with Canadian ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry Canada.

Compliance Information for 2.4-GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

Declaration of Conformity with Regard to the EU Directive 1999/5/EC (R&TTE Directive)

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

NOTE: For all products, the Declaration of Conformity is available through one or more of these options:

- A pdf file is included on the product's CD.
- A print copy is included with the product.
- A pdf file is available on the product's webpage. Visit www.linksys.com/international and select your country or region. Then select your product.

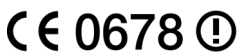
If you need any other technical documentation, see the "Technical Documents on www.linksys.com/international" section, as shown later in this appendix.

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950

CE Marking

For the Linksys Wireless-B and Wireless-G products, the following CE mark, notified body number (where applicable), and class 2 identifier are added to the equipment.

 or  or 

Check the CE label on the product to find out which notified body was involved during the assessment.

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

France

In case the product is used outdoors, the output power is restricted in some parts of the band. See Table 1 or check http://www.art-telecom.fr/ for more details.

Dans la cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez http://www.art-telecom.fr/ pour de plus amples détails.

Table 1: Applicable Power Levels in France

Location	Frequency Range (MHz)	Power (EIRP)
Indoor (No restrictions)	2400-2483.5	100 mW (20 dBm)
Outdoor	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless operating within the boundaries of the owner's property, the use of this 2.4 GHz Wireless LAN product requires a 'general authorization'. Please check with http://www.comunicazioni.it/it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Product Usage Restrictions

This product is designed for indoor usage only. Outdoor usage is not recommended.

This product is designed for use with the standard, integral or dedicated (external) antenna(s) that is/are shipped together with the equipment. However, some applications may require the antenna(s), if removable, to be separated from the product and installed remotely from the device by using extension cables. For these applications, Linksys offers an R-SMA extension cable (AC9SMA) and an R-TNC extension cable (AC9TNC). Both of these cables are 9 meters long and have a cable loss (attenuation) of 5 dB. To compensate for the attenuation, Linksys also offers higher gain antennas, the HGA7S (with R-SMA connector) and HGA7T (with R-TNC connector). These antennas have a gain of 7 dBi and may only be used with either the R-SMA or R-TNC extension cable.

Combinations of extension cables and antennas resulting in a radiated power level exceeding 100 mW EIRP are illegal.

Power Output of Your Device

To comply with your country's regulations, you may have to change the power output of your wireless device. Proceed to the appropriate section for your device.

NOTE: The power output setting may not be available on all wireless products. For more information, refer to the documentation on your product's CD or http://www.linksys.com/international.

Wireless Adapters

Wireless adapters have the power output set to 100% by default. Maximum power output on each adapter does not exceed 20 dBm (100 mW); it is generally 18 dBm (64 mW) or below. If you need to alter your wireless adapter's power output, follow the appropriate instructions for your computer's Windows operating system:

Windows XP
1. Double-click the **Wireless** icon in your desktop's system tray.
2. Open the *Wireless Network Connection* window.
3. Click the **Properties** button.
4. Select the **General** tab, and click the **Configure** button.
5. In the *Properties* window, click the **Advanced** tab.
6. Select **Power Output**.
7. From the pull-down menu on the right, select the wireless adapter's power output percentage.

Windows 2000
1. Open the **Control Panel**.
2. Double-click **Network and Dial-Up Connections**.
3. Select your current wireless connection, and select **Properties**.
4. From the *Properties* screen, click the **Configure** button.
5. Click the **Advanced** tab, and select **Power Output**.
6. From the pull-down menu on the right, select the wireless adapter's power setting.

If your computer is running Windows Millennium or 98, then refer to Windows Help for instructions on how to access the advanced settings of a network adapter.

Wireless Access Points, Routers, or Other Wireless Products

If you have a wireless access point, router or other wireless product, use its Web-based Utility to configure its power output setting (refer to the product's documentation for more information).

Technical Documents on www.linksys.com/international

Follow these steps to access technical documents:

1. Browse to http://www.linksys.com/international.
2. Click the region in which you reside.
3. Click the name of the country in which you reside.
4. Click **Products**.
5. Click the appropriate product category.
6. Select a product.
7. Click the type of documentation you want. The document will automatically open in PDF format.

NOTE: If you have questions regarding the compliance of these products or you cannot find the information you need, please contact your local sales office or visit http://www.linksys.com/international for more details.

Appendix I: Contact Information

Need to contact Linksys?
Visit us online for information on the latest products and updates to your existing products at:
http://www.linksys.com/international

If you experience problems with any Linksys product, you can e-mail us at:

In Europe	E-mail Address
Austria	support.at@linksys.com
Belgium	support.be@linksys.com
Denmark	support.dk@linksys.com
France	support.fr@linksys.com
Germany	support.de@linksys.com
Italy	support.it@linksys.com
Netherlands	support.nl@linksys.com
Norway	support.no@linksys.com
Portugal	support.pt@linksys.com
Spain	support.es@linksys.com
Sweden	support.se@linksys.com
Switzerland	support.ch@linksys.com
United Kingdom & Ireland	support.uk@linksys.com

Outside of Europe	E-mail Address
Asia Pacific	asiasupport@linksys.com (English only)
Latin America	support.portuguese@linksys.com or support.spanish@linksys.com
Middle East & Africa	support.mea@linksys.com (English only)
U.S. and Canada	support@linksys.com

LINKSYS®
A Division of Cisco Systems, Inc.

2,4 GHz 802.11g

Wireless-G

WIRELESS

ADSL-Gateway mit SRX200

Benutzerhandbuch

Modell-Nr. **WAG54GX2 (DE)**

CISCO SYSTEMS

Copyright und Marken

Hinweise zur Verwendung dieses Handbuchs

Ziel des Benutzerhandbuchs zum Wireless-G ADSL-Gateway mit SRX200 ist, Ihnen den Einstieg in den Netzwerkbetrieb mit dem Gateway noch weiter zu erleichtern. Achten Sie beim Lesen dieses Benutzerhandbuchs auf Folgendes:

Dieses Häkchen kennzeichnet einen Hinweis, den Sie bei Verwendung des Gateways besonders beachten sollten.

Dieses Ausrufezeichen kennzeichnet eine Warnung und weist darauf hin, dass unter bestimmten Umständen Schäden an Ihrem Eigentum oder am Gateway verursacht werden können.

Dieses Fragezeichen dient als Erinnerung an bestimmte Schritte, die bei Verwendung des Gateways durchzuführen sind.

Neben den Symbolen finden Sie Definitionen für technische Begriffe, die in folgender Form dargestellt werden:

Wort: *Definition.*

Alle Abbildungen (Diagramme, Bildschirmdarstellungen und andere Bilder) sind mit einer Abbildungsnummer und einer Kurzbeschreibung versehen (siehe folgendes Beispiel):

Abbildung 0-1: Kurzbeschreibung der Abbildung

Die Abbildungsnummern und die zugehörigen Kurzbeschreibungen finden Sie auch im Inhalt unter „Abbildungsverzeichnis“.

Inhalt

Abbildungsverzeichnis

Kapitel 1: Einführung

Willkommen

Vielen Dank, dass Sie sich für ein Wireless-G ADSL-Gateway mit SRX200 entschieden haben. Mit diesem Gateway stehen den Computern eine High Speed-Internetverbindung und Ressourcen wie beispielsweise Dateien und Drucker zur Verfügung.

Wie schafft das Gateway das? Wenn das Gateway mit dem Internet sowie Computern und Peripheriegeräten verbunden wird, kann die Netzwerkkommunikation durch das Gateway gesteuert und überwacht werden. Und da es sich um ein Wireless-Gateway handelt, kann der Internetzugriff sowohl als Wireless-Übertragung als auch über das verdrahtete Netzwerk erfolgen.

Der Wireless-G ADSL-Gateway mit SRX200 kombiniert eine neue Antennentechnologie mit dem standardisierten Wireless-G (802.11g)-Netzwerkbetrieb. Die hier verwendete MIMO-Technologie (*Multiple Inputs - Multiple Outputs*) überlagert die Signale zweier Wireless-G-kompatibler Funkgeräte und verdoppelt so praktisch die Datenrate. Im Gegensatz zu den üblichen Wireless-Netzwerktechnologien, bei denen sich Signalreflexionen störend auswirken, verwendet die MIMO-Technologie diese Reflexionen, um die Reichweite zu erhöhen und tote Punkte im Wireless-Empfangsbereich zu beseitigen. Das robuste Signal hat eine größere Reichweite, so dass in Wireless-Verbindungen über bis zu zweimal höhere Entfernungen aufrechterhalten werden können als bei standardmäßigen Wireless-G-Systemen. Je größer die Entfernung, desto größer der Vorteil: Mit der höheren Datenrate und der reflexionsresistenten Technologie lässt sich in manchen Situationen ein bis zu sechsmal höherer Durchsatz erzielen als bei Wireless-G. Interferenzen werden dadurch vermieden, dass das Gateway dynamisch zum Kanal mit dem deutlichsten Signal wechselt. Auch bei standardmäßigen Wireless-G- und Wireless-B-Systemen lässt sich die Leistung verbessern, wenn diese mit SRX-fähigen Geräten kommunizieren.

Zum Schutz der Daten und der Privatsphäre bietet die WEP-Verschlüsselung darüber hinaus bessere Sicherheitsoptionen, während das gesamte Netzwerk durch die SPI-Firewall (*Stateful Packet Inspection*) und NAT-Technologie geschützt ist. Zudem können Sie Ihre Familie mit Kinderschutzfunktionen wie dem Einschränken der Internetzugriffszeiten und dem Blockieren von Schlüsselwörtern schützen. Der Zugriff auf diese Sicherheitsfunktionen sowie auf die anderen Einstellungen des Gateways erfolgt über ein benutzerfreundliches, browserbasiertes Dienstprogramm.

Und was genau bedeutet das?

***802.11b**: IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 11 MBit/s sowie eine Betriebsfrequenz von 2,4 GHz festlegt.*

***802.11g**: IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 MBit/s und eine Betriebsfrequenz von 2,4 GHz festlegt sowie Abwärtskompatibilität mit Geräten garantiert, die dem Standard 802.11b entsprechen.*

***WPA** (Wi-Fi Protected Access): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (Temporal Key Integrity Protocol) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann.*

***SPI-Firewall** (Stateful Packet Inspection): Eine Technologie zur Überprüfung von eingehenden Datenpaketen, bevor diese an das Netzwerk weitergeleitet werden.*

***Firewall**: Sicherheitsmaßnahmen, durch die die Ressourcen in einem lokalen Netzwerk vor dem Zugriff durch nicht autorisierte Dritte geschützt werden.*

***NAT** (Network Address Translation): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.*

Mit Netzwerken können Sie einen Internetzugang und Computer-Ressourcen gemeinsam mit anderen nutzen. Sie können von verschiedenen Computern aus auf einem Drucker drucken und auf Daten zugreifen, die auf der Festplatte eines anderen Computers gespeichert sind. Netzwerke eignen sich darüber hinaus auch für Videospiele mit mehreren Spielern. Netzwerke sind also nicht nur zu Hause und im Büro nützlich, sondern lassen sich auch für Unterhaltungszwecke nutzen.

Mehrere PCs in einem verdrahteten Netzwerk stellen ein LAN (*Local Area Network*; Lokales Netzwerk) dar. Sie werden über Ethernetkabel angeschlossen, daher die Bezeichnung „verdrahtetes“ Netzwerk. Mit Wireless-Karten oder -Adaptern ausgerüstete PCs können ganz ohne lästige Kabel kommunizieren. Indem sie innerhalb ihres Übertragungsradius dieselben Wireless-Einstellungen verwenden, bilden sie ein Wireless-Netzwerk. Dies wird oft als WLAN oder *Wireless Local Area Network* (drahtloses lokales Netzwerk) bezeichnet. Da das Gateway mit Wireless-Funktionen ausgestattet ist, können verdrahtete Netzwerke und Wireless-Netzwerke miteinander verbunden werden, sodass sie miteinander kommunizieren können.

Durch das Verbinden aller verdrahteten und Wireless-Netzwerke sowie des Internets können Sie jetzt Dateien gemeinsam verwenden, auf das Internet zugreifen und sogar Spiele spielen. Dabei schützt der Wireless-G ADSL-Gateway mit SRX200 die Netzwerke stets vor nicht autorisierten und nicht willkommenen Benutzern.

Linksys empfiehlt die Verwendung der Installations-CD-ROM zur erstmaligen Installation des Gateways. Wenn Sie den Setup-Assistenten auf der Installations-CD-ROM nicht ausführen möchten, können Sie das Gateway anhand der Anweisungen in diesem Handbuch anschließen, einrichten und für die Verbindung mit den verschiedenen Netzwerken konfigurieren. Diese Anweisungen enthalten alle Informationen, die Sie zur optimalen Nutzung des Wireless-G ADSL-Gateways mit SRX200 benötigen.

***Netzwerk**: Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam verwenden, speichern und miteinander austauschen können.*

***LAN** (Local Area Network): Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr Heim- oder Büronetzwerk zusammensetzt.*

Inhalt dieses Benutzerhandbuchs

In diesem Benutzerhandbuch sind die zur Installation und Verwendung des Wireless-G ADSL-Gateways mit SRX200 erforderlichen Schritte aufgeführt.

- Kapitel 1: Einführung
  In diesem Kapitel werden die Anwendungen des Wireless-G ADSL-Gateways mit SRX200 sowie dieses Benutzerhandbuch beschrieben.

- Kapitel 2: Planen des Netzwerks
  In diesem Kapitel werden die Grundlagen des Netzwerkbetriebs beschrieben.

- Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways mit SRX200
  In diesem Kapitel werden die physischen Merkmale des Gateways beschrieben.

- Kapitel 4: Anschließen des Wireless-G Broadband-Gateways mit SRX200
  In diesem Kapitel finden Sie Anleitungen zum Anschließen des Gateways an Ihr Netzwerk.

- Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200
  In diesem Kapitel wird das Einrichten des Gateways mit dem Setup-Assistenten beschrieben.

- Kapitel 6: Konfigurieren des Wireless-G Broadband-Gateways mit SRX200
  In diesem Kapitel wird beschrieben, wie Sie die Einstellungen des Gateways mithilfe des webbasierten Dienstprogramms konfigurieren.

- Anhang A: Fehlerbehebung
  In diesem Anhang werden einige Probleme und Lösungsansätze sowie häufig gestellte Fragen im Zusammenhang mit der Installation und Verwendung des Wireless-G ADSL-Gateways mit SRX200 erörtert.

- Anhang B: Wireless-Sicherheit
  In diesem Anhang werden die Risiken des Wireless-Netzwerkbetriebs sowie einige Lösungen zur Eingrenzung der Risiken erklärt.

- Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters
  In diesem Anhang wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter des Computers ermitteln, um die MAC-Filterung bzw. die Gateway-Funktion zum Kopieren von MAC-Adressen verwenden zu können.

- Anhang D: Aktualisieren der Firmware
  In diesem Anhang finden Sie eine Anleitung zum Aktualisieren der Firmware des Gateways, sollte dies einmal erforderlich sein.

- Anhang E: Glossar
  In diesem Anhang finden Sie ein kurzes Glossar mit häufig verwendeten Begriffen aus dem Bereich Netzwerkbetrieb.

- Anhang F: Spezifikationen
  In diesem Anhang sind die technischen Spezifikationen des Gateways aufgeführt.

- Anhang G: Garantieinformationen
  Dieser Anhang enthält die Garantieinformationen für das Gateway.

- Anhang H: Zulassungsinformationen
  Dieser Anhang enthält die für das Gateway geltenden Zulassungsinformationen.

- Anhang I: Kontaktinformationen
  In diesem Anhang finden Sie Kontaktinformationen zu einer Reihe von Linksys Ressourcen, darunter auch zum Support.

Kapitel 2: Planen des Netzwerks

Funktionen des Gateways

Ein Gateway ist ein Netzwerkgerät, das zwei Netzwerke miteinander verbindet.

In diesem Fall verbindet das Gateway das lokale Netzwerk (LAN) oder die Computer zu Hause oder im Büro mit dem Internet. Das Gateway verarbeitet und lenkt die zwischen diesen beiden Netzwerken übertragenen Daten.

Mit der NAT-Funktion des Gateways wird das Computernetzwerk geschützt, sodass Ihre Computer für andere Benutzer im Internet nicht „sichtbar" sind. Somit wird der private Charakter des Netzwerks bewahrt. Das Gateway schützt das Netzwerk, indem es alle über den Internet-Port eingehenden Datenpakete überprüft, bevor sie an den entsprechenden Computer in Ihrem Netzwerk geliefert werden. Das Gateway überprüft Internet-Anschlussdienste, wie z. B. den Webserver, FTP-Server oder andere Internetanwendungen, und leitet, falls zulässig, das jeweilige Paket an den entsprechenden Computer im LAN weiter.

Beachten Sie, dass über die Ports des Gateways eine Verbindung zwischen zwei Netzwerken hergestellt wird. Mit den LAN-Ports können Sie Verbindungen zum LAN und mit dem Port **ADSL** eine Verbindung zum Internet herstellen. Die LAN-Ports übertragen Daten mit einer Geschwindigkeit von 10/100 Mbit/s.

Abbildung 2-1: Netzwerk

IP-Adressen

Was ist eine IP-Adresse?

IP steht für *Internet Protocol* (Internet-Protokoll). Jedes Gerät in einem IP-basierten Netzwerk, einschließlich Computern, Druckservern und Gateways, benötigt eine IP-Adresse, mit der sein „Standort" bzw. seine Adresse im Netzwerk identifiziert werden kann. Dies gilt sowohl für Internet- als auch für LAN-Verbindungen. Es gibt zwei Möglichkeiten, den Netzwerkgeräten eine IP-Adresse zuzuweisen. Sie können statische IP-Adressen oder mithilfe des Gateways dynamische IP-Adressen zuweisen.

***IP** (Internet Protocol): Ein Protokoll zum Senden von Daten über Netzwerke.*

HINWEIS: Da es sich bei dem Gateway um ein Gerät handelt, mit dem zwei Netzwerke verbunden werden, sind zwei IP-Adressen erforderlich, eine für das LAN und eine für das Internet. In diesem Benutzer-handbuch wird auf „Internet-IP-Adressen" und „LAN-IP-Adressen" verwiesen.

Da bei dem Gateway NAT-Technologie eingesetzt wird, ist die einzige IP-Adresse Ihres Netzwerks, die vom Internet aus sichtbar ist, die Internet-IP-Adresse des Gateways. Es kann jedoch auch diese Internet-IP-Adresse blockiert werden, so dass Gateway und Netzwerk für das Internet unsichtbar sind. Weitere Informationen hierzu finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200" im Abschnitt zur Registerkarte **Security – Firewall** (Sicherheit – Firewall).

Statische IP-Adressen

Bei einer statischen IP-Adresse handelt es sich um eine feste IP-Adresse, die einem Computer oder einem anderen Netzwerkgerät manuell zugewiesen wird. Da eine statische IP-Adresse solange gültig ist, bis Sie sie deaktivieren, wird durch das Zuweisen einer statischen IP-Adresse sichergestellt, dass das entsprechende Gerät stets dieselbe IP-Adresse hat, bis diese geändert wird. Statische IP-Adressen müssen eindeutig sein und werden im Allgemeinen bei Netzwerkgeräten, z. B. Server-Computern oder Druckservern, verwendet.

Da Sie das Gateway für den gemeinsamen Zugriff auf Ihre DSL-Internetverbindung verwenden, fragen Sie Ihren ISP, ob Ihrem Konto eine statische IP-Adresse zugewiesen wurde. Ist dies der Fall, benötigen Sie diese statische IP-Adresse für die Konfiguration des Gateways. Sie erhalten diese Informationen von Ihrem ISP.

Dynamische IP-Adressen

Eine dynamische IP-Adresse wird einem Netzwerkgerät, z. B. einem Computer oder Druckserver, automatisch zugewiesen. Diese IP-Adressen werden als „dynamisch“ bezeichnet, da sie den Netzwerkgeräten nur vorübergehend zugewiesen werden. Nach einem bestimmten Zeitraum laufen Sie ab und können geändert werden. Wenn ein Computer beim Netzwerk (oder im Internet) angemeldet wird und seine dynamische IP-Adresse abgelaufen ist, wird ihm vom DHCP-Server automatisch eine neue dynamische IP-Adresse zugewiesen.

DHCP-Server (*Dynamic Host Configuration Protocol*)

Computern und anderen Netzwerkgeräten mit dynamischen IP-Adressen wird von einem DHCP-Server jeweils eine neue IP-Adresse zugewiesen. Computer bzw. Netzwerkgeräte, die eine IP-Adresse erhalten, werden als DHCP-Clients bezeichnet. Durch DHCP müssen Sie nicht jedes Mal, wenn dem Netzwerk ein neuer Benutzer hinzugefügt wird, manuell eine IP-Adresse zuweisen.

Als DHCP-Server kann entweder ein bestimmter Computer im Netzwerk oder ein anderes Netzwerkgerät (z. B. das Gateway) fungieren. Die DHCP-Serverfunktion des Gateways ist standardmäßig aktiviert.

Wenn im Netzwerk bereits ein DHCP-Server ausgeführt wird, müssen Sie einen der beiden DHCP-Server deaktivieren. Wenn mehrere DHCP-Server in Ihrem Netzwerk ausgeführt werden, treten Netzwerkfehler (z. B. IP-Adresskonflikte) auf. Hinweise zum Deaktivieren von DHCP für das Gateway finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“ im Abschnitt „DHCP“.

Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways mit SRX200

Ports und Taste „Reset“ an der Geräteseite

Die Ports und die Taste **Reset** befinden sich an der Geräteseite des Gateways.

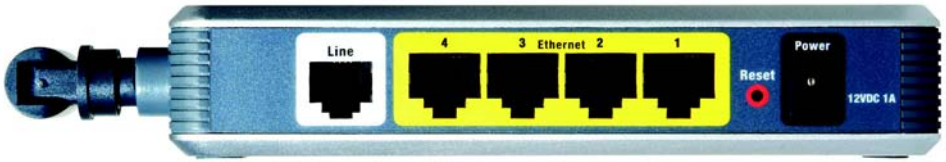


Abbildung 3-1: Ports und Taste „Reset“ an der Geräteseite

Line (Verbindung) Der Port **Line** (Verbindung) dient zum Anschließen an die ADSL-Verbindung.

Ethernet (1-4) Die **Ethernet**-Ports dienen zum Anschließen an die Computer und andere Netzwerkgeräte.

Reset (Taste) Das Gateway kann auf zweierlei Weise auf die Werkseinstellungen zurückgesetzt werden. Halten Sie die Taste **Reset** ungefähr fünf Sekunden lang gedrückt, oder setzen Sie die Einstellungen im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Administration** (Verwaltung) im Fenster *Factory Defaults* (Werkseinstellungen) zurück.

Power (Netzstrom) Der Port **Power** (Netzstrom) dient zum Anschließen des Netzstromadapters.

WICHTIG: Durch das Zurücksetzen des Gateways auf die Werkseinstellungen werden alle Einstellungen gelöscht (einschließlich der Einstellungen für die Internetverbindung, der Wireless-Einstellungen und anderer Einstellungen) und durch die Werkseinstellungen ersetzt. Setzen Sie das Gateway nicht zurück, wenn Sie die Einstellungen beibehalten möchten.

LEDs an der Geräteseite

Die LEDs des Gateways, die Netzwerkaktivität anzeigen, befinden sich an der anderen Geräteseite.

Abbildung 3-2: LEDs an der Geräteseite

Ein/Aus (Taste) Drücken Sie diese Taste, wenn Sie das Gateway ein- oder ausschalten möchten.

POWER (Netzstrom) Grün. Die LED **POWER** (Netzstrom) leuchtet, wenn das Gateway eingeschaltet wird.

WIRELESS Grün. Die LED **WIRELESS** leuchtet bei jeder erfolgreichen Wireless-Verbindung. Wenn die LED blinkt, werden gerade aktiv Daten vom Gateway an eines der Netzwerkgeräte gesendet oder es werden gerade Daten empfangen.

ETHERNET (1-4) Grün. Die LED **ETHERNET** hat zwei Funktionen. Wenn die LED durchgängig leuchtet, ist das Gateway erfolgreich über den entsprechenden Ethernet-Port mit einem Gerät verbunden. Wenn die LED blinkt, finden Netzwerkaktivitäten statt.

DSL Grün. Die LED **DSL** leuchtet bei jeder erfolgreichen DSL-Verbindung. Die LED blinkt, wenn mit dem Gateway eine ADSL-Verbindung hergestellt wurde.

INTERNET Grün. Die LED **INTERNET** leuchtet grün, wenn eine Internetverbindung zum Internet-Dienstanbieter (ISP) hergestellt wurde. Die LED leuchtet rot, wenn bei der Verbindung zum ISP Fehler auftreten.

Kapitel 4: Anschließen des Wireless-G ADSL-Gateways mit SRX200

Übersicht

In der Regel erhalten Sie vom Installationstechniker Ihres Internet-Dienstanbieters (ISP) nach der Installation der Breitbandverbindung Informationen zur Einrichtung des Modems. Wenn diese Daten nicht zur Verfügung stehen, fordern Sie sie von Ihrem ISP an.

Wenn Sie über die für Ihren Internetverbindungstyp erforderlichen Einrichtungsinformationen verfügen, können Sie mit der Installation und Einrichtung des Gateways beginnen.

Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Ethernet-Adapter verwenden möchten, fahren Sie mit Abschnitt „Verdrahtete Verbindung mit einem Computer“ fort. Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Wireless-Adapter verwenden möchten, fahren Sie mit Abschnitt „Wireless-Verbindung mit einem Computer“ fort.

Verdrahtete Verbindung mit einem Computer

1. Stellen Sie sicher, dass alle Hardwaregeräte des Netzwerks (einschließlich des Gateways und der Computer) ausgeschaltet sind.

2. Schließen Sie ein Ende des Telefonkabels an den Port **Line** (Verbindung) an der Geräteseite des Gateways an und das andere Ende an den Splitter der ADSL-Leitung. Um Störungen zu vermeiden, muss u. U. zwischen Telefon und Splitter ein so genannter Mikrofilter (nicht im Lieferumfang enthalten) geschaltet werden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.

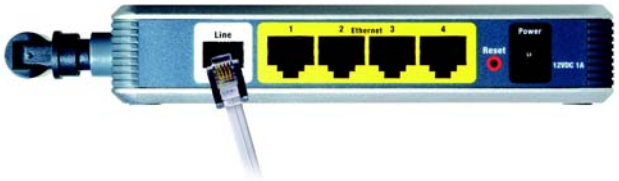


Abbildung 4-1: Herstellen der ADSL-Verbindung

HINWEIS: Um Störungen zu vermeiden, muss u. U. zwischen Telefon und Splitter ein so genannter Mikrofilter (nicht im Lieferumfang enthalten) geschaltet werden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.

WICHTIG: Vergewissern Sie sich in Ländern, in denen Telefonbuchsen mit RJ-11-Steckern verwendet werden, dass Sie die Mikrofilter nur zwischen das Telefon und den Splitter und **nicht** zwischen das Gateway und den Splitter schalten. Andernfalls kann keine ADSL-Verbindung hergestellt werden.

In Ländern, in denen **keine** Telefonbuchsen mit RJ-11-Steckern verwendet werden (z. B. Frankreich, Schweden, Schweiz, Großbritannien), muss der Mikrofilter – mit Ausnahme von ISDN – zwischen das Gateway und die Wandbuchse geschaltet werden, da sich der RJ-11-Stecker am Mikrofilter befindet.

Benutzer von Annex B (Gateway-Versionen E1 und DE) verwenden zum Anschließen des Gateways an den Splitter oder den NTBA das im Lieferumfang enthaltene Netzwerkkabel. Wenn Sie Splitter oder spezielle Stecker benötigen, wenden Sie sich an Ihren Internet-Dienstanbieter.

3. Schließen Sie ein Ende des Ethernet-Netzwerkkabels an einen der Ethernet-Ports (mit 1-4 beschriftet) an der Geräteseite des Gateways und das andere Ende am Ethernet-Port eines Computers an.

   Wiederholen Sie diesen Schritt, um weitere Computer, einen Switch oder andere Netzwerkgeräte an das Gateway anzuschließen.

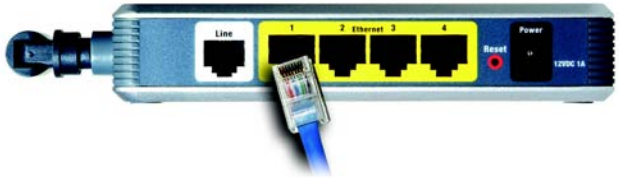


Abbildung 4-2: Anschließen eines PCs

4. Schließen Sie den Netzstromadapter an den Port **Power** (Netzstrom) des Gateways an, und stecken Sie ihn anschließend in eine Steckdose.

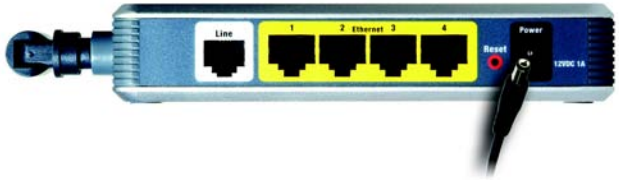


Abbildung 4-3: Anschließen des Netzstroms

HINWEIS: Schließen Sie den Netzstromadapter des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

Wenn der Netzstromadapter ordnungsgemäß angeschlossen ist, leuchtet die LED **Power** (Netzstrom) an der Geräteseite grün. Die LED **Power** (Netzstrom) blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen wurde. Wenn die LED länger als eine Minute blinkt, finden Sie entsprechende Informationen zur Fehlerbehebung in „Anhang A: Fehlerbehebung“.

5. Schalten Sie einen Computer ein, der mit dem Gateway verbunden ist.

Fahren Sie mit „Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200“ fort.

Wireless-Verbindung mit einem Computer

Befolgen Sie die nachstehenden Anweisungen, wenn Sie über eine Wireless-Verbindung auf das Gateway zugreifen möchten:

1. Stellen Sie sicher, dass alle Hardwaregeräte des Netzwerks (einschließlich des Gateways und der Computer) ausgeschaltet sind.

2. Schließen Sie ein Ende des Telefonkabels an den Port **Line** (Verbindung) an der Rückseite des Gateways an und das andere Ende an die Wandbuchse der ADSL-Leitung. Um Störungen zu vermeiden, muss u. U. zwischen Telefon und Splitter ein so genannter Mikrofilter (nicht im Lieferumfang enthalten) geschaltet werden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.

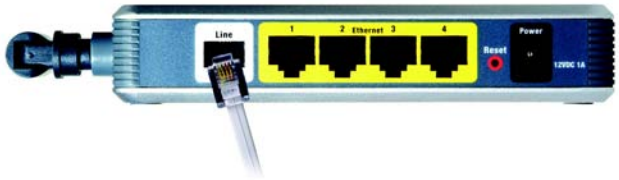


Abbildung 4-4: Herstellen der ADSL-Verbindung

HINWEIS: Um Störungen zu vermeiden, muss u. U. zwischen Telefon und Splitter ein so genannter Mikrofilter (nicht im Lieferumfang enthalten) geschaltet werden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.

WICHTIG: Vergewissern Sie sich in Ländern, in denen Telefonbuchsen mit RJ-11-Steckern verwendet werden, dass Sie die Mikrofilter nur zwischen das Telefon und den Splitter und **nicht** zwischen das Gateway und den Splitter schalten. Andernfalls kann keine ADSL-Verbindung hergestellt werden.

In Ländern, in denen **keine** Telefonbuchsen mit RJ-11-Steckern verwendet werden (z. B. Frankreich, Schweden, Schweiz, Großbritannien), muss der Mikrofilter – mit Ausnahme von ISDN – zwischen das Gateway und die Wandbuchse geschaltet werden, da sich der RJ-11-Stecker am Mikrofilter befindet.

Benutzer von Annex B (Gateway-Versionen E1 und DE) verwenden zum Anschließen des Gateways an den Splitter oder den NTBA das im Lieferumfang enthaltene Netzwerkkabel. Wenn Sie Splitter oder spezielle Stecker benötigen, wenden Sie sich an Ihren Internet-Dienstanbieter.

3. Schließen Sie den Netzstromadapter an den Port **Power** (Netzstrom) an, und stecken Sie ihn anschließend in eine Steckdose.

HINWEIS: Schließen Sie den Netzstromadapter des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

Wenn der Netzstromadapter ordnungsgemäß angeschlossen ist, leuchtet die LED **Power** (Netzstrom) an der Geräteseite grün. Die LED **Power** (Netzstrom) blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen wurde. Wenn die LED länger als eine Minute blinkt, finden Sie entsprechende Informationen zur Fehlerbehebung in „Anhang A: Fehlerbehebung“.

4. Schalten Sie einen der Computer im Wireless-Netzwerk ein.

5. Stellen Sie beim erstmaligen Zugriff auf das Gateway über eine Wireless-Verbindung sicher, dass die SSID des Wireless-Adapters für den Computer auf **linksys** (die Standardeinstellung des Gateways) eingestellt und die Option zur Sicherheit im Wireless-Netzwerkbetrieb deaktiviert ist. Wenn Sie Zugriff auf das Gateway haben, können Sie die Einstellungen des Gateways und des Adapters für den Computer an die üblichen Netzwerkeinstellungen anpassen.

Fahren Sie mit „Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200“ fort.

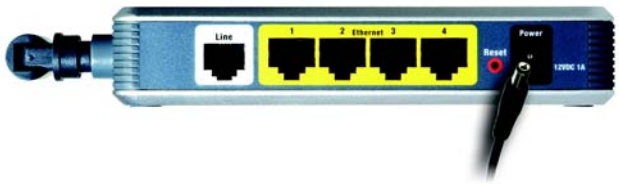


Abbildung 4-5: Anschließen des Netzstroms

HINWEIS: Sie sollten auf jeden Fall die SSID-Standardeinstellung **linksys** ändern und die Option zur Sicherheit im Wireless-Netzwerkbetrieb aktivieren.

Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200

Übersicht

Der Setup-Assistent für das Wireless-G ADSL-Gateway mit SRX200 führt Sie durch den Installationsvorgang. Er zeigt Ihnen Schritt für Schritt auf, wie Sie die Netzwerk- und Wireless-Einstellungen des Gateways konfigurieren.

Verwenden des Setup-Assistenten

1. Legen Sie die **Setup Wizard CD-ROM** (Setup-Assistenten-CD-ROM) in Ihr CD-ROM-Laufwerk ein. Der Setup-Assistent sollte automatisch gestartet und das Willkommensfenster angezeigt werden. Ist dies nicht der Fall, klicken Sie auf die Schaltfläche **Start**, und wählen Sie **Ausführen** aus. Geben Sie im daraufhin angezeigten Feld **D:\setup.exe** ein (wobei „D“ für den Buchstaben des CD-ROM-Laufwerks steht).

2. Die Spracheinstellung des Computers wird vom Setup-Assistenten automatisch erkannt. Ist dies nicht der Fall, wählen Sie eine der verfügbaren Sprachen im Dropdown-Menü *Language* (Sprache) aus. Klicken Sie im ersten Willkommensfenster auf die Schaltfläche **Next** (Weiter), wenn Sie den Setup-Assistenten in der aktuellen Sprache ausführen möchten. Wenn Sie eine andere Sprache verwenden möchten, wählen Sie die entsprechende Sprache aus, und klicken Sie dann auf die Schaltfläche **Next** (Weiter).

3. Klicken Sie im nächsten Willkommensfenster auf die Schaltfläche **Click Here to Start** (Klicken Sie hier, um zu starten). Darüber hinaus stehen Ihnen folgende Wahlmöglichkeiten zur Verfügung:

   Norton Internet Security: Klicken Sie auf die Schaltfläche **Norton Internet Security**, um das Softwareprogramm Norton Internet Security zu installieren.

   User Guide (Benutzerhandbuch): Klicken Sie auf diese Schaltfläche, um das Benutzerhandbuch als PDF-Datei zu öffnen.

   Exit (Beenden): Klicken Sie auf diese Schaltfläche, um den Setup-Assistenten zu beenden.

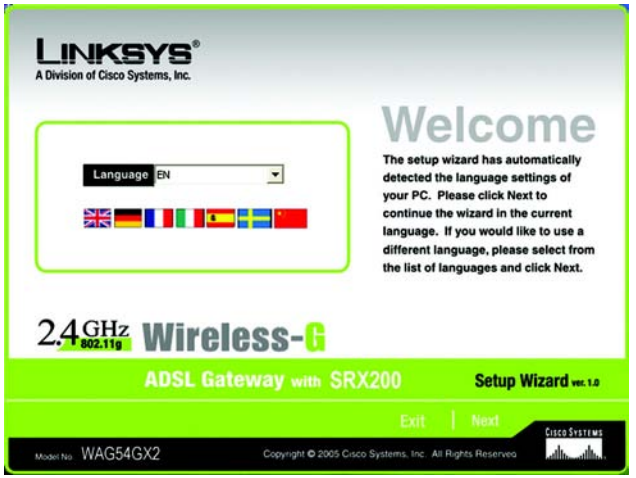


Abbildung 5-1: Setup-Assistent – Willkommensfenster – Sprachauswahl

Abbildung 5-2: Setup-Assistent – Willkommensfenster – Fenster zum Starten des Assistenten

4. Klicken Sie nach dem Lesen der Lizenzvereinbarung auf die Schaltfläche **Next** (Weiter), wenn Sie diese akzeptieren, oder auf die Schaltfläche **Exit** (Beenden), um den Installationsvorgang zu beenden. Klicken Sie auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

Abbildung 5-3: Setup-Assistent – Fenster *License Agreement* (Lizenzvereinbarung)

5. Der Setup-Assistent fordert Sie auf, das Breitband-Modem vom Computer und vom ADSL-Splitter zu trennen. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

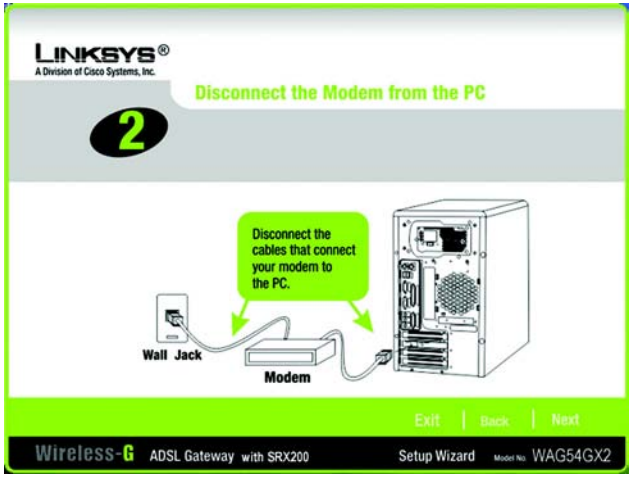


Abbildung 5-4: Setup-Assistent – Fenster *Disconnect the Modem from the PC and ADSL Wall Jack* (Trennen des Modems vom PC und vom ADSL-Splitter)

6. Der Setup-Assistent fordert Sie auf, das Gateway an den ADSL-Splitter anzuschließen. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

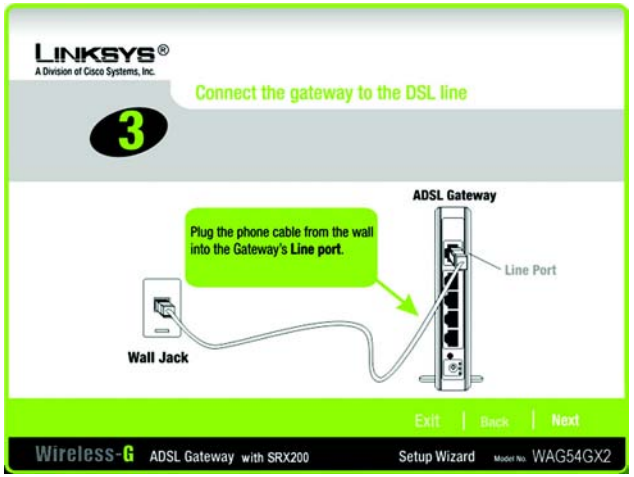


Abbildung 5-5: Setup-Assistent – Fenster *Connect the Gateway to the ADSL Wall Jack* (Anschließen des Gateways an den ADSL-Splitter)

7. Der Setup-Assistent fordert Sie auf, ein Netzwerkkabel an den Computer anzuschließen. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

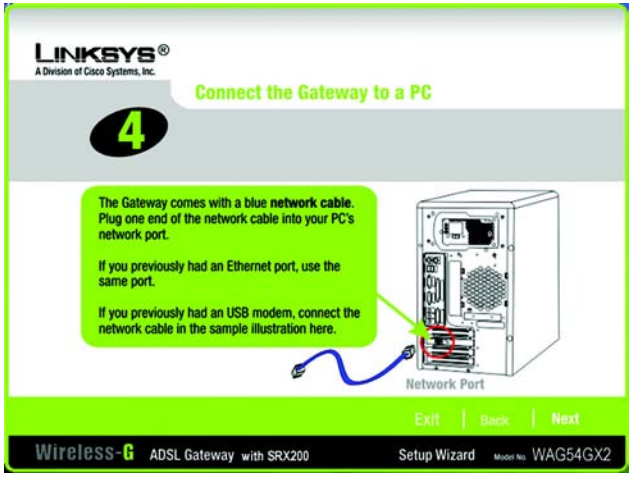


Abbildung 5-6: Setup-Assistent – Fenster *Connect a Network Cable to a PC* (Anschließen des Netzwerkkabels an einen PC)

8. Der Setup-Assistent fordert Sie auf, das andere Ende des Netzwerkkabels an das Gateway anzuschließen.

   Sie können dann weitere Computer an das Gateway anschließen.

   Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

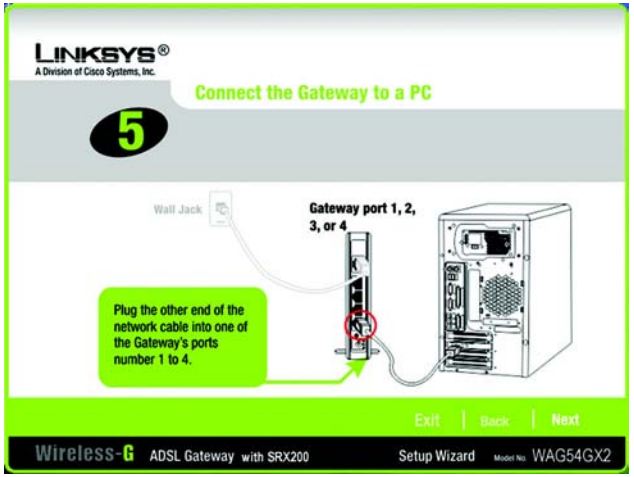


Abbildung 5-7: Setup-Assistent – Fenster *Connect the Network Cable to the Gateway* (Anschließen des Netzwerkkabels an das Gateway)

9. Der Setup-Assistent fordert Sie auf, das Gateway einzuschalten. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

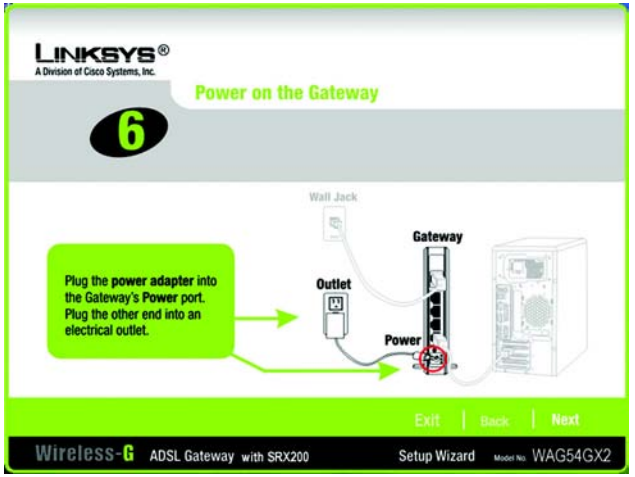


Abbildung 5-8: Setup-Assistent – Fenster *Power on the Gateway* (Einschalten des Gateways)

10. Vergewissern Sie sich, dass die LEDs für Netzstrom und DSL sowie die nummerierten LEDs (entsprechend der Anzahl der angeschlossenen Computer) an der Vorderseite des Gateways leuchten. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

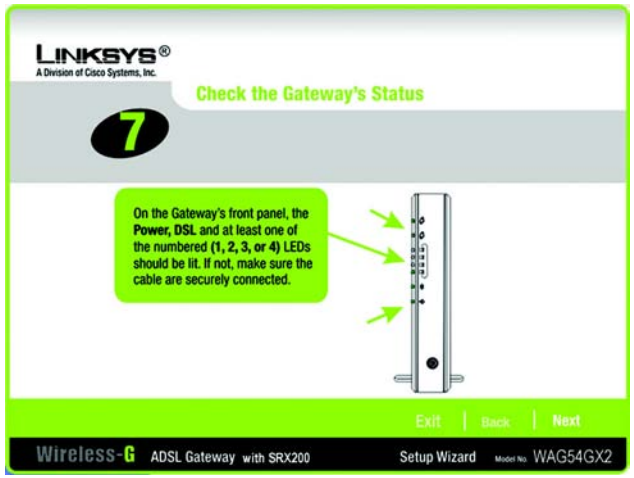


Abbildung 5-9: Setup-Assistent – Fenster *Check the Gateway's Status* (Überprüfen des Gateway-Status)

11. Sie werden nach Ihrem Wohnort gefragt. Wählen Sie im Dropdown-Menü das entsprechende Land aus. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

HINWEIS: Wenn Ihr Land nicht aufgeführt ist, verwenden Sie zum Konfigurieren der Einstellungen das webbasierte Dienstprogramm des Gateways. Entsprechende Anweisungen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.

Abbildung 5-10: Setup-Assistent – Fenster *Select Your Country* (Auswahl des Landes)

12. Die Internet-Dienstanbieter (*Internet Service Provider*, ISP) für das ausgewählte Land werden angezeigt. (Je nach dem im vorherigen Fenster ausgewählten Land werden andere Optionen angezeigt.) Klicken Sie auf die Schaltfläche für Ihren ISP.

    Wenn Ihr ISP nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Next** (Weiter), um die Einstellungen manuell einzugeben.

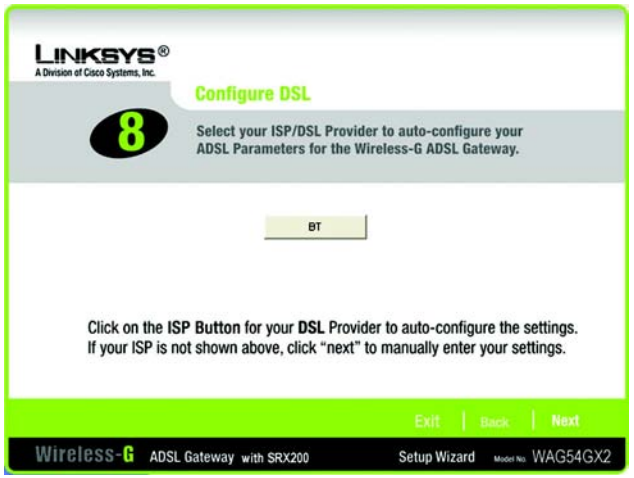


Abbildung 5-11: Setup-Assistent – Fenster *Select Your Internet Service Provider (UK)* (Auswahl des Internet-Dienstanbieters in Großbritannien)

13. Gegebenenfalls erkennt der Setup-Assistent automatisch die verwendete Kapselungsmethode: **1483 Bridged** (1483-Überbrückung), **1483 Routed** (1483-Weiterleitung), **PPPoA** oder **PPPoE**. Wenn Sie die Einstellungen manuell eingeben, wählen Sie zuerst die Kapselungsmethode aus: **1483 Bridged** (1483-Überbrückung), **1483 Routed** (1483-Weiterleitung), **PPPoA** oder **PPPoE**.

    HINWEIS: Wenn als Kapselungsmethode **IPoA** oder **Bridge Mode Only** (Nur Überbrückungsmodus) eingesetzt wird, müssen Sie zum Konfigurieren des Gateways das zugehörige webbasierte Dienstprogramm verwenden. Entsprechende Anweisungen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.

    Fahren Sie dann mit dem entsprechenden Abschnitt für die ausgewählte Kapselungsmethode fort.

1483 Bridged (1483-Überbrückung)

Nach der Auswahl eines Internet-Dienstanbieters werden die Einstellungen für Kapselung, VPI, VCI und Multiplexing im Setup-Assistenten automatisch vorgenommen. Wählen Sie dann die entsprechende IP-Einstellung für die DSL-Verbindung aus.

In diesem Fenster können Sie die Einstellungen manuell vornehmen.

VPI/VCI: Wenn Sie die Einstellungen manuell eingeben müssen, tragen Sie hier die von Ihrem Internet-Dienstanbieter zur Verfügung gestellten Werte für VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) ein.

Multiplexing: Wenn Sie die Einstellungen manuell eingeben müssen, wählen Sie je nach ISP **LLC** oder **VC** aus.

Auto IP (Automatische IP-Adresse): Klicken Sie bei Verwendung einer dynamischen IP-Adresse auf das Optionsfeld **Auto IP** (Automatische IP-Adresse).

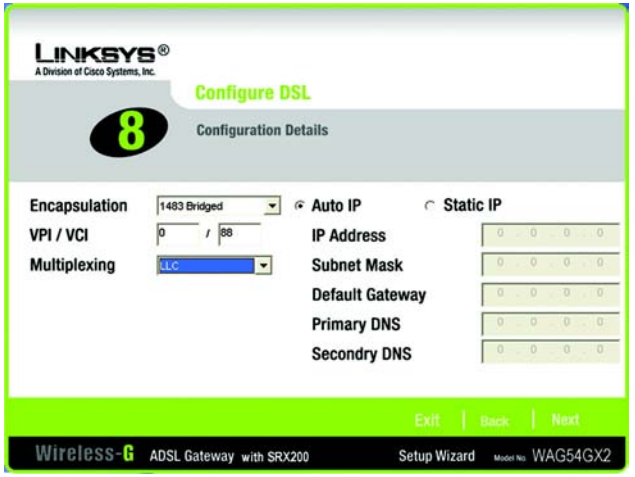


Abbildung 5-12: Setup-Assistent – Fenster *Configure DSL* (Konfigurieren von DSL) – „1483 Bridged“ (1483-Überbrückung)

Static IP (Statische IP-Adresse): Klicken Sie bei Verwendung einer statischen IP-Adresse auf das Optionsfeld **Static IP** (Statische IP-Adresse). Geben Sie geeignete Werte in den Feldern *IP Address* (IP-Adresse), *Subnet Mask* (Subnetzmaske), *Default Gateway* (Standard-Gateway), *Primary DNS* (Primärer DNS) und *Secondary DNS* (Sekundärer DNS) ein. (Sie müssen mindestens die IP-Adresse eines DNS-Servers eingeben.)

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

1483 Routed (1483-Weiterleitung)

Nach der Auswahl eines Internet-Dienstanbieters werden die Einstellungen für Kapselung, VPI, VCI und Multiplexing im Setup-Assistenten automatisch vorgenommen. Wählen Sie dann die entsprechenden IP-Einstellungen für die DSL-Verbindung aus.

In diesem Fenster können Sie die Einstellungen manuell vornehmen.

VPI/VCI: Wenn Sie die Einstellungen manuell eingeben müssen, tragen Sie hier die von Ihrem Internet-Dienstanbieter zur Verfügung gestellten Werte für VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) ein.

Multiplexing: Wenn Sie die Einstellungen manuell eingeben müssen, wählen Sie je nach ISP **LLC** oder **VC** aus.

Static IP (Statische IP-Adresse): Geben Sie geeignete Werte in den Feldern *IP Address* (IP-Adresse), *Subnet Mask* (Subnetzmaske), *Default Gateway* (Standard-Gateway), *Primary DNS* (Primärer DNS) und *Secondary DNS* (Sekundärer DNS) ein. (Sie müssen mindestens die IP-Adresse eines DNS-Servers eingeben.)

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

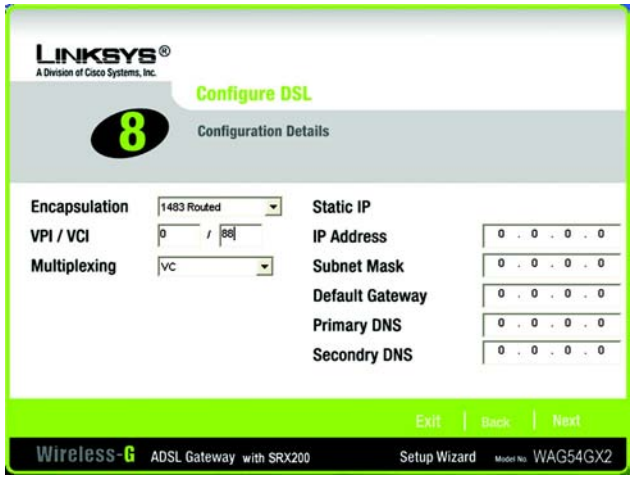


Abbildung 5-13: Setup-Assistent – Fenster *Configure DSL* (Konfigurieren von DSL) – „1483 Routed“ (1483-Weiterleitung)

PPPoA

Nach der Auswahl eines Internet-Dienstanbieters werden die Einstellungen für Kapselung, VPI, VCI und Multiplexing im Setup-Assistenten automatisch vorgenommen. Geben Sie dann die Benutzer-ID und das Passwort für die DSL-Verbindung ein.

In diesem Fenster können Sie die Einstellungen manuell vornehmen.

VPI/VCI: Wenn Sie die Einstellungen manuell eingeben müssen, tragen Sie hier die von Ihrem Internet-Dienstanbieter zur Verfügung gestellten Werte für VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) ein.

Multiplexing: Wenn Sie die Einstellungen manuell eingeben müssen, wählen Sie je nach ISP **LLC** oder **VC** aus.

User ID (Benutzer-ID) und **Password** (Passwort): Geben Sie die Werte für Benutzer-ID und Passwort ein, die Sie von Ihrem ISP erhalten haben.

Connection (Verbindung): Wählen Sie für eine ständige Verbindung zu Ihrem ISP die Option **Keep Alive** (Verbindung aufrecht halten), oder wählen Sie **Connect on Demand** (Bei Bedarf verbinden), falls die Verbindungszeit mit Ihrem ISP gebührenpflichtig ist.

Keep Alive (Verbindung aufrechterhalten): Bei dieser Option behält der Gateway die Internetverbindung bei. Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Die Standardeinstellung beträgt **5** Minuten.

Connect on Demand (Bei Bedarf verbinden): Wenn Sie diese Option auswählen, trennt das Gateway die Internetverbindung, nachdem alle Online-Anwendungen in einem angegebenen Zeitraum beendet sind. Dieser Zeitraum wird im Feld *Max Idle Time* (Max. Leerlaufzeit) festgelegt; die Standardeinstellung beträgt **30** Sekunden.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

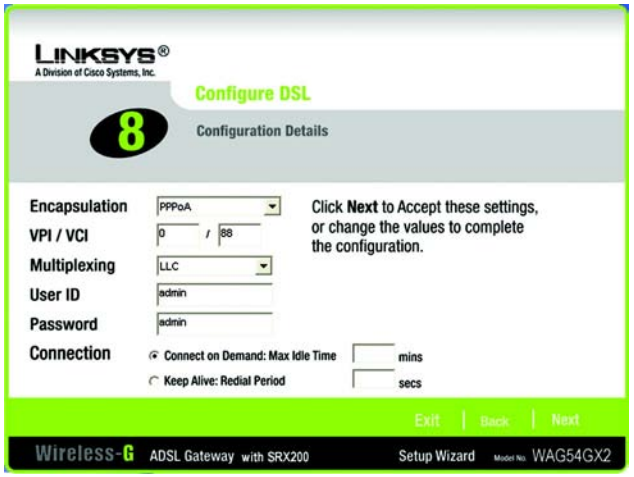


Abbildung 5-14: Setup-Assistent – Fenster *Configure DSL* (Konfigurieren von DSL) – „PPPoA“

PPPoE

Nach der Auswahl eines Internet-Dienstanbieters werden die Einstellungen für Kapselung, VPI, VCI und Multiplexing im Setup-Assistenten automatisch vorgenommen. Geben Sie dann die Benutzer-ID und das Passwort für die DSL-Verbindung ein.

In diesem Fenster können Sie die Einstellungen manuell vornehmen.

VPI/VCI: Wenn Sie die Einstellungen manuell eingeben müssen, tragen Sie hier die von Ihrem Internet-Dienstanbieter zur Verfügung gestellten Werte für VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) ein.

Multiplexing: Wenn Sie die Einstellungen manuell eingeben müssen, wählen Sie je nach ISP **LLC** oder **VC** aus.

User ID (Benutzer-ID) und **Password** (Passwort): Geben Sie die Werte für Benutzer-ID und Passwort ein, die Sie von Ihrem ISP erhalten haben.

Connection (Verbindung): Wählen Sie für eine ständige Verbindung zu Ihrem ISP die Option **Keep Alive** (Verbindung aufrecht halten), oder wählen Sie **Connect on Demand** (Bei Bedarf verbinden), falls die Verbindungszeit mit Ihrem ISP gebührenpflichtig ist.

Keep Alive (Verbindung aufrechterhalten): Bei dieser Option behält der Gateway die Internetverbindung bei. Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Die Standardeinstellung beträgt **5** Minuten.

Connect on Demand (Bei Bedarf verbinden): Wenn Sie diese Option auswählen, trennt das Gateway die Internetverbindung, nachdem alle Online-Anwendungen in einem angegebenen Zeitraum beendet sind. Dieser Zeitraum wird im Feld *Max Idle Time* (Max. Leerlaufzeit) festgelegt; die Standardeinstellung beträgt **30** Sekunden.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

14. Für das Gateway steht ein webbasiertes Dienstprogramm zur Verfügung, mit dem Sie das Gateway über jeden Netzwerkcomputer konfigurieren können. Der Zugriff auf das Dienstprogramm ist passwortgeschützt.

    Password (Passwort): Das Standardpasswort lautet **admin**. Ändern Sie es in ein Passwort Ihrer Wahl.

    Confirm (Bestätigen): Geben Sie im Feld *Confirm* (Bestätigen) das Passwort erneut ein.

    Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

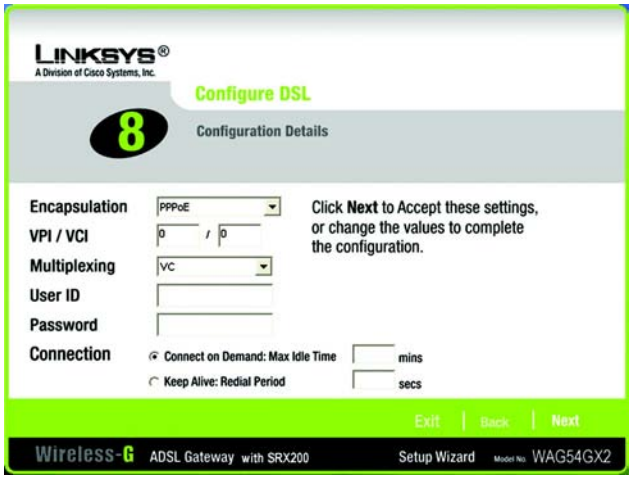


Abbildung 5-15: Setup-Assistent – Fenster *Configure DSL* (Konfigurieren von DSL) – „PPPoE“

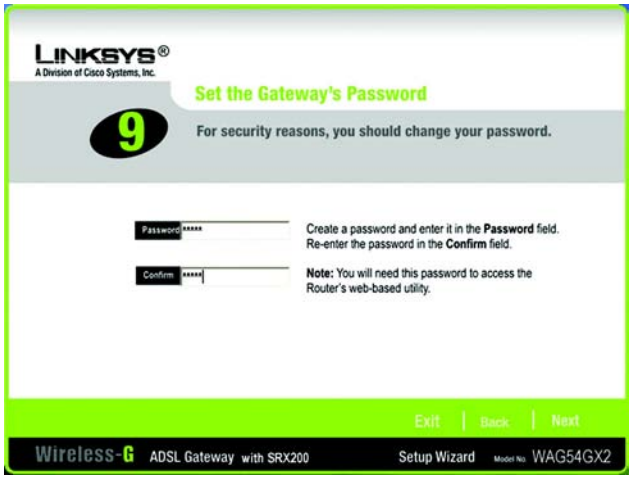


Abbildung 5-16: Setup-Assistent – Fenster *Set the Gateway's Password* (Einrichten des Gateway-Passworts)

15. Der Setup-Assistent fordert Sie auf, die Einstellungen für das Wireless-Netzwerk einzugeben.

SSID: Geben Sie im Feld *SSID* den Namen des Wireless-Netzwerks ein. Die SSID muss für alle Geräte im Netzwerk identisch sein. Die Standardeinstellung ist **linksys** (Kleinbuchstaben).

HINWEIS: Bei der SSID handelt es sich um den Netzwerknamen, der von allen Geräten in einem Wireless-Netzwerk gemeinsam verwendet wird. Die SSID Ihres Netzwerks muss eindeutig und für alle Geräte im Netzwerk identisch sein.

Channel (Kanal): Wählen Sie den Betriebskanal für Ihr Wireless-Netzwerk aus. Über diesen Kanal kommunizieren alle Wireless-Geräte.

Network Mode (Netzwerkmodus): Wählen Sie im Dropdown-Menü *Network Mode* (Netzwerkmodus) die Wireless-Standards aus, die im Netzwerk verwendet werden. Wenn sich sowohl 802.11g- als auch 802.11b-Geräte in Ihrem Netzwerk befinden, behalten Sie die Standardeinstellung **Mixed** (Gemischt) bei. Wenn ausschließlich 802.11g-Geräte vorhanden sind, wählen Sie **G-Only** (Nur G) aus. Wenn ausschließlich 802.11b-Geräte vorhanden sind, wählen Sie **B-Only** (Nur B) aus. Wenn Sie das Wireless-Netzwerk deaktivieren möchten, wählen Sie **Disable** (Deaktivieren) aus.

Device Name (Gerätename): Geben Sie im Feld *Device Name* (Gerätename) einen Namen für das Gateway ein.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

16. Wählen Sie die zu verwendende Sicherheitsmethode aus: **WPA Personal**, **WPA2 Personal**, **WPA2 Mixed Mode** (WPA2 Gemischter Modus), **WEP (64-Bit)** oder **WEP (128-Bit)**. WPA ist die Abkürzung für *Wi-Fi Protected Access*, WEP für *Wired Equivalent Privacy*. WPA bietet eine höhere Sicherheit als WEP. Bei WPA2 handelt es sich um eine WPA-Version mit stärkerer Verschlüsselung. Fahren Sie mit den entsprechenden Anweisungen für die gewünschte Sicherheitsmethode fort.

Wenn Sie keine Wireless-Sicherheitsmethode verwenden möchten, klicken Sie auf **Disabled** (Deaktiviert) und dann auf die Schaltfläche **Next** (Weiter). Fahren Sie mit Schritt 17 fort.

HINWEIS: Wenn Sie die Sicherheitsmethode WPA Enterprise oder WPA2 Enterprise verwenden möchten, klicken Sie auf **Disabled** (Deaktiviert) und dann auf die Schaltfläche **Next** (Weiter). Sobald Sie den Setup-Assistenten beendet haben, konfigurieren Sie die Wireless-Sicherheitseinstellungen mit dem webbasierten Dienstprogramm des Gateways. Entsprechende Anweisungen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.

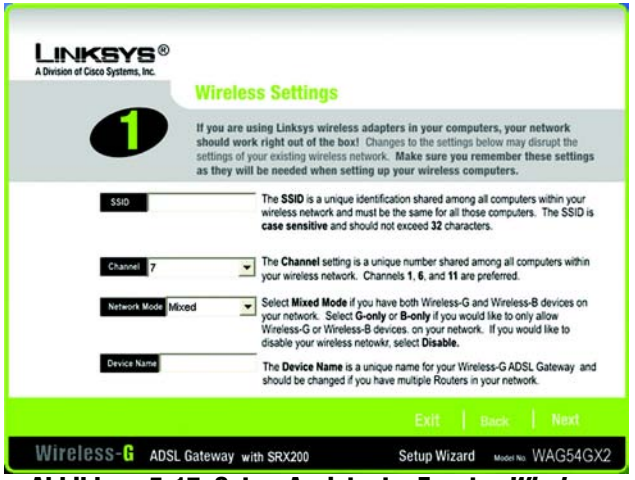


Abbildung 5-17: Setup-Assistent – Fenster *Wireless Settings* (Wireless-Einstellungen)

***WPA** (Wi-Fi Protected Access): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (Temporal Key Integrity Protocol) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann.*

***WEP** (Wired Equivalent Privacy): Eine hochgradig sichere Methode zum Verschlüsseln von Netzwerkdaten, die in einem Wireless-Netzwerk übertragen werden.*

Abbildung 5-18: Setup-Assistent – Fenster *Configure Wireless Security Settings* (Konfigurieren der Wireless-Sicherheitseinstellungen)

WPA Personal

Encryption (Verschlüsselung): Wählen Sie den gewünschten Algorithmus aus (**TKIP** oder **AES**).

Passphrase: Geben Sie eine Passphrase (auch als vorläufiger gemeinsamer Schlüssel bezeichnet) mit einer Länge von 8 bis 63 Zeichen ein. Je länger und komplexer Ihre Passphrase ist, desto sicherer ist Ihr Netzwerk.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

***Verschlüsselung**: Die Codierung von Daten, die über ein Netzwerk übertragen werden.*

Abbildung 5-19: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WPA Personal“

WPA2 Personal

Encryption (Verschlüsselung): Für den Modus **WPA2 Personal** wird automatisch die Option **AES** ausgewählt.

Passphrase: Geben Sie eine Passphrase (auch als vorläufiger gemeinsamer Schlüssel bezeichnet) mit einer Länge von 8 bis 63 Zeichen ein. Je länger und komplexer Ihre Passphrase ist, desto sicherer ist Ihr Netzwerk.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

Abbildung 5-20: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WPA2 Personal“

WPA2 Mixed Mode (WPA2 Gemischter Modus)

Encryption (Verschlüsselung): Es wird automatisch **TKIP + AES** ausgewählt, so dass beide Methoden verwendet werden können.

Passphrase: Geben Sie eine Passphrase (auch als vorläufiger gemeinsamer Schlüssel bezeichnet) mit einer Länge von 8 bis 63 Zeichen ein. Je länger und komplexer Ihre Passphrase ist, desto sicherer ist Ihr Netzwerk.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

Abbildung 5-21: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WPA2 Mixed Mode“ (WPA2 Gemischter Modus)

WEP (64-Bit)

Geben Sie eine Passphrase oder einen WEP-Schlüssel ein.

Passphrase: Geben Sie eine Passphrase in das Feld *Passphrase* ein, sodass automatisch ein WEP-Schlüssel generiert wird. Bei der Passphrase wird zwischen Groß- und Kleinschreibung unterschieden. Die Länge von 16 alphanumerischen Zeichen darf nicht überschritten werden. Sie muss mit den Passphrasen Ihrer anderen Wireless-Netzwerkgeräte übereinstimmen und ist nur mit Wireless-Produkten von Linksys kompatibel. (Wenn Sie Wireless-Produkte anderer Anbieter verwenden, geben Sie den WEP-Schlüssel bei den entsprechenden Produkten manuell ein.)

Key 1 (Schlüssel 1): Der eingegebene WEP-Schlüssel muss mit dem WEP-Schlüssel des Wireless-Netzwerks übereinstimmen. Geben Sie für die 64-Bit-Verschlüsselung genau 10 hexadezimale Zeichen ein. Gültige hexadezimale Zeichen sind Zeichen von „0“ bis „9“ und von „A“ bis „F“.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

Abbildung 5-22: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WEP (64-Bit)“

WEP (128-Bit)

Geben Sie eine Passphrase oder einen WEP-Schlüssel ein.

Passphrase: Geben Sie eine Passphrase in das Feld *Passphrase* ein, sodass automatisch ein WEP-Schlüssel generiert wird. Bei der Passphrase wird zwischen Groß- und Kleinschreibung unterschieden. Die Länge von 16 alphanumerischen Zeichen darf nicht überschritten werden. Sie muss mit den Passphrasen Ihrer anderen Wireless-Netzwerkgeräte übereinstimmen und ist nur mit Wireless-Produkten von Linksys kompatibel. (Wenn Sie Wireless-Produkte anderer Anbieter verwenden, geben Sie den WEP-Schlüssel bei den entsprechenden Produkten manuell ein.)

Key 1 (Schlüssel 1): Der eingegebene WEP-Schlüssel muss mit dem WEP-Schlüssel des Wireless-Netzwerks übereinstimmen. Geben Sie für die 128-Bit-Verschlüsselung genau 26 hexadezimale Zeichen ein. Gültige hexadezimale Zeichen sind Zeichen von „0“ bis „9“ und von „A“ bis „F“.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

Abbildung 5-23: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WEP (128-Bit)“

17. Der Setup-Assistent fordert Sie auf, die Einstellungen vor dem Speichern zu überprüfen. Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie auf die Schaltfläche **Yes** (Ja). Klicken Sie auf die Schaltfläche **No** (Nein), falls Sie die neuen Einstellungen nicht speichern möchten.

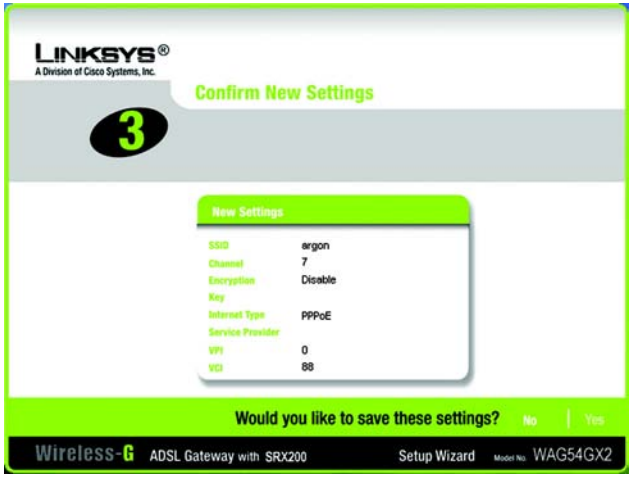


Abbildung 5-24: Setup-Assistent – Fenster *Confirm New Settings* (Bestätigen der neuen Einstellungen)

18. Nach dem Speichern der Einstellungen wird das Fenster *Safe Surfing* (Sicheres Surfen) angezeigt. Klicken Sie auf die Schaltfläche **Norton Internet Security Suite**, um Norton Internet Security Special Edition auf dem Computer zu installieren, oder auf die Schaltfläche **Finish** (Fertig stellen), um den Setup-Assistenten zu beenden.

Abbildung 5-25: Setup-Assistent – Fenster *Safe Surfing* (Sicheres Surfen)

19. Das Fenster *Congratulations* (Herzlichen Glückwunsch) wird angezeigt. Klicken Sie auf die Schaltfläche **Online Registration** (Online-Registrierung), um das Gateway zu registrieren, oder auf die Schaltfläche **Exit** (Beenden), um den Setup-Assistenten zu beenden.

Herzlichen Glückwunsch! Die Installation des Wireless-G ADSL-Gateways mit SRX200 ist hiermit abgeschlossen.

Wenn Sie komplexere Änderungen an der Konfiguration vornehmen möchten, fahren Sie mit „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“ fort.

Abbildung 5-26: Setup-Assistent – Fenster *Congratulations* (Herzlichen Glückwunsch)

Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200

Übersicht

Konfigurieren Sie das Gateway anhand der Anweisungen in diesem Kapitel und mithilfe des webbasierten Dienstprogramms des Gateways. In diesem Kapitel werden alle Webseiten des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können das Dienstprogramm über einen an das Gateway angeschlossenen Computer mit dem Webbrowser aufrufen. Bei der grundlegenden Netzwerkeinrichtung verwenden die meisten Benutzer die folgenden Fenster des Dienstprogramms:

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie im Fenster **Basic Setup** (Grundlegende Einrichtung) die von Ihrem Internet-Dienstanbieter bereitgestellten Einstellungen ein.
- **Management** (Verwaltungsfunktionen): Klicken Sie auf die Registerkarte **Administration** (Verwaltung) und anschließend auf die Registerkarte **Management** (Verwaltungsfunktionen). Der Standardbenutzername und das Standardpasswort des Gateways lauten **admin**. Ändern Sie zum Schutz des Gateways den Standardbenutzernamen und das Passwort.

Es stehen sieben Hauptregisterkarten zur Verfügung: **Setup** (Einrichtung), **Wireless**, **Security** (Sicherheit), **Access Restrictions** (Zugriffsbeschränkungen), **Applications & Gaming** (Anwendungen & Spiele), **Administration** (Verwaltung) und **Status**. Wenn Sie auf eine der Hauptregisterkarten klicken, sind jeweils zusätzliche Registerkarten verfügbar. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Einrichtung

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie in diesem Fenster die Internetverbindung und die Netzwerkeinstellungen ein.
- **DDNS**: Füllen Sie die Felder dieses Fensters aus, um die Funktion **DDNS** (*Dynamic Domain Name System*) des Gateways zu aktivieren.
- **Advanced Routing** (Erweitertes Routing): In diesem Fenster können Sie die Konfigurationseinstellungen für NAT und Routing ändern.

HABEN SIE: TCP/IP auf den Computern aktiviert? Computer tauschen mit diesem Protokoll über das Netzwerk Daten aus. Weitere Informationen zu TCP/IP erhalten Sie in der Windows-Hilfe.

HINWEIS: Zur zusätzlichen Sicherheit sollten Sie den Benutzernamen und das Passwort auf der Registerkarte **Administration** (Verwaltung) ändern.

Wireless

- **Basic Wireless Settings** (Grundlegende Wireless-Einstellungen): In diesem Fenster können Sie die Wireless-Netzwerkeinstellungen auswählen.
- **Wireless Security** (Wireless-Sicherheit): Konfigurieren Sie in diesem Fenster die Wireless-Sicherheitseinstellungen.
- **Wireless Access** (Wireless-Zugriff): In diesem Fenster können Sie den Zugriff auf das Wireless-Netzwerk steuern.
- **Advanced Wireless Settings** (Erweiterte Wireless-Einstellungen): Über dieses Fenster können Sie auf die erweiterten Wireless-Netzwerkeinstellungen zugreifen.

Sicherheit

- **Firewall**: In diesem Fenster können Sie die Firewall aktivieren bzw. deaktivieren, Filter einrichten und anonyme Internet-Anfragen blockieren.
- **VPN Passthrough** (VPN-Passthrough): In diesem Fenster können Sie VPN-Passthrough (*Virtual Private Network*) aktivieren oder deaktivieren.
- **VPN**: In diesem Fenster können Sie bis zu fünf VPN-Tunnel konfigurieren.

***VPN** (Virtual Private Network): Eine Sicherheitsmaßnahme, mit der Daten geschützt werden, wenn sie über das Internet von einem Netzwerk in ein anderes übertragen werden.*

„Access Restrictions“ (Zugriffsbeschränkungen)

- **Internet Access Policy** (Richtlinien für Internetzugriff): In diesem Fenster können Sie die Internetverwendung und den Datenverkehr im lokalen Netzwerk steuern.

„Applications & Gaming“ (Anwendungen & Spiele)

- **Single Port Range Forwarding** (Einfache Anschlussweiterleitung): In diesem Fenster können Sie gängige Dienste oder Anwendungen einrichten, für die das Weiterleiten eines einzelnen Ports erforderlich ist.
- **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich): In diesem Fenster können Sie öffentliche Dienste oder andere spezielle Internetanwendungen einrichten, für die das Weiterleiten eines Anschlussbereichs erforderlich ist.
- **Port Range Triggering** (Anschlussbereich-Triggering): Klicken Sie auf diese Registerkarte, um die Bereiche für Port-Triggering und Port-Forwarding für Internetanwendungen festzulegen.

- **DMZ**: Richten Sie in diesem Fenster die Internetverbindung für einen lokalen Computer so ein, dass spezielle Dienste verwendet werden können.
- **QoS**: Ordnen Sie mit QoS (*Quality of Service*) unterschiedliche Arten der Datenübertragung verschiedenen Prioritätsstufen zu.

„Administration“ (Verwaltungsfunktionen)

- **Management** (Verwaltungsfunktionen): In diesem Fenster können Sie den Gateway-Zugriff sowie die Einstellungen für SNMP (*Simple Network Management Protocol*), UPnP (*Universal Plug and Play*), die Wireless-Verwaltung und die IGMP-Proxy-Einstellungen ändern.
- **Reporting** (Berichtaufzeichnung): Klicken Sie auf diese Registerkarte, um Aktivitätsprotokolle anzuzeigen oder zu speichern.
- **Diagnostics** (Diagnose): In diesem Fenster können Sie Ping-Tests ausführen.
- **Backup & Restore** (Sichern & Wiederherstellen): In diesem Fenster können Sie die Konfiguration des Gateways sichern und wiederherstellen.
- **Factory Defaults** (Werkseinstellungen): In diesem Fenster können Sie die Werkseinstellungen des Gateways wiederherstellen.
- **Firmware Upgrade** (Aktualisieren der Firmware): Klicken Sie auf diese Registerkarte, um die Gateway-Firmware zu aktualisieren.

Status

- **Gateway**: In diesem Fenster sind die Statusinformationen des Gateways aufgeführt.
- **Local Network** (Lokales Netzwerk): In diesem Fenster sind die Statusinformationen des lokalen Netzwerks aufgeführt.
- **Wireless** (Wireless-Netzwerk): In diesem Fenster sind die Statusinformationen des Wireless-Netzwerks aufgeführt.
- **DSL Connection** (DSL-Verbindung): In diesem Fenster sind die Statusinformationen der DSL-Verbindung aufgeführt.

Hinweis für den Zugriff auf das webbasierte Dienstprogramm

Wenn Sie auf das webbasierte Dienstprogramm zugreifen möchten, starten Sie Internet Explorer oder Netscape Navigator, und geben Sie im Feld *Adresse* die Standard-IP-Adresse des Gateways (**192.168.1.1**) ein. Drücken Sie anschließend die Eingabetaste.

Daraufhin wird ein Anmeldefenster angezeigt. (Unter Windows XP wird ein ähnliches Fenster angezeigt.) Geben Sie **admin** (Standardbenutzername) im Feld *Benutzername* und **admin** (Standardkennwort) im Feld *Kennwort* ein. Klicken Sie anschließend auf die Schaltfläche **OK**.

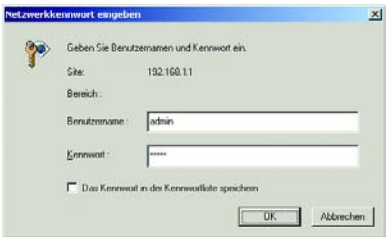


Abbildung 6-1: Anmeldefenster

Registerkarte „Setup“ (Einrichtung)

Registerkarte „Basic Setup“ (Grundlegende Einrichtung)

Im ersten geöffneten Fenster wird die Registerkarte **Basic Setup** (Grundlegende Einrichtung) angezeigt. Auf dieser Registerkarte können Sie die allgemeinen Einstellungen des Gateways ändern. Ändern Sie die Einstellungen entsprechend den folgenden Erläuterungen, und klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen zu verwerfen. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

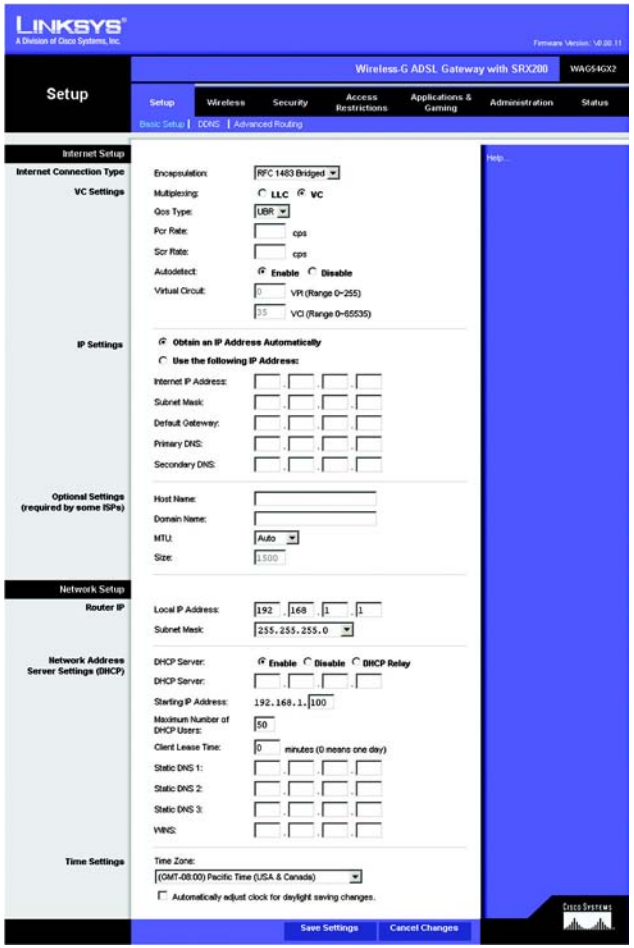


Abbildung 6-2: „Basic Setup“ (Grundlegende Einrichtung)

„Internet Setup“ (Internet-Einrichtung)

- **Internet Connection Type** (Internet-Verbindungstyp): Das Gateway unterstützt sechs Kapselungstypen: **RFC 1483 Bridged** (RFC 1483-Überbrückung), **RFC 1483 Routed** (RFC 1483-Weiterleitung), **IPoA**, **RFC 2516 PPPoE**, **RFC 2364 PPPoA** und **Bridge Mode Only** (Nur Überbrückungsmodus). Wählen Sie im Dropdown-Menü den gewünschten Kapselungstyp aus. Das jeweilige Fenster *Basic Setup* (Grundlegende Einrichtung) und die verfügbaren Funktionen unterscheiden sich je nach ausgewähltem Kapselungstyp.

- **VC Settings** (VC-Einstellungen): In diesem Bereich können Sie die VC-Einstellungen (*Virtual Circuit*, virtuelle Verbindung) konfigurieren.

  - **Multiplexing**: Wählen Sie entsprechend dem verwendeten ISP die Option **LLC** (LLC-Multiplexing) oder **VC** (VC-Multiplexing) aus.

  - **QoS Type** (QoS-Typ): Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus: **CBR** (*Continuous Bit Rate*, Konstante Bitrate), um eine feste Bandbreite für Sprach- oder Datenverkehr festzulegen, **UBR** (*Unspecific Bit Rate*, Unbestimmte Bitrate) für Anwendungen, die zeitunabhängig sind (z. B. E-Mail), oder **VBR** (*Variable Bit Rate*, Variable Bitrate) für diskontinuierlichen Datenverkehr und Bandbreiten, die mit anderen Anwendungen gemeinsam verwendet werden.

- **Pcr Rate** (PCR-Rate): Wenn Sie die Übertragungsrate der DSL-Leitung durch 424 dividieren, erhalten Sie die PCR-Rate. Diese gibt die maximale Rate an, mit der ein Sender Zellen senden kann. Geben Sie die Rate in diesem Feld ein (sofern dies für den Dienstanbieter erforderlich ist).

- **Scr Rate** (SCR-Rate): Gibt den Mittelwert der Zellrate an, die übertragen werden kann. Der Wert der SCR-Rate liegt gewöhnlich unter dem Wert der PCR-Rate. Geben Sie die Rate in diesem Feld ein (sofern dies für den Dienstanbieter erforderlich ist).

- **Autodetect** (Automatisch erkennen): Wählen Sie **Enable** (Aktivieren) aus, damit die Einstellungen automatisch eingetragen werden, oder **Disable** (Deaktivieren), um die Werte manuell einzugeben.

- **Virtual Circuit** (Virtuelle Verbindung): Für diese Option sind zwei Einstellungen erforderlich: **VPI** (*Virtual Path Identifier*, Virtueller Pfadidentifizierer) und **VCI** (*Virtual Channel Identifier*, Virtueller Kanalidentifizierer). Die korrekten Einstellungen erhalten Sie von Ihrem ISP.

- **IP Settings** (IP-Einstellungen): Befolgen Sie die Anweisungen, die im Abschnitt für den jeweils verwendeten Kapselungstyp aufgeführt sind.

„RFC 1483 Bridged“ (RFC 1483-Überbrückung)

Dynamische IP-Adresse

IP Settings (IP-Einstellungen): Aktivieren Sie **Obtain an IP Address Automatically** (IP-Adresse automatisch beziehen), wenn Sie laut Angaben Ihres ISP die Verbindung über eine dynamische IP-Adresse herstellen.

Statische IP-Adresse

Wenn Sie für die Internetverbindung eine permanente (statische) IP-Adresse verwenden, aktivieren Sie **Use the following IP Address** (Folgende IP-Adresse verwenden).

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways im WAN bzw. im Internet. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.

- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.

- **Default Gateway** (Standard-Gateway): Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.

- **Primary DNS** (Primärer DNS, erforderlich) und **Secondary DNS** (Sekundärer DNS, optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

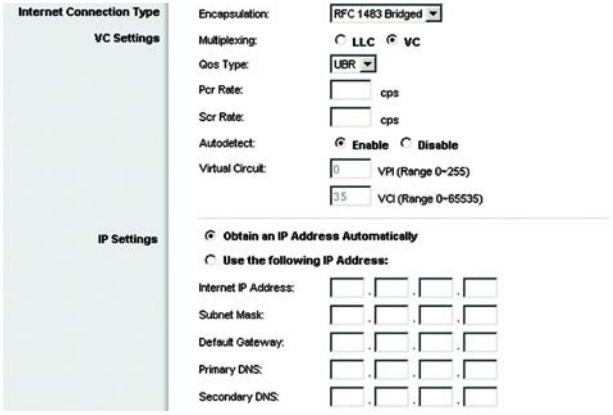


Abbildung 6-3: „RFC 1483 Bridged“ (RFC 1483-Überbrückung)

„RFC 1483 Routed“ (RFC 1483-Weiterleitung)

Wählen Sie zur Verwendung des Modus „RFC 1483 Routed“ die Option **RFC 1483 Routed** (RFC 1483-Weiterleitung) aus.

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways im WAN bzw. im Internet. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.
- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Default Gateway** (Standard-Gateway): Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primary DNS** (Primärer DNS, erforderlich) und **Secondary DNS** (Sekundärer DNS, optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

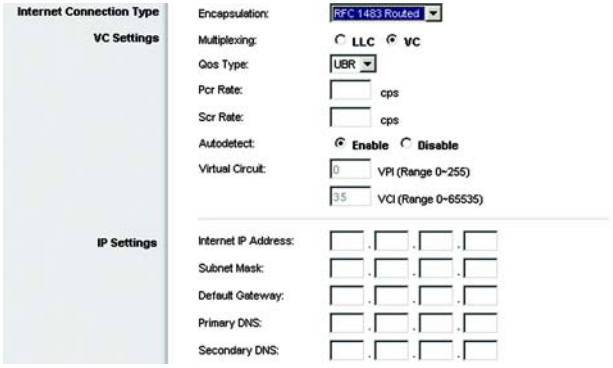


Abbildung 6-4: „RFC 1483 Routed“ (RFC 1483-Weiterleitung)

IPoA

Wenn Sie IPoA (*IP over ATM*) verwenden müssen, wählen Sie die Option **IPoA** aus.

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways im WAN bzw. im Internet. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.
- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Default Gateway** (Standard-Gateway): Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primary DNS** (Primärer DNS, erforderlich) und **Secondary DNS** (Sekundärer DNS, optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

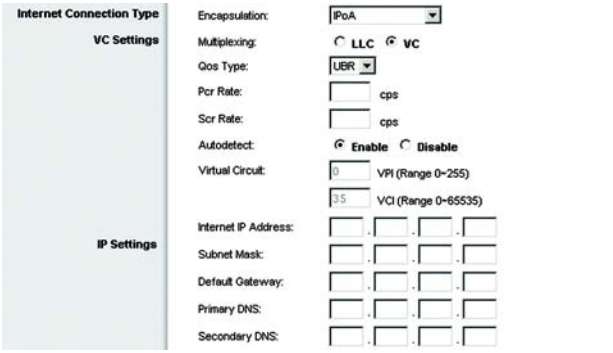


Abbildung 6-5: IPoA

RFC 2516 PPPoE

Einige ISPs mit DSL-Option verwenden PPPoE (*Point-to-Point Protocol over Ethernet*) zur Herstellung von Internetverbindungen. Wenn die Verbindung mit dem Internet über eine DSL-Leitung hergestellt wird, klären Sie mit dem ISP, ob PPPoE verwendet wird. Falls ja, aktivieren Sie die Option **PPPoE**.

- **User Name** (Benutzername) und **Password** (Passwort): Geben Sie den Benutzernamen und das Passwort ein, die Sie von Ihrem ISP erhalten haben.
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Connect on Demand** (Bei Bedarf verbinden). Geben Sie in das Feld *Max Idle Time* (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf die Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Bei Auswahl dieser Option überprüft das Gateway die Internetverbindung in regelmäßigen Abständen. Wenn die Verbindung getrennt wird, wird sie über das Gateway automatisch wieder hergestellt. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Keep Alive** (Verbindung aufrechterhalten). Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Standardmäßig erfolgt die Wahlwiederholung nach **30** Sekunden.

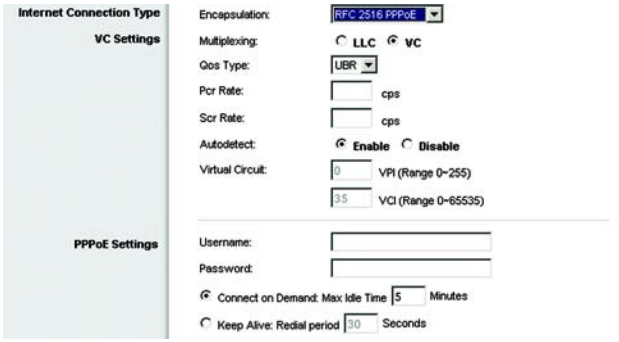


Abbildung 6-6: RFC 2516 PPPoE

WICHTIG: Damit die Funktion **Connect on Demand** (Bei Bedarf verbinden) ordnungsgemäß arbeitet, schließen Sie alle Internetanwendungen. Ansonsten kann das Gateway unter Umständen die Verbindung nicht beenden, je nachdem, wie oft die Anwendung versucht, eine Verbindung mit dem Internet aufzubauen (z. B. Chat-Programme).

RFC 2364 PPPoA

Einige ISPs mit DSL-Option verwenden PPPoA (*Point-to-Point Protocol over ATM*) zur Herstellung von Internetverbindungen. Wenn die Verbindung mit dem Internet über eine DSL-Leitung hergestellt wird, klären Sie mit dem ISP, ob PPPoA verwendet wird. Falls ja, aktivieren Sie die Option **PPPoA**.

- **User Name** (Benutzername) und **Password** (Passwort): Geben Sie den Benutzernamen und das Passwort ein, die Sie von Ihrem ISP erhalten haben.
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Connect on Demand** (Bei Bedarf verbinden). Geben Sie in das Feld *Max Idle Time* (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf die Internetverbindung getrennt werden soll.

  Keep Alive: Redial Period (Verbindung aufrechterhalten: Wahlwiederholung): Bei Auswahl dieser Option überprüft das Gateway die Internetverbindung in regelmäßigen Abständen. Wenn die Verbindung getrennt wird, wird sie über das Gateway automatisch wieder hergestellt. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Keep Alive** (Verbindung aufrechterhalten). Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Standardmäßig erfolgt die Wahlwiederholung nach **30** Sekunden.

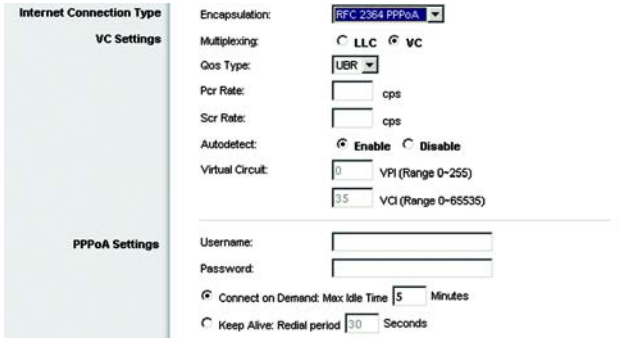


Abbildung 6-7: RFC 2364 PPPoA

„Bridge Mode Only“ (Nur Überbrückungsmodus)

Wenn Sie das Gateway als Überbrückung verwenden (Gateway agiert als Standalone-Modem), wählen Sie die Option **Bridge Mode Only** (Nur Überbrückungsmodus) aus. In diesem Modus sind alle Einstellungen für NAT und Routing deaktiviert.

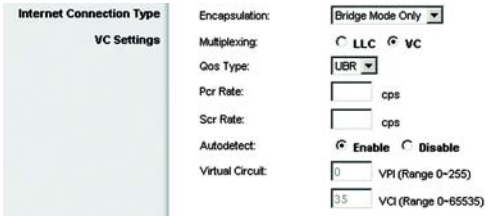


Abbildung 6-8: „Bridge Mode Only“ (Nur Überbrückungsmodus)

„Optional Settings (required by some ISPs)“ (Optionale Einstellungen (für einige ISPs erforderlich))

- **Host Name/Domain Name** (Hostname/Domänenname): In diesen Feldern können Sie einen Hostnamen und Domänennamen für das Gateway eingeben. Für einige ISPs sind diese Namen zu Identifikationszwecken erforderlich. Erfragen Sie bei Ihrem ISP, ob Ihr Breitband-Internetdienst mit einem Host- und Domänennamen konfiguriert wurde. In den meisten Fällen können diese Felder leer gelassen werden.
- **MTU** und **Size** (Größe): Mit der MTU-Einstellung (*Maximum Transmission Unit*, Maximale Übertragungseinheit) wird die maximale Paketgröße festgelegt, die zur Netzwerkübertragung zugelassen ist. Wählen Sie **Manual** (Manuell) aus, und geben Sie im Feld *Size* (Größe) den gewünschten Wert ein. Es wird empfohlen, einen Wert zwischen 1200 und 1500 einzugeben. Die maximale Übertragungseinheit (MTU) wird standardmäßig automatisch konfiguriert.

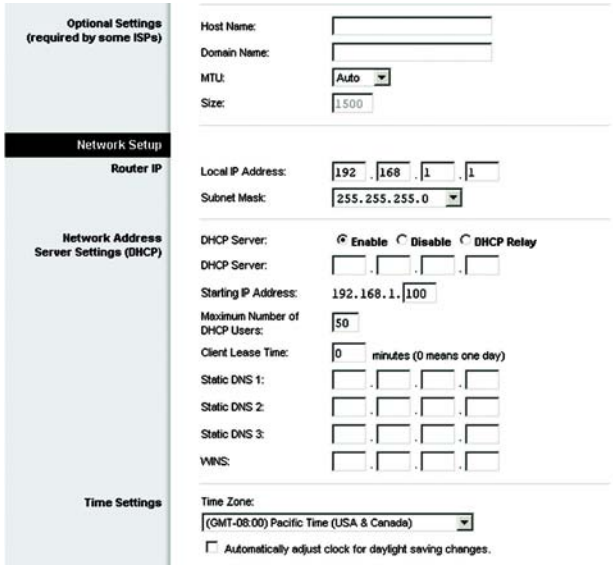


Abbildung 6-9: „Optional Settings“ (Optionale Einstellungen)

„Network Setup“ (Netzwerkeinrichtung)

- **Router IP** (IP-Adresse des Routers): Die Werte für die lokale IP-Adresse und Subnetzmaske des Gateways sind hier aufgeführt. In den meisten Fällen können die Standardwerte beibehalten werden.
  - **Local IP Address** (Lokale IP-Adresse): Der Standardwert ist **192.168.1.1**.
  - **Subnet Mask** „Subnetzmaske“: Der Standardwert ist **255.255.255.0**.
- **Network Address Server Settings (DHCP)** (Einstellungen des Netzwerkadressenservers (DHCP)): In diesem Bereich können Sie die DHCP-Einstellungen (*Dynamic Host Configuration Protocol*) des Gateways konfigurieren.
  - **DHCP Server** (DHCP-Server): Ein DHCP-Server (*Dynamic Host Configuration Protocol*) weist jedem Computer im Netzwerk automatisch eine IP-Adresse zu. Wenn Sie nicht schon über eine IP-Adresse verfügen, ist es äußerst empfehlenswert, das Gateway als DHCP-Server aktiviert zu lassen. Das Gateway kann auch im DHCP-Relay-Modus verwendet werden. (Diese Einstellung ist nicht bei allen Kapselungstypen verfügbar.)
  - **DHCP Server** (DHCP-Server): Wenn Sie für die Einstellung *DHCP Server* (DHCP-Server) den DHCP-Relay-Modus aktivieren, geben Sie die IP-Adresse für den DHCP-Relay-Server in den entsprechenden Feldern ein. (Diese Einstellung ist nicht bei allen Kapselungstypen verfügbar.)

- **Starting IP Address** (Start-IP-Adresse): Geben Sie einen Wert ein, mit dem der DHCP-Server beim Zuweisen von IP-Adressen beginnen soll. Der Wert muss mindestens 192.168.1.2 betragen, da die Standard-IP-Adresse für das Gateway **192.168.1.1** ist.

- **Maximum Number of DHCP Users** (Maximale Anzahl der DHCP-Benutzer): Geben Sie die maximale Anzahl der Benutzer bzw. Clients ein, denen eine IP-Adresse zugewiesen werden kann. Diese Zahl hängt von der eingegebenen Start-IP-Adresse ab.

- **Client Lease Time** (Client-Leasedauer): Bei der Client-Leasedauer handelt es sich um den Zeitraum, in dem ein Computer über seine aktuelle dynamische IP-Adresse eine Verbindung mit dem Gateway herstellen kann. Geben Sie in Minuten an, wie lange diese dynamische IP-Adresse dem Computer zugewiesen bleiben soll.

- **Static DNS 1-3** (Statisches DNS 1-3): Mit dem DNS (*Domain Name System*) übersetzt das Internet Domänen- oder Website-Namen in Internetadressen oder URLs. Sie erhalten von Ihrem ISP mindestens eine IP-Adresse für den DNS-Server. Hier können Sie bis zu drei IP-Adressen für den DNS-Server eingeben. Das Gateway verwendet diese für einen schnelleren Zugriff auf laufende DNS-Server.

- **WINS**: Mithilfe von WINS (*Windows Internet Naming Service*) werden NetBIOS-Namen in IP-Adressen umgewandelt. Wenn Sie einen WINS-Server verwenden, geben Sie hier die IP-Adresse des Servers ein. Andernfalls lassen Sie dieses Feld leer.

- **Time Setting** (Zeiteinstellung): Wählen Sie die entsprechende Zeitzone für den Standort des Gateways aus. Aktivieren Sie gegebenenfalls das Kontrollkästchen **Automatically adjust clock for daylight saving changes** (Uhr automatisch an Zeitumstellung anpassen).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „DDNS“

Das Gateway verfügt über die Funktion DDNS (*Dynamic Domain Name System*). Mit DDNS können Sie einer dynamischen Internet-IP-Adresse einen festen Host- und Domänennamen zuweisen. Dies kann sich für das Hosting Ihrer eigenen Website, Ihres FTP-Servers oder anderer Server hinter dem Gateway als nützlich erweisen.

Bevor Sie diese Funktion verwenden können, müssen Sie sich für den DDNS-Dienst unter www.dyndns.org oder www.tzo.com anmelden.

Abbildung 6-10: DDNS – DynDNS.org

DDNS

DDNS Service (DDNS-Dienst): Wenn der verwendete DDNS-Dienst von DynDNS.org zur Verfügung gestellt wird, wählen Sie im Dropdown-Menü die Option **DynDNS.org** aus. Wenn der verwendete DDNS-Dienst von TZO.com zur Verfügung gestellt wird, wählen Sie im Dropdown-Menü die Option **TZO.com** aus. Zum Deaktivieren des DDNS-Dienstes wählen Sie **Disabled** (Deaktiviert) aus.

DynDNS.org

- **User Name** (Benutzername), **Password** (Passwort) und **Host Name** (Hostname): Geben Sie den Benutzernamen, das Passwort und den Hostnamen des mithilfe von DynDNS.org festgelegten Kontos an.
- **Status**: Hier wird der Status der Verbindung zum DDNS-Dienst aufgeführt.
- **Connect** (Verbinden): Klicken Sie auf die Schaltfläche **Connect** (Verbinden), um die Verbindung mit dem DDNS-Dienst herzustellen.

TZO.com

- **E-mail Address** (E-Mail-Adresse), **Password** (Passwort) und **Domain Name** (Domänenname): Geben Sie die E-Mail-Adresse, das Passwort und den Domänennamen des Kontos ein, das Sie bei TZO eingerichtet haben.
- **Status**: Hier wird der Status der Verbindung zum DDNS-Dienst aufgeführt.
- **Connect** (Verbinden): Klicken Sie auf die Schaltfläche **Connect** (Verbinden), um die Verbindung mit dem DDNS-Dienst herzustellen.

Abbildung 6-11: DDNS – TZO.com

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „Advanced Routing“ (Erweitertes Routing)

Über das Fenster *Advanced Routing* (Erweitertes Routing) können Sie die Einstellungen für NAT sowie für das dynamische und statische Routing konfigurieren.

„Advanced Routing“ (Erweitertes Routing)

- **Operating Mode** (Betriebsmodus): In diesem Bereich können Sie die allgemeinen Routing-Einstellungen des Gateways konfigurieren.
    - **NAT**: Bei NAT handelt es sich um eine Sicherheitsfunktion, die standardmäßig aktiviert ist. Das Gateway kann über diese Funktion IP-Adressen des lokalen Netzwerks in eine andere IP-Adresse für die Internetnutzung umwandeln. Um NAT zu deaktivieren, klicken Sie auf das Optionsfeld **Disabled** (Deaktiviert).
- **Dynamic Routing** (Dynamisches Routing): Mit der Option **Dynamic Routing** (Dynamisches Routing) kann das Gateway automatisch an physische Änderungen in der Netzwerkanordnung angepasst werden. Bei Verwendung von RIP legt das Gateway die Route der Netzwerkpakete auf Grundlage der geringsten Anzahl der Gateways zwischen Quelle und Ziel fest. Über das RIP-Protokoll werden in regelmäßigen Abständen Routing-Informationen an andere Gateways im Netzwerk gesendet.
    - **RIP**: Bei mehreren Routern empfiehlt es sich, RIP (*Routing Information Protocol*) zu verwenden, damit die Router untereinander Routing-Informationen austauschen können. Klicken Sie zur Verwendung von RIP auf das Optionsfeld **Enabled** (Aktiviert). Behalten Sie andernfalls die Standardeinstellung **Disabled** (Deaktiviert) bei.
    - **RIP Send Packet Version** (RIP-Version für gesendete Pakete): Wählen Sie die gewünschte Protokollversion aus: **RIPv1** oder **RIPv2**.
    - **RIP Recv Packet Version** (RIP-Version für erhaltene Pakete): Wählen Sie die gewünschte Protokollversion aus: **RIPv1** oder **RIPv2**.
- **Static Routing** (Statisches Routing): Wenn das Gateway an mehr als einem Netzwerk angeschlossen ist, muss u. U. zwischen den Gateways eine statische Route eingerichtet werden. Eine statische Route ist ein vordefinierter Pfad, über den Netzwerkinformationen an einen bestimmten Host oder ein bestimmtes Netzwerk übertragen werden. Ändern Sie die folgenden Einstellungen, um eine statische Route zu erstellen:
    - **Select set number** (Set-Nummer auswählen): Wählen Sie im Dropdown-Menü die Nummer der statischen Route aus. Das Gateway unterstützt bis zu 20 Einträge für statische Routeneinträge. Wenn Sie eine Route löschen möchten, wählen Sie den entsprechenden Eintrag aus, und klicken Sie auf die Schaltfläche **Delete This Entry** (Diesen Eintrag löschen).

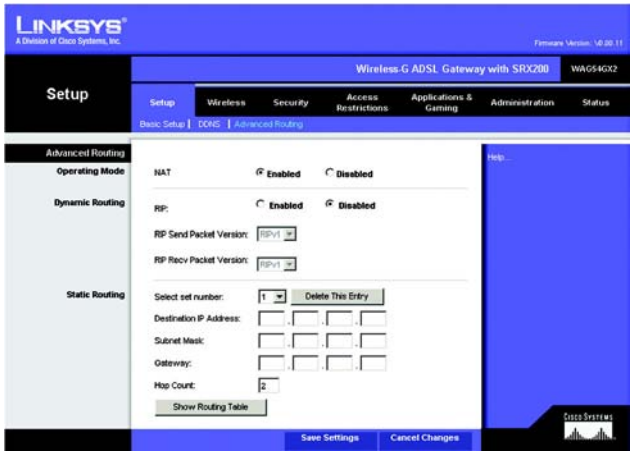


Abbildung 6-12: „Advanced Routing“ (Erweitertes Routing)

- **Destination IP Address** (Ziel-IP-Adresse): Bei der Ziel-IP-Adresse handelt es sich um die Adresse des entfernten Netzwerks bzw. Hosts, dem Sie eine statische Route zuweisen möchten. Geben Sie die IP-Adresse des Hosts ein, für den Sie eine statische Route erstellen möchten. Wenn Sie eine Route zu einem gesamten Netzwerk erstellen, vergewissern Sie sich, dass für den Netzwerkbereich der IP-Adresse der Wert **0** festgelegt ist.

- **Subnet Mask** (Subnetzmaske): Geben Sie die Subnetzmaske (auch Netzwerkmaske genannt) ein, mit der festgelegt wird, welcher Bereich einer IP-Adresse der Netzwerkbereich und welcher Bereich der Hostbereich ist.

- **Gateway**: Geben Sie die IP-Adresse des Gateway-Geräts ein, das eine Verbindung zwischen dem Gateway und dem entfernten Netzwerk bzw. Host ermöglicht.

- **Hop Count** (Anzahl der Gateways): Gibt die Anzahl der Gateways bis zu den einzelnen Knoten an, bevor das Ziel erreicht wird (max. 16 Gateways). Geben Sie die gewünschte Anzahl im entsprechenden Feld ein.

- **Show Routing Table** (Routing-Tabelle anzeigen): Klicken Sie auf die Schaltfläche **Show Routing Table** (Routing-Tabelle anzeigen), um ein Fenster zu öffnen, in dem die Weiterleitung von Daten im lokalen Netzwerk angezeigt wird. Für jede Route wird die IP-Adresse des Ziel-LANs, die Subnetzmaske, das Gateway und die Schnittstelle angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Daten zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster zurückzukehren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

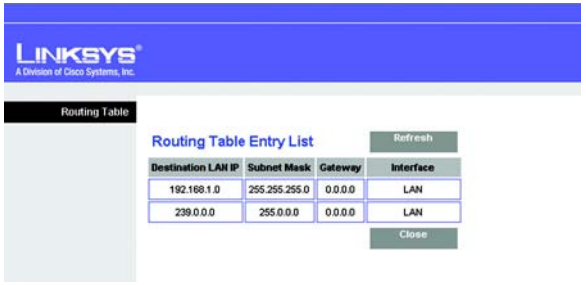


Abbildung 6-13: „Routing Table“ (Routing-Tabelle)

Registerkarte „Wireless“

Registerkarte „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen)

In diesem Fenster können Sie den Wireless-Netzwerkmodus und die Sicherheit im Wireless-Netzwerkbetrieb festlegen.

„Wireless Network“ (Wireless-Netzwerk)

- **Wireless Network Mode** (Wireless-Netzwerkmodus): Wenn sich sowohl 802.11g- als auch 802.11b-Geräte im Netzwerk befinden, behalten Sie die Standardeinstellung **Mixed** (Gemischt) bei. Wenn ausschließlich 802.11g-Geräte vorhanden sind, wählen Sie **G-Only** (Nur G) aus. Wenn ausschließlich 802.11b-Geräte vorhanden sind, wählen Sie **B-Only** (Nur B) aus. Um das Wireless-Netzwerk zu deaktivieren, wählen Sie **Disable** (Deaktivieren).

- **Wireless Network Name (SSID)** (Wireless-Netzwerkname (SSID)): Geben Sie in diesem Feld den Namen für das Wireless-Netzwerk ein. Bei der SSID handelt es sich um den Netzwerknamen, der von allen Geräten im drahtlosen Netzwerk verwendet wird. Sie muss für alle Geräte im Wireless-Netzwerk identisch sein. Für die maximal 32 Zeichen lange SSID dürfen alle alphanumerischen Zeichen der Tastatur verwendet werden. Es wird nach Groß- und Kleinschreibung unterschieden. Sie sollten die standardmäßige SSID (linksys) in einen eindeutigen Namen Ihrer Wahl ändern.

- **Wireless Channel** (Wireless-Kanal): Wählen Sie aus der Liste den Ihren Netzwerkeinstellungen entsprechenden Kanal aus. Eine korrekte Funktion Ihres Wireless-Netzwerks ist nur gewährleistet, wenn die Übertragung für alle Geräte über denselben Kanal erfolgt. Die Wireless-Computer oder -Clients erkennen den Wireless-Kanal des Gateways automatisch.

- **Wireless SSID Broadcast** (Wireless-SSID-Übertragung): Wenn Wireless-Computer oder -Clients im lokalen Netzwerk nach Wireless-Netzwerken suchen, mit denen sie eine Verbindung herstellen können, erkennen sie die vom Gateway übertragene SSID. Wenn die SSID des Gateways übertragen werden soll, behalten Sie die Standardeinstellung **Enable** (Aktivieren) bei. Wenn die SSID des Gateways nicht übertragen werden soll, wählen Sie **Disable** (Deaktivieren) aus.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-14: „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen)

Registerkarte „Wireless Security“ (Sicherheit im Wireless-Netzwerkbetrieb)

Mit den Wireless-Sicherheitseinstellungen wird die Sicherheit des Wireless-Netzwerks konfiguriert. Das Gateway unterstützt sechs Optionen für die Sicherheit im Wireless-Netzwerkbetrieb: **WPA-Personal**, **WPA2-Personal**, **WPA2-Mixed** (WPA2 Gemischt), WPA Enterprise, WPA2 Enterprise und **WEP**. WPA steht für *Wi-Fi Protected Access*. Dies ist ein höherer Sicherheitsstandard als die WEP-Verschlüsselung (*Wired Equivalent Privacy*). WPA2 ist eine komplexere, sicherere Version von WPA. WPA Enterprise und WPA2 Enterprise verwenden RADIUS (Remote Authentication Dial-In User Service) für die Authentifizierung. Im Folgenden werden diese Sicherheitsstandards kurz erläutert. Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Gateways finden Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“.

Um die Option zur Sicherheit im Wireless-Netzwerkbetrieb zu deaktivieren, wählen Sie im Dropdown-Menü *Security Mode* (Sicherheitsmodus) die Option **Disable** (Deaktivieren) aus.

- **Security Mode** (Sicherheitsmodus): Wählen Sie den im Netzwerk zu verwendenden Modus aus: **WPA-Personal**, **WPA2-Personal**, **WPA2-Mixed** (WPA2 Gemischt), **WPA Enterprise**, **WPA2 Enterprise** oder **WEP**. Wenn Geräte für **WPA-Personal** und **WPA2-Personal** verwendet werden, wählen Sie **WPA2-Mixed** (WPA2 Gemischt) aus.

WPA-Personal

- **Encryption** (Verschlüsselung): Wählen Sie die gewünschte Verschlüsselungsmethode aus: **TKIP** oder **AES**. (AES bietet eine stärkere Verschlüsselung als TKIP.)
- **Passphrase**: Geben Sie den Schlüssel ein, der vom Gateway und von den anderen Netzwerkgeräten gemeinsam verwendet wird. Er muss aus 8 bis 63 Zeichen bestehen.
- **Key Renewal** (Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu speichern, oder klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen rückgängig zu machen. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

WPA2-Personal

- **Encryption** (Verschlüsselung): Es wird automatisch **AES** ausgewählt.
- **Passphrase**: Geben Sie den Schlüssel ein, der vom Gateway und von den anderen Netzwerkgeräten gemeinsam verwendet wird. Er muss aus 8 bis 63 Zeichen bestehen.
- **Key Renewal** (Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Abbildung 6-15: „Wireless Security“ (Wireless-Sicherheit) – „WPA-Personal“

WICHTIG: Wenn Sie die Wireless-Sicherheit verwenden, MUSS jedes Gerät im Wireless-Netzwerk dieselbe Methode für die Wireless-Sicherheit und denselben gemeinsamen Schlüssel verwenden, damit das Wireless-Netzwerk ordnungsgemäß funktioniert. Wenn Geräte für **WPA-Personal** und **WPA2-Personal** verwendet werden, sollten Sie **WPA2-Mixed** (WPA2 Gemischt) auswählen. Sie können WPA und WPA2 Enterprise mischen, nicht jedoch Personal und Enterprise, Personal und WEP bzw. Enterprise und WEP.

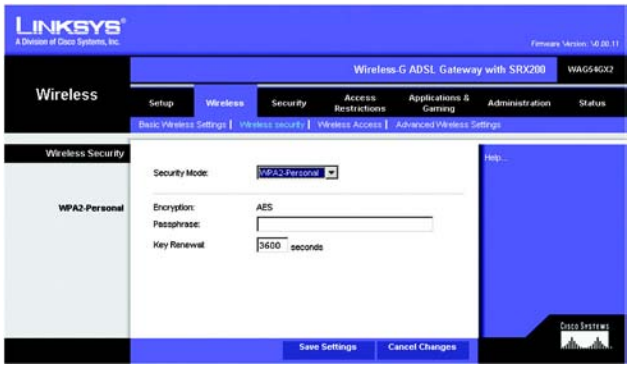


Abbildung 6-16: „Wireless Security“ (Wireless-Sicherheit) – „WPA2-Personal“

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu speichern, oder klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen rückgängig zu machen. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

„WPA2-Mixed“ (WPA2 Gemischt)

- **Encryption** (Verschlüsselung): Es wird automatisch **TKIP + AES** ausgewählt, damit beide Methoden verfügbar sind.
- **Passphrase**: Geben Sie den Schlüssel ein, der vom Gateway und von den anderen Netzwerkgeräten gemeinsam verwendet wird. Er muss aus 8 bis 63 Zeichen bestehen.
- **Key Renewal** (Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-17: „Wireless Security“ (Wireless-Sicherheit) – „WPA2-Mixed“ (WPA2 Gemischt)

„WPA Enterprise“ (WPA-Enterprise)

Bei der Verschlüsselungsmethode WPA Enterprise wird WPA in Kombination mit einem RADIUS-Server verwendet. (Diese Methode sollte nur dann eingesetzt werden, wenn das Gateway mit einem RADIUS-Server verbunden ist.)

- **RADIUS Server Address** (RADIUS-Server-Adresse): Geben Sie die IP-Adresse des RADIUS-Servers ein.
- **RADIUS Port** (RADIUS-Port): Geben Sie die Port-Nummer des RADIUS-Servers ein.
- **Shared Key** (Freigegebener Schlüssel): Geben Sie den Schlüssel ein, der vom Gateway und dem zugehörigen RADIUS-Server gemeinsam verwendet wird.
- **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-18: „Wireless Security“ (Wireless-Sicherheit) – „WPA Enterprise“

WPA2 Enterprise

Bei der Verschlüsselungsmethode **WPA2 Enterprise** wird WPA2 in Kombination mit einem RADIUS-Server verwendet. (Diese Methode sollte nur dann eingesetzt werden, wenn das Gateway mit einem RADIUS-Server verbunden ist.)

- **RADIUS Server Address** (RADIUS-Server-Adresse): Geben Sie die IP-Adresse des RADIUS-Servers ein.
- **RADIUS Port** (RADIUS-Port): Geben Sie die Port-Nummer des RADIUS-Servers ein.
- **Shared Key** (Freigegebener Schlüssel): Geben Sie den Schlüssel ein, der vom Gateway und dem zugehörigen RADIUS-Server gemeinsam verwendet wird.
- **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-19: „Wireless Security“ (Wireless-Sicherheit) – „WPA2 Enterprise“

WEP

- **Encryption** (Verschlüsselung): Wählen Sie die entsprechende Verschlüsselungsebene aus: **64 Bit** oder **128 Bit**. Eine höhere Verschlüsselungsebene bedeutet mehr Sicherheit.
- **Passphrase**: Sie können anstelle der manuellen Eingabe von WEP-Schlüsseln eine Passphrase verwenden. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden, und die Länge von 32 alphanumerischen Zeichen darf nicht überschritten werden. (Die Passphrase ist nur mit Wireless-Produkten von Linksys kompatibel und kann nicht mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung verwendet werden. Wenn Sie mit Wireless-Produkten anderer Hersteller oder mithilfe der drahtlosen Verbindung unter Windows XP kommunizieren möchten, notieren Sie die generierten WEP-Schlüssel, und geben Sie den entsprechenden Schlüssel manuell am Wireless-Computer bzw. im Client ein.) Wenn Sie eine Passphrase verwenden möchten, geben Sie sie im Feld *Passphrase* ein, und klicken Sie auf die Schaltfläche **Generate** (Erstellen).
- **WEP Key 1** (WEP-Schlüssel 1) bis **WEP Key 4** (WEP-Schlüssel 4): Wenn Sie keine Passphrase verwenden, geben Sie manuell einen Wertesatz ein. (Lassen Sie ein Schlüsselfeld nicht leer, und geben Sie nicht in allen Schlüsselfeldern den Wert 0 ein, da es sich hierbei nicht um gültige Schlüsselwerte handelt.) Wenn Sie eine 40/64-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 10 Hexadezimalziffern betragen. Wenn Sie eine 128-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 26 hexadezimale Zeichen betragen. Gültige hexadezimale Zeichen sind Zeichen von „0“ bis „9“ und von „A“ bis „F“.

Abbildung 6-20: „Wireless Security“ (Wireless-Sicherheit) – „WEP“

- **TX Key** (TX-Schlüssel): Wählen Sie eine Standardnummer für den Übertragungsschlüssel aus, um den zu verwendenden WEP-Schlüssel anzugeben.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „Wireless Access“ (Wireless-Zugriff)

„Wireless Network Access“ (Wireless-Netzwerkzugriff)

Wireless Network Access (Wireless-Netzwerkzugriff): Aktivieren Sie **Allow All** (Alle zulassen), wenn allen Computern der Zugriff auf das Wireless-Netzwerk ermöglicht werden soll. Soll der Zugriff eingeschränkt werden, wählen Sie **Restrict Access** (Zugriff beschränken) und anschließend zum Verweigern des Zugriffs für bestimmte Computer die Option **Prevent** (Verweigern) oder zum Gestatten des Zugriffs für bestimmte Computer die Option **Permit only** (Nur Zugriff) aus. Klicken Sie auf die Schaltfläche **Update Filter List** (Filterliste aktualisieren). Daraufhin wird das Fenster *Mac Address Filter List* (MAC-Adressen-Filterliste) angezeigt.

Geben Sie die MAC-Adressen der Computer ein, die Sie festlegen möchten. Wenn Sie eine Liste der MAC-Adressen für Wireless-Computer oder -Clients anzeigen möchten, klicken Sie auf die Schaltfläche **Wireless Client MAC List** (MAC-Liste der Wireless-Clients).

Im Fenster *Wireless Client List* (Liste der Wireless-Clients) sind die MAC-Adressen der Wireless-Geräte aufgeführt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), damit die aktuellsten Informationen angezeigt werden. Wenn der MAC-Adressen-Filterliste ein bestimmter Computer hinzugefügt werden soll, aktivieren Sie das Kontrollkästchen **Enable MAC Filter** (MAC-Filter aktivieren), und klicken Sie anschließend auf die Schaltfläche **Update Filter List** (Filterliste aktualisieren). Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *MAC Address Filter List* (MAC-Adressen-Filterliste) zurückzukehren.

Klicken Sie im Fenster *MAC Address Filter List* (MAC-Adressen-Filterliste) auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Liste zu speichern, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Eingaben zu löschen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-21: „Wireless Access“ (Wireless-Zugriff)

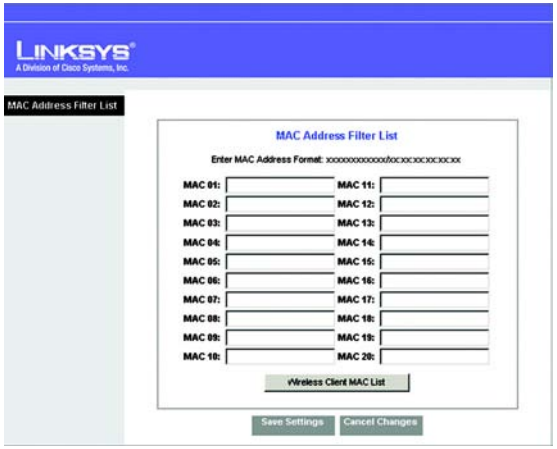


Abbildung 6-22: „MAC Address Filter List“ (MAC-Adressen-Filterliste)

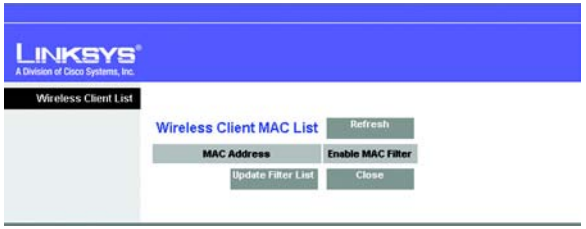


Abbildung 6-23: „Wireless Client MAC List“ (MAC-Liste der Wireless-Clients)

Registerkarte „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen)

In diesem Fenster können Sie auf die erweiterten Wireless-Funktionen zugreifen.

„Advanced Wireless“ (Erweitertes Wireless)

„Wireless-G Settings“ (Wireless-G-Einstellungen)

Auf dieser Registerkarte werden die erweiterten Wireless-Funktionen des Gateways eingerichtet. Diese Einstellungen sollten nur von einem erfahrenen Administrator angepasst werden, da falsche Einstellungen die Leistung des Routers im Wireless-Betrieb beeinträchtigen können.

- **Basic Rate Set** (Eingestellte Grundrate): Die eingestellte Grundrate stellt einen Satz von Raten dar, mit denen das Gateway Übertragungen ausführen kann. (Wenn Sie die Datenübertragungsrate des Gateways festlegen möchten, konfigurieren Sie die Einstellung **Transmission Rate** (Übertragungsrate).) Das Gateway teilt anderen Wireless-Geräten im Netzwerk seine eingestellte Grundrate mit, sodass bekannt ist, welche Raten unterstützt werden. Der Gateway gibt außerdem bekannt, dass automatisch die optimale Übertragungsrate ausgewählt wird. In den meisten Fällen sollten Sie die Standardeinstellung übernehmen, also **Default (1-2-5.5-11)** (Standard (1-2-5.5-11). Weitere verfügbare Optionen sind **1-2Mbps** (1-2 MBit/s) für die Verwendung mit älterer Wireless-Technologie und **All** (Alle), wenn das Gateway bei allen standardmäßigen Wireless-Raten Übertragungen ausführen kann.

- **Transmission Rate** (Übertragungsrate): Die Datenübertragungsrate sollte gemäß der Geschwindigkeit des Wireless-Netzwerks eingestellt werden. Sie können aus einer Reihe von Übertragungsgeschwindigkeiten auswählen oder auch die Option **Auto** (Automatisch) aktivieren, mit der das Gateway automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert wird. Mit der Funktion für automatisches Fallback wird die optimale Verbindungsgeschwindigkeit zwischen dem Gateway und einem Wireless-Client ermittelt. Die Standardeinstellung lautet **Auto** (Automatisch).

- **CTS Protection Mode** (CTS-Schutzmodus): Behalten Sie die Standardeinstellung **Auto** (Automatisch) für die Option **CTS Protection Mode** (CTS-Schutzmodus; CTS = Clear-To-Send) bei, damit der CTS-Schutzmodus verwendet wird, wenn Ihre Wireless-G-Produkte in einer Umgebung mit hohem 802.11b-Datenverkehr keine Übertragungen an den Gateway ausführen können. Diese Funktion verbessert zwar die Fähigkeit des Gateways, alle Wireless-G-Übertragungen zu empfangen, verringert jedoch auch beträchtlich seine Leistung.

- **Beacon Interval** (Beacon-Intervall): Ein Beacon ist eine Paketübertragung des Gateways zur Synchronisierung des Wireless-Netzwerks.**Beacon Interval** (Beacon-Intervall): Der Standardwert ist **100**. Geben Sie einen Wert zwischen 1 und 65.535 Millisekunden ein. Der Wert des Beacon-Intervalls gibt das Sendeintervall des Beacons an. Ein Beacon ist eine Paketübertragung des Gateways zur Synchronisierung des Wireless-Netzwerks.

Abbildung 6-24: „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen)

- **DTIM Interval** (DTIM-Intervall): Der Wert (zwischen 1 und 255) gibt das Intervall der DTIM (*Delivery Traffic Indication Message*) an. Ein DTIM-Feld ist ein Zeitkontrollfeld, das die Clients über das nächste Fenster informiert, in dem nach Broadcast- und Multicast-Meldungen gesucht wird. Wenn das Gateway Broadcast- oder Multicast-Meldungen für die zugewiesenen Clients gepuffert hat, sendet er die nächste DTIM mit einem DTIM-Intervallwert. Die zugewiesenen Clients empfangen das Beacon-Signal und sind zum Empfang der Broadcast- und Multicast-Meldungen bereit. Der Standardwert lautet **1**.

- **Fragmentation Threshold** (Fragmentierungsschwelle): Dieser Wert gibt die maximale Größe eines Pakets an, bevor die Daten in mehrere Pakete unterteilt werden. Wenn Sie eine hohe Paketfehlerrate wahrnehmen, können Sie die Fragmentierungsschwelle leicht anheben. Liegt die Fragmentierungsschwelle zu niedrig, kann dies zu einer Herabsetzung der Netzwerkleistung führen. Es wird empfohlen, den Standardwert nur geringfügig zu senken. In den meisten Fällen sollte er beim Standardwert **2346** belassen werden.

- **RTS Threshold** (RTS-Schwelle): Bei einem schwankenden Datenfluss wird eine nur geringfügige Senkung empfohlen. Wenn ein Netzwerkpaket kleiner als die voreingestellte RTS-Schwellengröße ist, wird der RTS/CTS-Mechanismus nicht aktiviert. Das Gateway sendet RTS-Blöcke (*RTS = Request to Send*) an eine bestimmte Empfangsstation und handelt das Senden eines Daten-Blocks aus. Nach dem Empfang eines RTS-Blocks antwortet die Wireless-Station mit einem CTS-Block (*CTS = Clear to Send*), um das Recht, mit der Übertragung zu beginnen, zu bestätigen. Dieser Wert sollte bei dem Standardwert **2346** belassen werden.

- **Preamble Type** (Präambeltyp): Die Präambel legt die Länge des CRC-Blocks (*Cyclic Redundancy Check*) zur Kommunikation des Gateways mit den Wireless-Roaming-Clients fest. (In Bereichen mit hohem Netzwerkverkehr sollte der kürzere Präambeltyp verwendet werden.) Wählen Sie den geeigneten Präambeltyp aus: **Long** (Lang; Standardeinstellung) oder **Short** (Kurz).

- **Network Density** (Netzwerkdichte): Diese Einstellung bestimmt den Übertragungs- und Empfangsbereich des Gateways. Wählen Sie eine der folgenden Einstellungen aus: **Low** (Niedrig; größere Reichweite), **Medium** (Mittel; mittelgroße Reichweite) oder **High** (Hoch; kleinere Reichweite). Die Einstellung **Low** (Niedrig) wird empfohlen, wenn nur wenige Wireless-Netzwerke in Ihrer Arbeitsumgebung betrieben werden, die Einstellung **High** (Hoch) entsprechend dann, wenn starker Datenverkehr in nahe gelegenen Wireless-Netzwerken vorliegt. Die Einstellung **Medium** (Mittel) bildet den Mittelweg bei der Reichweite. Die Standardeinstellung lautet **Low** (Niedrig).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „Security“ (Sicherheit)

Registerkarte „Firewall“

Sie können die Firewall aktivieren oder deaktivieren, Filter zum Blockieren bestimmter Internetdatentypen auswählen und anonyme Internet-Anfragen blockieren. Verwenden Sie diese Funktionen, um die Sicherheit des Netzwerks zu erhöhen.

Firewall

- **SPI Firewall Protection** (SPI-Firewall-Schutz): Die Firewall-Funktion SPI (*Stateful Packet Inspection*) erhöht die Sicherheit des Netzwerks. Klicken Sie zur Verwendung dieser Funktion auf **Enable** (Aktivieren). Wenn die Firewall nicht verwendet werden soll, klicken Sie auf **Disable** (Deaktivieren).

„Additional Filters“ (Zusätzliche Filter)

- **Filter Proxy** (Proxy filtern): Die Verwendung von WAN-Proxyservern kann die Sicherheit des Gateways beeinträchtigen. Wenn Sie die Proxyfilterung verweigern, wird der Zugriff auf alle WAN-Proxyserver deaktiviert. Aktivieren Sie zum Verwenden der Proxy-Filterung das entsprechende Kontrollkästchen.
- **Filter Cookies** (Cookies filtern): Bei einem Cookie handelt es sich um Daten, die auf einem Computer gespeichert sind und von Websites beim Zugriff auf diese Sites verwendet werden. Aktivieren Sie zum Verwenden der Cookie-Filterung das entsprechende Kontrollkästchen.
- **Filter Java Applets** (Java-Applets filtern): Bei Java handelt es sich um eine Programmiersprache für Websites. Wenn Sie Java-Applets ablehnen, haben Sie möglicherweise keinen Zugriff auf Websites, die mit dieser Programmiersprache erstellt wurden. Aktivieren Sie zum Verwenden der Java Applet-Filterung das entsprechende Kontrollkästchen.
- **Filter ActiveX** (ActiveX filtern): Bei ActiveX handelt es sich um eine Programmiersprache für Websites. Wenn Sie ActiveX ablehnen, haben Sie möglicherweise keinen Zugriff auf Websites, die mit dieser Programmiersprache erstellt wurden. Aktivieren Sie zum Verwenden der ActiveX-Filterung das entsprechende Kontrollkästchen.

„Block WAN Requests“ (WAN-Anfragen blockieren)

- **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren): Mit dieser Option können Sie Ihr Netzwerk vor Ping-Angriffen oder dem Erkennen durch andere Internetbenutzer schützen. Darüber hinaus können Sie mit dieser Option die Sicherheit des Netzwerks erhöhen, indem die Netzwerk-Ports nicht angezeigt werden und das Netzwerk vor Angreifern aus dem Internet besser geschützt ist. Aktivieren Sie die Option **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren), um anonyme Internet-Anfragen zu blockieren, oder deaktivieren Sie die Option, um anonyme Internet-Anfragen zuzulassen.

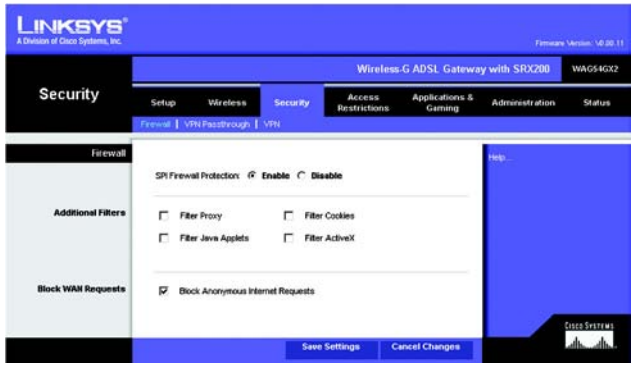


Abbildung 6-25: Firewall

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „VPN Passthrough“ (VPN-Passthrough)

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, durch die eine sichere Verbindung zwischen zwei entfernten Standorten hergestellt wird. Konfigurieren Sie die folgenden Einstellungen so, dass das Gateway die Übertragung durch VPN-Tunnel zulässt.

Abbildung 6-26: „VPN Passthrough“ (VPN-Passthrough)

„VPN Passthrough“ (VPN-Passthrough)

- **IPSec Passthrough** (IPSec-Passthrough): IPSec (*Internet Protocol Security*) ist ein Protokollsatz, der zur Implementierung eines sicheren Paketaustauschs auf der IP-Ebene verwendet wird. Um IPSec-Passthrough zu aktivieren, klicken Sie auf das Optionsfeld **Enable** (Aktivieren). Um IPSec-Passthrough zu deaktivieren, klicken Sie auf das Optionsfeld **Disable** (Deaktivieren).

- **PPTP Passthrough** (PPTP-Passthrough): PPTP-Passthrough (*Point-to-Point Tunneling Protocol Passthrough*) ist eine Methode zur Aktivierung von VPN-Sitzungen auf einem Windows NT 4.0- oder Windows 2000-Server. Um PPTP-Passthrough zu aktivieren, klicken Sie auf das Optionsfeld **Enable** (Aktivieren). Um PPTP-Passthrough zu deaktivieren, klicken Sie auf das Optionsfeld **Disable** (Deaktivieren).

- **L2TP Passthrough** (L2TP-Passthrough): Bei L2TP-Passthrough (*Layering 2 Tunneling Protocol Passthrough*) handelt es sich um eine Erweiterung von PPTP (Point-to-Point Tunneling Protocol), mit der der Betrieb eines VPN über das Internet ermöglicht wird. Um P2TP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren). Um P2TP-Passthrough zu deaktivieren, klicken Sie auf das Optionsfeld **Disable** (Deaktivieren).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „VPN“

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, durch die eine sichere Verbindung zwischen zwei entfernten Standorten hergestellt wird. Mit diesen Einstellungen lassen Sie bis zu fünf VPN-Tunnel durch das Gateway anlegen.

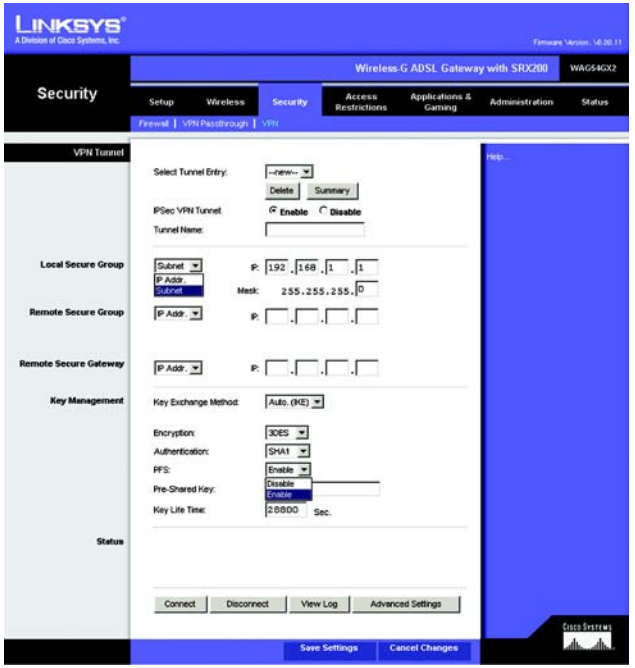


Abbildung 6-27: VPN

„VPN Tunnel“ (VPN-Tunnel)

- **Select Tunnel Entry** (Tunneleintrag auswählen): Um diesen Tunnel einzurichten, wählen Sie **New** (Neu). Sollen die Einstellungen für einen Tunnel geändert werden, wählen Sie den gewünschten Tunnel aus.
- **Delete** (Löschen): Zum Löschen eines Tunnels wählen Sie diesen im Dropdown-Menü aus, und klicken Sie auf die Schaltfläche **Delete** (Löschen).
- **Summary** (Zusammenfassung): Um die Einstellungen für einen Tunnel abzurufen, wählen Sie den gewünschten Tunnel im Dropdown-Menü aus, und klicken Sie auf die Schaltfläche **Summary** (Zusammenfassung).
- **IPSec VPN Tunnel** (IPSec VPN-Tunnel): Soll der aktuelle VPN-Tunnel aktiviert werden, wählen Sie entsprechend **Enable** (Aktivieren). Andernfalls wählen Sie **Disable** (Deaktivieren) aus.
- **Tunnel Name** (Tunnelname): Wenn der Tunnel aktiviert ist, geben Sie den Namen des Tunnels ein. Verwenden Sie eindeutige Namen, um so mehrere Tunnel zweifelsfrei voneinander unterscheiden zu können. Der Name, den Sie dem Tunnel am lokalen Ende geben, muss nicht mit dem Namen am entfernten Ende des Tunnels übereinstimmen.

„Local Secure Group“ (Lokale sichere Gruppe)

Die lokale sichere Gruppe umfasst die Computer in Ihrem lokalen Netzwerk, die auf den Tunnel zugreifen können. Wählen Sie im Dropdown-Menü die Option **IP Addr.** (IP-Adresse) oder **Subnet** (Subnetz) aus.

- „IP Addr.“ (IP-Adr.) Mit der Option **IP Addr.** (IP-Adresse) können Sie einen bestimmten Computer angeben. Geben Sie anschließend in das Feld *IP* (IP-Adresse) die IP-Adresse des Computers ein.
- **Subnet** (Subnetz): Mit der Option **Subnet** (Subnetz) nehmen Sie das gesamte Netzwerk in den Tunnel auf. Geben Sie anschließend in das Feld *IP* (IP-Adresse) die IP-Adresse des Gateways ein und in das Feld *Mask* (Maske) entsprechend die Subnetzmaske.

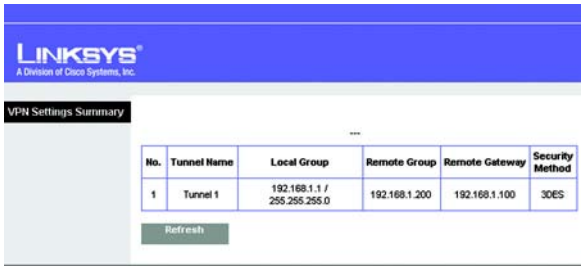


Abbildung 6-28: „VPN Settings Summary“ (Zusammenfassung der VPN-Einstellungen)

„Remote Secure Group“ (Entfernte sichere Gruppe)

Die entfernte sichere Gruppe umfasst die Computer am entfernten Ende des Tunnels, also die Computer, die auf den Tunnel zugreifen können. Wählen Sie im Dropdown-Menü die Option **IP Addr.** (IP-Adresse), **Subnet** (Subnetz) oder **Any** (Alle) aus.

- **IP Addr.** (IP-Adr.) Mit der Option **IP Addr.** (IP-Adresse) können Sie einen bestimmten Computer angeben. Geben Sie anschließend in das Feld *IP* (IP-Adresse) die IP-Adresse des Computers ein.
- **Subnet** (Subnetz): Mit der Option **Subnet** (Subnetz) nehmen Sie das gesamte Netzwerk in den Tunnel auf. Geben Sie in das Feld *IP* (IP-Adresse) die IP-Adresse des entfernten VPN-Geräts ein (z. B. für einen Router) und in das Feld *Mask* (Maske) die zugehörige Subnetzmaske.
- **Any** (Alle): Mit der Option **Any** (Alle) legen Sie fest, dass Anforderungen von jeglicher IP-Adresse durch das Gateway angenommen werden.

„Remote Secure Gateway“ (Entferntes Sicherheits-Gateway)

Das entfernte Sicherheits-Gateway ist das VPN-Gerät am entfernten Ende des VPN-Tunnels. Das VPN-Gerät kann ein VPN-Router, ein VPN-Server oder ein Computer mit VPN-Client-Software sein, der IPSec unterstützt. Wählen Sie im Dropdown-Menü die Option **IP Addr.** (IP-Adresse) oder **Any** (Alle) aus.

- **IP Addr.** (IP-Adr.) Mit der Option **IP Addr.** (IP-Adresse) legen Sie eine statische IP-Adresse fest. Geben Sie anschließend in das Feld *IP* (IP-Adresse) die IP-Adresse des VPN-Geräts ein.
- **Any** (Alle): Mit der Option **Any** (Alle) legen Sie fest, dass Anforderungen von jeglicher IP-Adresse durch das Gateway angenommen werden.

„Key Management“ (Schlüsselverwaltung)

- **Key Exchange Method** (Methode für den Schlüsselaustausch): Wählen Sie die Option **Auto (IKE)** oder **Manual** (Manuell) als Methode für den Schlüsselaustausch ausd. An beiden Enden eines VPN-Tunnels muss derselbe Modus für die Schlüsselverwaltung verwendet werden. Beide Methoden werden im Folgenden beschrieben. Sobald Sie eine Methode auswählen, ändert sich dieses Fenster, und die verfügbaren Einstellungen für die Methode werden eingeblendet.

  Auto (IKE)

  IKE (*Internet Key Exchange*) ist ein Protokoll für den Internet-Schlüsselaustausch, mit dem Schlüsselmaterial für eine Sicherheitsverknüpfung (*Security Association*, SA) ausgehandelt wird. Bei IKE wird der entfernte IDE-Peer mithilfe des vorläufigen gemeinsamen Schlüssels authentifiziert.

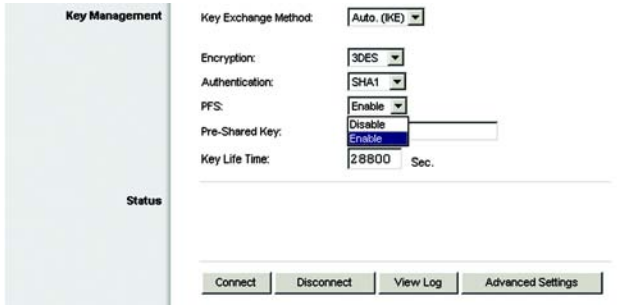


Abbildung 6-29: „Key Exchange Method“ (Methode für den Schlüsselaustausch) – „Auto (IKE)“

- **Encryption** (Verschlüsselung): Wenn Sie die Option **Auto (IKE)** auswählen, wird automatisch die 3DES-Verschlüsselung (168 Bit) aktiviert. Das VPN-Gerät am entfernten Ende des Tunnels muss dieselbe Verschlüsselungsart verwenden.
- **Authentication** (Authentifizierung): Wählen Sie eine der beiden verfügbaren Verschlüsselungsmethoden aus: **SHA1** oder **MD5**. MD5 besteht aus einem unidirektionalen Hash-Algorithmus, mit dem eine 128-Bit-Prüfsumme erzeugt wird. SHA ist ein unidirektionaler Hash-Algorithmus, der eine 160-Bit-Prüfsumme erzeugt. Die Verwendung von **SHA1** wird empfohlen, da diese Verschlüsselungsart sicherer ist. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels dieselbe Verschlüsselungsmethode eingesetzt wird.
- **PFS** (PFS, *Perfect Forward Secrecy*): PFS (*Perfect Forward Secrecy*) gewährleistet, dass der anfängliche Schlüsselaustausch und die IKE-Vorschläge sicher sind. Wählen Sie zum Verwenden von PFS die Option **Enable** (Aktivieren) aus. Andernfalls wählen Sie **Deaktivieren** aus.
- **Pre-Shared Key** (Vorläufiger gemeinsamer Schlüssel): Geben Sie eine Reihe von Zahlen oder Buchstaben in das Feld *Pre-shared Key* (Vorläufiger gemeinsamer Schlüssel) ein. Auf der Grundlage dieses Worts, das an beiden Enden des Tunnels eingegeben werden MUSS, wird ein Schlüssel erstellt, mit dem die über den Tunnel versendeten Daten verschlüsselt und entschlüsselt werden. Sie können in diesem Feld eine Kombination aus bis zu 24 Zahlen und Buchstaben eingeben. Es dürfen keine Sonderzeichen oder Leerzeichen verwendet werden.
- **Key Life Time** (Schlüssel-Verwendungsdauer): Hier können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, oder lassen Sie das Feld leer, sodass der Schlüssel unbegrenzt lange zur Verfügung steht.

„Manual“ (Manuell)

Bei der Option **Manual** (Manuell) erzeugen Sie den Schlüssel selbst; das Aushandeln eines Schlüssels ist nicht notwendig. Die manuelle Schlüsselverwaltung wird in der Regel in kleinen statischen Umgebungen sowie zur Fehlerbehebung eingesetzt.

- **Encryption Algorithm** (Verschlüsselungsalgorithmus): Wenn Sie die Option **Manual** (Manuell) auswählen, wird automatisch die 3DES-Verschlüsselung (168 Bit) aktiviert. Das VPN-Gerät am entfernten Ende des Tunnels muss dieselbe Verschlüsselungsart verwenden.
- **Encryption Key** (Verschlüsselungsschlüssel): Dieses Feld bestimmt den Schlüssel, der für die Ver- und Entschlüsselung des IP-Datenverkehrs eingesetzt werden soll. Der Verschlüsselungsschlüssel besteht aus 48 Bit; geben Sie also einen Schlüssel mit 24 ASCII-Zeichen ein. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels derselbe Verschlüsselungsschlüssel eingesetzt wird.

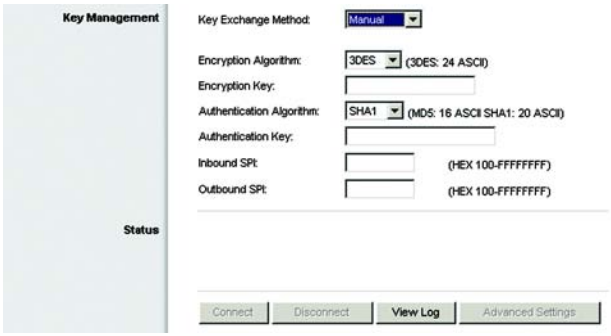


Abbildung 6-30: „Key Exchange Method“ (Methode für den Schlüsselaustausch) – „Manual“ (Manuell)

- **Authentication Algorithm** (Authentifizierungsalgorithmus): Wählen Sie eine Authentifizierungsmethode aus: **MD5** oder **SHA1**. Hiermit legen Sie das Verfahren fest, mit dem die ESP-Pakete authentifiziert werden. MD5 besteht aus einem unidirektionalen Hash-Algorithmus, mit dem eine 128-Bit-Prüfsumme erzeugt wird. SHA ist ein unidirektionaler Hash-Algorithmus, der eine 160-Bit-Prüfsumme erzeugt. Die Verwendung von **SHA1** wird empfohlen, da diese Verschlüsselungsart sicherer ist. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels dieselbe Verschlüsselungsmethode eingesetzt wird.

- **Authentication Key** (Authentifizierungsschlüssel): Dieses Feld bestimmt den Schlüssel, der für die Authentifizierung des IP-Datenverkehrs eingesetzt werden soll. Geben Sie einen Schlüssel mit Hexadezimalwerten ein. Bei der Option MD5 besteht der Authentifizierungsschlüssel aus 32 Bit; geben Sie daher 16 ASCII-Zeichen ein. Bei der Option SHA besteht der Authentifizierungsschlüssel aus 40 Bit, sodass entsprechend 20 ASCII-Zeichen einzugeben sind. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels derselbe Authentifizierungsschlüssel eingesetzt wird.

- **Inbound SPI** (Eingangs-SPI) und **Outbound SPI** (Ausgangs-SPI): Der SPI (*Security Parameter Index*, Sicherheitsparameter-Index) wird im ESP-Header (Encapsulating Security Payload) übertragen. Mit diesem Index sind der Empfänger und der Absender in der Lage, die Sicherheitsverknüpfung (*Security Association*, SA) auszuwählen, mit der ein Paket verarbeitet werden soll. Hexadezimalwerte sind möglich; der zulässige Bereich ist 100 bis ffffffff. Jeder Tunnel muss einen eindeutigen Eingangs-SPI und einen eindeutigen Ausgangs-SPI besitzen. Ein bestimmter SPI darf nicht von mehreren Tunneln verwendet werden. Der hier für **Inbound SPI** (Eingangs-SPI) eingestellte Wert muss dem Wert entsprechen, der am anderen Ende des Tunnels für eingestellt ist, und umgekehrt.

Status

Hier werden die Statusinformationen für die VPN-Tunnel des Gateways angezeigt.

Wenn Sie die Option **Manual** (Manuell) ausgewählt hatten, steht hier eine Schaltfläche bereit. Mit der Schaltfläche **View Log** (Protokoll anzeigen) rufen Sie die Aktivitätsprotokolle ab.

Wenn Sie die Option **Auto (IKE)** ausgewählt hatten, sind hier vier Schaltflächen verfügbar. Mit der Schaltfläche **Connect** (Verbinden) stellen Sie die VPN-Verbindung her.Mit der Schaltfläche **Disconnect** (Trennen) wird die VPN-Verbindung beendet. Mit der Schaltfläche **View Log** (Protokoll anzeigen) rufen Sie die Aktivitätsprotokolle ab. Mit der Schaltfläche **Advanced Settings** (Erweiterte Einstellungen) konfigurieren Sie die erweiterten Einstellungen für den VPN-Tunnel.

Abbildung 6-31: „VPN Log“ (VPN-Protokoll)

„Advanced VPN Tunnel Setup“ (Erweiterte IPSec VPN-Tunnel-Einrichtung)

Klicken Sie auf die Schaltfläche **Advanced Settings** (Weitere Einstellungen). Das Fenster *Advanced VPN Tunnel Setup* (Erweiterte VPN-Tunnel-Einrichtung) wird geöffnet.

Diese erweiterten IPSec-Einstellungen sind fortgeschrittenen Benutzern vorbehalten.

Phase 1

Phase 1 wird zur Erstellung einer Sicherheitsverknüpfung (SA), auch „IKE SA“ (*Internet Key Exchange, Security Association*) genannt, verwendet. Nach Abschluss von Phase 1 wird in Phase 2 mindestens eine „IPSec SA“ erstellt und für IPSec-Sitzungen verwendet.

Operation Mode (Betriebsmodus): Die beiden verfügbaren Betriebsmodi **Main** (Hauptmodus) und **Aggressive** (Aggressiver Modus) tauschen die gleichen IKE-Nutzlasten auf unterschiedlichen Sequenzen aus. Der Hauptmodus wird häufiger verwendet, wobei einige Anwender jedoch den schnelleren aggressiven Modus vorziehen. Der Hauptmodus kann zur durchschnittlichen Verwendung eingesetzt werden und enthält mehr Authentifizierungserfordernisse als der aggressive Modus. Die Verwendung des Hauptmodus wird empfohlen, da dieser Modus sicherer ist. Bei beiden Modi werden vom VPN-Router Anfragen sowohl im Haupt- als auch im aggressiven Modus vom standortfernen VPN-Gerät akzeptiert.

Local Identity (Lokale Identität): Wählen Sie das Optionsfeld **Local IP address** (Lokale IP-Adresse) oder **Name** aus. Bei der Option **Local IP address** (Lokale IP-Adresse) wird die Internet-IP-Adresse des Gateways verwendet. Wenn Sie die Option **Name** auswählen, geben Sie den vollständigen Domänennamen (Fully Qualified Domain Name, FQDN) des Gateways in das entsprechende Feld ein, sodass dessen aktuelle IP-Adresse per DDNS aufgefunden werden kann.

Remote Identity (Entfernte Identität): Wählen Sie das Optionsfeld **Remote IP address** (Entfernte IP-Adresse) oder **Name** aus. Bei der Option **Remote IP address** (Entfernte IP-Adresse) wird die Internet-IP-Adresse des entfernten VPN-Geräts verwendet. Wenn Sie die Option **Name** auswählen, geben Sie den vollständigen Domänennamen (Fully Qualified Domain Name, FQDN) des entfernten VPN-Geräts in das entsprechende Feld ein, so dass dessen aktuelle IP-Adresse per DDNS aufgefunden werden kann.

Encryption (Verschlüsselung): Diese Option dient zur Ver- und Entschlüsselung von ESP-Paketen. Die 3DES-Verschlüsselung (168 Bit) wird automatisch aktiviert.

Authentication (Authentifizierung): Wählen Sie die Methode aus, die zur Authentifizierung von ESP-Paketen verwendet wird. Sie können zwischen zwei Methoden wählen: MD5 und SHA1. Die Verwendung von **SHA1** wird empfohlen, da diese Verschlüsselungsart sicherer ist.

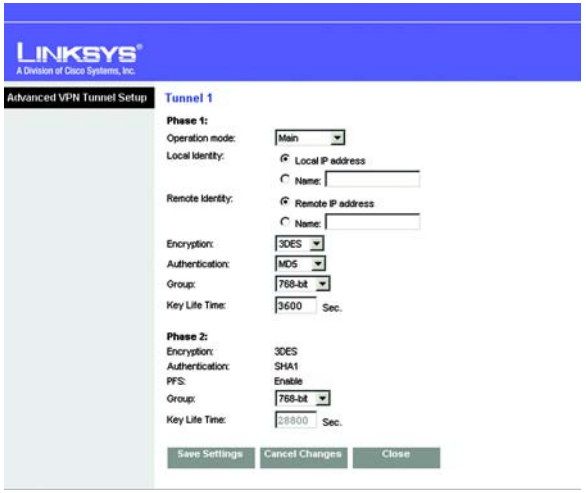


Abbildung 6-32: „Advanced VPN Tunnel Setup“ (Erweiterte IPSec VPN-Tunnel-Einrichtung)

Group (Gruppe): Es stehen drei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit, 1024 Bit und 1536 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.

Key Life Time (Schlüssel-Verwendungsdauer): Im Feld *Key Lifetime* (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, sodass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

Phase 2

Encryption (Verschlüsselung): Die in Phase 1 ausgewählte Verschlüsselungsmethode wird angezeigt.

Authentication (Authentifizierung): Die in Phase 2 ausgewählte Authentifizierungsmethode wird angezeigt.

PFS: Hier wird der Status der PFS-Funktion (Perfect Forward Secrecy) angezeigt.

Group (Gruppe): Es stehen drei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit, 1024 Bit und 1536 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.

Key Life Time (Schlüssel-Verwendungsdauer): Im Feld **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, sodass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu speichern, oder klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen rückgängig zu machen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen)

Registerkarte „Internet Access Policy“ (Richtlinien für Internetzugriff)

Im Fenster *Internet Access Policy* (Richtlinien für Internetzugriff) können Sie bestimmte Arten der Internetverwendung blockieren oder zulassen. Sie können für bestimmte Computer Richtlinien für den Internetzugriff einrichten und Websites nach URL-Adresse oder Schlüsselwort blockieren.

„Internet Access Policy“ (Richtlinien für Internetzugriff)

Internet Access Policy (Richtlinien für Internetzugriff): Der Zugriff kann mithilfe einer Richtlinie verwaltet werden. Über die Einstellungen in diesem Fenster können Sie Zugriffsrichtlinien anwenden, nachdem Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern) geklickt haben. Wenn Sie im Dropdown-Menü eine Richtlinie auswählen, werden die Einstellungen dieser Richtlinie angezeigt. Wenn Sie eine Richtlinie löschen möchten, wählen Sie die Nummer dieser Richtlinie aus, und klicken Sie auf die Schaltfläche **Delete** (Löschen). Klicken Sie zum Anzeigen aller Richtlinien auf die Schaltfläche **Summary** (Zusammenfassung). (Sie können Richtlinien im Fenster *Summary* (Zusammenfassung) löschen, indem Sie die entsprechende Richtlinie auswählen und auf die Schaltfläche **Delete** (Löschen) klicken. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Internet Access* (Internetzugriff) zurückzukehren.

Status: Die Richtlinien sind standardmäßig deaktiviert. Wenn Sie eine Richtlinie aktivieren möchten, wählen Sie im Dropdown-Menü die Nummer der Richtlinie aus, und klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren).

So erstellen Sie eine Richtlinie für den Internetzugriff:

1. Wählen Sie im Dropdown-Menü *Internet Access Policy* (Richtlinien für Internetzugriff) eine Nummer aus.
2. Klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren), um diese Richtlinie zu aktivieren.
3. Geben Sie in das vorgesehene Feld einen Richtliniennamen ein.

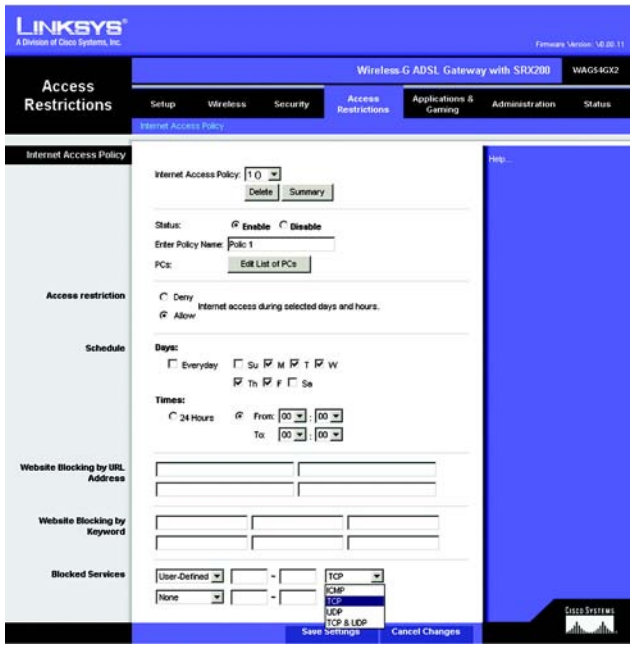


Abbildung 6-33: „Internet Access Policy“ (Richtlinien für Internetzugriff)

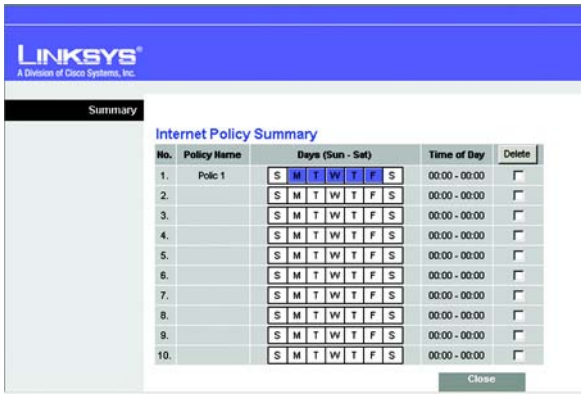


Abbildung 6-34: „Internet Policy Summary“ (Internetrichtlinien – Zusammenfassung)

4. Klicken Sie auf die Schaltfläche **Edit List of PCs** (PC-Liste bearbeiten), um die Computer auszuwählen, für die die Richtlinie gelten soll. Das Fenster *List of PCs* (PC-Liste) wird angezeigt. Ein PC kann nach MAC-Adresse oder IP-Adresse ausgewählt werden. Sie können auch eine Reihe von IP-Adressen eingeben, wenn die jeweilige Richtlinie für eine Gruppe von PCs gelten soll. Nachdem Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, oder auf **Cancel Changes** (Änderungen verwerfen), um die Änderungen zu verwerfen. Klicken Sie dann auf die Schaltfläche **Close** (Schließen), um das Fenster zu schließen.

5. Klicken Sie auf die entsprechende Option **Deny** (Verweigern) oder **Allow** (Zulassen), je nachdem, ob Sie den Internetzugriff für die im Fenster *List of PCs* (PC-Liste) aufgeführten Computer blockieren oder zulassen möchten.

6. Geben Sie an, an welchen Tagen und zu welchen Uhrzeiten diese Richtlinie gelten soll. Wählen Sie die einzelnen Tage aus, an denen die Richtlinie gültig sein soll, oder wählen Sie die Option **Everyday** (An allen Tagen) aus. Geben Sie anschließend den Gültigkeitszeitraum in Stunden und Minuten für die Richtlinie ein, oder wählen Sie die Option **24 Hours** (24 Stunden) aus.

7. Wenn Sie Websites mit bestimmten URL-Adressen blockieren möchten, geben Sie jeden URL in einem separaten Feld neben *Website Blocking by URL Address* (Website nach URL-Adresse blockieren) ein.

8. Wenn Sie Websites mithilfe bestimmter Schlüsselwörter blockieren möchten, geben Sie jedes Schlüsselwort in einem separaten Feld neben *Website Blocking by Keyword* (Website nach Schlüsselwort blockieren) ein.

9. Sie können den Zugang zu verschiedenen Diensten filtern, auf die über das Internet zugegriffen werden kann, z. B. FTP oder Telnet, indem Sie diese Dienste in den Dropdown-Menüs neben **Blocked Services** (Blockierte Dienste) auswählen. Die Port-Nummern und das Protokoll für den ausgewählten Dienst werden automatisch angezeigt.

   Wenn der gewünschte Dienst nicht aufgeführt ist, wählen Sie **User-Defined** (Benutzerdefiniert) aus. Geben Sie in den entsprechenden Feldern die Port-Nummern des Dienstes ein. Wählen Sie dann im Dropdown-Menü das Protokoll aus: **ICMP**, **TCP**, **UDP** oder **TCP & UDP**.

10. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Einstellungen der Richtlinie zu speichern. Um die Einstellungen der Richtlinie rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

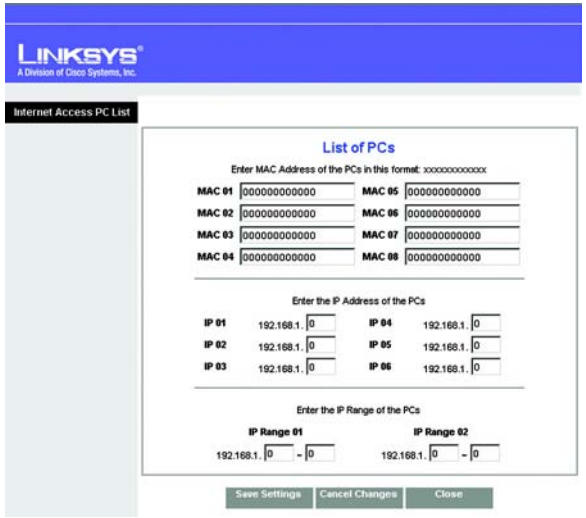


Abbildung 6-35: „List of PCs“ (PC-Liste)

Registerkarte „Applications & Gaming“ (Anwendungen und Spiele)

Registerkarte „Single Port Range Forwarding“ (Einfache Anschlussweiterleitung)

Verwenden Sie das Fenster *Single Port Range Forwarding* (Einfache Anschlussweiterleitung), wenn ein bestimmter Port geöffnet werden soll, damit Benutzer im Internet die Server hinter dem Gateway erkennen können (zu diesen Servern zählen u. a. FTP- oder E-Mail-Server). Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden Computer weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein; darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

„Single Port Forwarding“ (Einfache Anschlussweiterleitung)

- **Application** (Anwendung): Geben Sie den Namen der Anwendung im entsprechenden Feld ein.
- **External Port** (Externer Port) und **Internal Port** (Interner Port): Geben Sie die Nummern für den externen und internen Port ein.
- **Protocol** (Protokoll): Wählen Sie das Protokoll aus, das Sie für jede Anwendung verwenden möchten: **TCP** oder **UDP**.
- IP-Adresse: Geben Sie die IP-Adresse des entsprechenden Computers ein.
- **Enabled** (Aktiviert): Klicken Sie auf **Enabled** (Aktiviert), um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

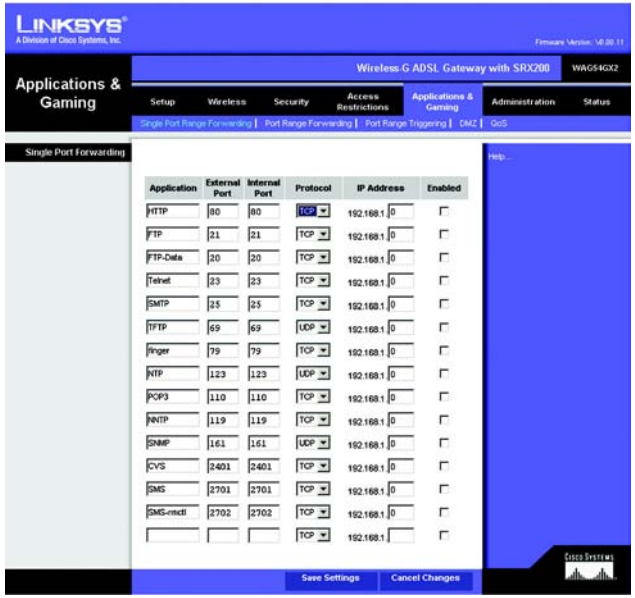


Abbildung 6-36: „Single Port Forwarding“ (Einfache Anschlussweiterleitung)

Registerkarte „Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich)

Im Fenster *Port Range Forwarding* (Weiterleitung an einen Anschlussbereich) können Sie öffentliche Dienste im Netzwerk festlegen, z. B. Web-, FTP-, E-Mail-Server oder andere spezielle Internetanwendungen. (Unter speziellen Internet-Anwendungen versteht man alle Anwendungen, die über den Internetzugang Funktionen wie z. B. Videokonferenzen oder Internet-Spiele ausführen. Bei einigen Internetanwendungen ist keine Weiterleitung erforderlich.)

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden Computer weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein; darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

„Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich)

- **Application** (Anwendung): Geben Sie den Namen der Anwendung im entsprechenden Feld ein.
- **Start** (Von) und **End** (Bis): Geben Sie die Anfangs- und Endnummern des Anschlussbereichs ein, der weitergeleitet werden soll.
- **Protocol** (Protokoll): Wählen Sie das Protokoll aus, das Sie für jede Anwendung verwenden möchten: **TCP**, **UDP** oder **Both** (Beide).
- „IP Address“ (IP-Adresse): Geben Sie die IP-Adresse des entsprechenden Computers ein.
- **Enable** (Aktivieren): Aktivieren Sie das Kontrollkästchen **Enable** (Aktivieren), um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

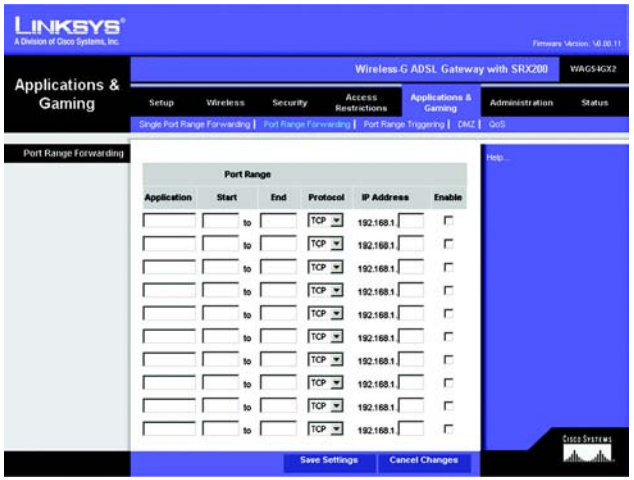


Abbildung 6-37: „Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich)

Registerkarte „Port Range Triggering“ (Anschlussbereich-Triggering)

Anschlussbereich-Triggering wird bei speziellen Anwendungen verwendet, über die ein Port auf Anfrage geöffnet werden kann. Bei dieser Funktion überprüft das Gateway ausgehende Daten auf spezielle Port-Nummern. Das Gateway speichert die IP-Adresse des Computers, der Daten zur Übertragung abruft. Wenn die abgerufenen Daten über das Gateway übertragen werden, werden die Daten über IP-Adresse und Port-Mapping-Regeln dem richtigen Computer weitergeleitet.

„Port Range Triggering“ (Anschlussbereich-Triggering)

- **Application** (Anwendung): Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Triggering Range** (Triggering-Bereich): Geben Sie die Anfangs- und Endnummern der Ports für den Triggering-Bereich ein.
- **Forwarded Range** (Weiterleitungsbereich): Geben Sie die Anfangs- und Endnummern der Ports für den Weiterleitungsbereich ein.
- **Enabled** (Aktiviert): Aktivieren Sie das Kontrollkästchen **Enabled** (Aktiviert), um das Anschlussbereich-Triggering für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-38: „Port Rage Triggering“ (Anschlussbereich-Triggering)

Registerkarte „DMZ“

Über das Fenster *DMZ* kann mithilfe von DMZ-Hosting für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser spezielle Dienste (z. B. Internet-Spiele und Videokonferenzen) nutzen kann. Mit DMZ-Hosting werden alle Ports gleichzeitig an einen PC weitergeleitet, im Unterschied zu **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich), bei dem nur maximal 10 Anschlussbereiche weitergeleitet werden können.

DMZ

- **DMZ Hosting** (DMZ-Hosting): Mit der DMZ-Funktion (*Demilitarized Zone*, entmilitarisierte Zone) kann für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser spezielle Dienste (z. B. Internet-Spiele oder Videokonferenzen) nutzen kann.ann.ann. Klicken Sie auf **Enable** (Aktivieren), um diese Funktion zu verwenden. Klicken Sie auf **Disable** (Deaktivieren), um die DMZ-Funktion zu deaktivieren.

- **DMZ Host IP Address** (IP-Adresse des DMZ-Hosts): Um einen Computer mit dem Internet zu verbinden, geben Sie die IP-Adresse des Computers ein. Weitere Informationen zum Ermitteln der IP-Adresse eines Computers finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-39: DMZ

Registerkarte „QoS“

QoS (Quality of Service)

QoS sorgt bei Netzwerkverkehr mit hoher Priorität, beispielsweise bei anspruchsvollen Echtzeitanwendungen wie Internettelefonie oder Videokonferenzen, für besseren Service.

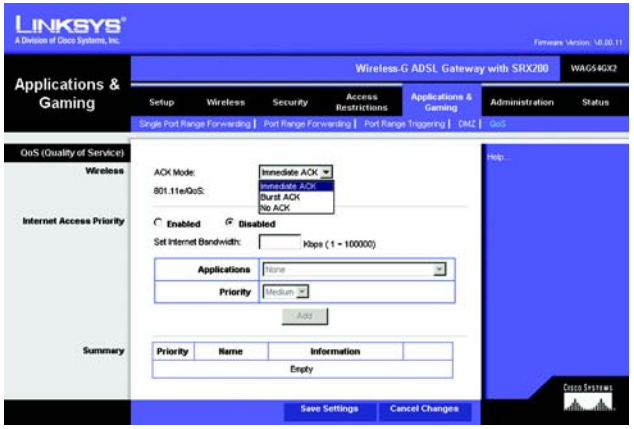


Abbildung 6-40: QoS

Wireless

- **ACK Mode** (ACK-Modus): Bei dieser Einstellung ist QoS für Benutzer priorisiert, bei denen auch der ACK-Modus aktiviert ist. Benutzer, bei denen die Option für das unmittelbare ACK-Signal aktiviert ist (Standardeinstellung), erzielen zuverlässige Verbindungen für die normale Nutzung des Netzwerks. Das diskontinuierliche ACK-Signal ist schneller, jedoch weniger zuverlässig, und kann sich negativ auf die Leistung im Wireless-Betrieb mit großer Reichweite auswirken. Die Einstellung **No ACK** (Kein ACK-Signal) deaktiviert die ACK-Funktion. Bei Clients mit ACK-Signal muss der Wireless-Adapter dieselbe Einstellung erhalten wie das Gateway. Dies ist in der Regel bei Multicast-Übertragungen wie Video der Fall. Diese Funktion sollten Sie nur als fortgeschrittener Benutzer verwenden.

- **802.11e/QoS**: QoS ist standardmäßig aktiviert, um so die bestmögliche Leistung für die Wireless-Verbindung zu erzielen. Bei einem gemischten Wireless-Netzwerk können Sie mit der Option **Disable** (Deaktivieren) die Leistungen noch verbessern.

Internet Access Priority (Priorität für Internetzugriff)

In diesem Bereich können Sie die Priorität auf Basis von Anwendung, Anschlussbereich oder MAC-Adresse festlegen. Es stehen vier Einstellungen für die Priorität zur Auswahl: **High** (Hoch), **Medium** (Mittel), **Normal** und **Low** (Niedrig).

- **Enable/Disable** (Aktivieren/Deaktivieren): Um die ausgehende Bandbreite für die verwendeten QoS-Richtlinien einzuschränken, wählen Sie die Option **Enabled** (Aktiviert) aus. Andernfalls wählen Sie **Disabled** (Deaktiviert) aus.

- **Set Internet Bandwidth** (Internetbandbreite einstellen): Mit dieser Einstellung können Sie die ausgehende Bandbreite für die verwendeten QoS-Richtlinien einschränken. Auf diese Weise können Sie steuern, wie viel Bandbreite eine bestimmte Anwendung verwenden darf. Geben Sie in dieses Feld die Bandbreite ein.

- **Application** (Anwendung): Hier stehen die Optionen **None** (Keine), **Online Game** (Online-Spiel), **MSN Messenger**, **YAHOO Messenger**, **Skype**, **Voice Device** (Sprachgerät) und **Add a New Application** (Neue Anwendung hinzufügen) zur Verfügung; außerdem können Sie aus einer Liste von Anwendungen auswählen. Um einen neuen Eintrag anzulegen, wählen Sie **Add a New Application** (Neue Anwendung hinzufügen), und beachten Sie den Bereich *Add a New Application* (Neue Anwendung hinzufügen).

- **Priority** (Priorität): Wählen Sie die Option **High** (Hoch), **Medium** (Mittel), **Normal** oder **Low** (Niedrig) für die Bandbreitenpriorität, die für die ausgewählte Anwendung erforderlich ist. Legen Sie nicht bei allen Anwendungen die Option **High** (Hoch) fest, weil hierdurch der Sinn und Zweck einer Zuweisung der verfügbaren Bandbreite aufgehoben würde. Soll die Bandbreite unter dem normalen Wert liegen, wählen Sie **Low** (Niedrig). Je nach Anwendung sind mehrere Versuche notwendig, um die passende Bandbreitenpriorität zu ermitteln. Klicken Sie abschließend auf **Add** (Hinzufügen), um den Eintrag in die Liste **Summary** (Zusammenfassung) aufzunehmen.

Online Game (Online-Spiel)

Mit der Option **Online Game** (Online-Spiel) öffnen Sie das Dropdown-Menü *Select a Game* (Spiel auswählen), in dem einige gängige, vorkonfigurierte Spiele aufgeführt sind. Wählen Sie das gewünschte Spiel in der Liste aus, und legen Sie die zugehörige Priorität fest.

MSN Messenger

Wählen Sie die Priorität in der Dropdown-Liste aus, und klicken Sie auf **Add** (Hinzufügen).

YAHOO Messenger

Wählen Sie die Priorität in der Dropdown-Liste aus, und klicken Sie auf **Add** (Hinzufügen).

Skype

Wählen Sie die Priorität in der Dropdown-Liste aus, und klicken Sie auf **Add** (Hinzufügen).

Voice Device (Sprachgerät)

Geben Sie in das Feld *Enter a Name* (Name eingeben) den Namen des Netzwerkgeräts ein, geben Sie die MAC-Adresse an, wählen Sie die Priorität in der Dropdown-Liste aus, und klicken Sie auf **Add** (Hinzufügen).

Add a New Application (Neue Anwendung hinzufügen)

Enter a Name (Name eingeben) — Geben Sie einen Namen für den Eintrag ein.

Category (Kategorie) — Wählen Sie die Option **Port Range** (Anschlussbereich) oder **MAC Address** (MAC-Adresse) für das Gateway, über das die Bandbreitenpriorität festgelegt werden soll.

Port Range (Anschlussbereich) — Wenn Sie die Option **Port Range** (Anschlussbereich) ausgewählt haben, steht diese Kategorie zur Verfügung. Hiermit können Sie den oder die Anschlussbereiche festlegen, die von der Anwendung genutzt werden sollen. Um beispielsweise die Bandbreite für FTP zuzuweisen, geben Sie **21-21** ein. Wenn Dienste für eine Anwendung benötigt werden, die auf Anschlüsse zwischen 1000 und 1250 zugreift, geben Sie entsprechend **1000-1250** ein. Zulässige Werte für die Anschlussnummern sind 1 bis 65535. Weitere Informationen zu den verwendeten Dienst-Ports finden Sie in der Dokumentation zur jeweiligen Anwendung.

Abbildung 6-41: QoS – „Online Game“ (Online-Spiel)

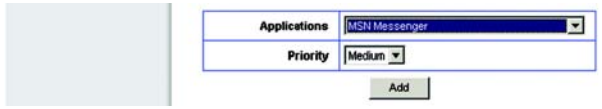


Abbildung 6-42: QoS – MSN Messenger

Abbildung 6-43: QoS – „Voice Device“ (Sprachgerät)

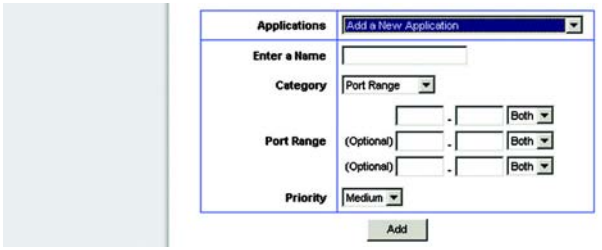


Abbildung 6-44: QoS – „Add a New Application“ (Neue Anwendung hinzufügen) – „Port Range“ (Anschlussbereich)

Sie können bis zu drei Bereiche für diese Bandbreitenzuweisung definieren. Legen Sie für die einzelnen Anschlussbereiche jeweils den oder die Protokolltyp(en) fest: **TCP**, **UDP** oder **Both** (Beide).

MAC Address (MAC-Adresse) Wenn Sie die Option **MAC Address** (MAC-Adresse) ausgewählt haben, steht diese Kategorie zur Verfügung. Geben Sie die zwölfstellige hexadezimale MAC-Adresse für das Gerät ein, das als Bandbreitenpriorität festgelegt werden soll. Diese Angabe bildet eine eindeutige ID für das Netzwerkgerät. Sobald das eingegebene Gerät im Gateway erkannt wird, erhält es die Priorität, die für den zugehörigen Eintrag eingestellt wurde. Weitere Informationen zum Abrufen der MAC-Adresse finden Sie in der Dokumentation zum Gerät.

Priority (Priorität) Legen Sie die Bandbreitenpriorität für die ausgewählte Anwendung fest. Für die Bandbreite stehen die Optionen **High** (Hoch), **Medium** (Mittel), **Normal** und **Low** (Niedrig) zur Auswahl; stellen Sie jedoch nicht alle Anwendungen auf **High** (Hoch) ein. Klicken Sie abschließend auf **Add** (Hinzufügen), um den Eintrag in die Liste **Summary** (Zusammenfassung) aufzunehmen.

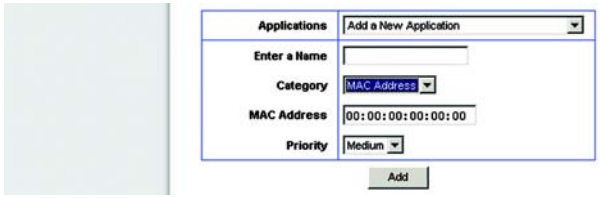


Abbildung 6-45: QoS – „Add a New Application“ (Neue Anwendung hinzufügen) – „MAC Address“ (MAC-Adresse)

„Summary“ (Zusammenfassung)

Priority (Priorität) Hier wird die Priorität für die Bandbreitenzuweisung angezeigt, die Sie für die Anwendung festgelegt haben, und zwar **High** (Hoch), **Medium** (Mittel), **Normal** oder **Low** (Niedrig).

Name Hier wird der Name der Anwendung angezeigt (bzw. die Einträge), die für die Zuweisung angegeben wurde.

Information (Informationen) Hier wird der Anschlussbereich oder die MAC-Adresse angezeigt, die Sie beim Hinzufügen einer neuen Anwendung eingegeben haben. Bei vorkonfigurierten Anwendungen wird in diesem Bereich kein gültiger Eintrag aufgeführt.

Remove (Entfernen) Mit dieser Schaltfläche können Sie den Eintrag einer Anwendung entfernen. Soll der Eintrag gelöscht werden, klicken Sie auf die Schaltfläche **Remove** (Entfernen). Zum Speichern der Konfiguration klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern). Um Ihre Änderungen zu verwerfen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „Administration“ (Verwaltungsfunktionen)

Registerkarte „Management“ (Verwaltungsfunktionen)

Über das Fenster *Management* (Verwaltungsfunktionen) können Sie die Einstellungen für den Gateway-Zugriff sowie die Verwaltungsfunktionen für SNMP (*Simple Network Management Protocol*), UPnP (*Universal Plug and Play*) und WLAN ändern.

„Gateway Access“ (Gateway-Zugriff)

Local Gateway Access (Lokaler Gateway-Zugriff): Um die Sicherheit des Gateways zu gewährleisten, werden Sie beim Zugriff auf das webbasierte Dienstprogramm des Gateways zur Eingabe Ihres Passworts aufgefordert. Der Standardbenutzername und das Standardpasswort lauten **admin**.

- **Gateway Userlist** (Gateway-Benutzerliste): Wählen Sie die Nummer des Benutzers im Dropdown-Menü aus.
- **Gateway Username** (Gateway-Benutzername): Geben Sie den Standardbenutzernamen **admin** ein. Es wird empfohlen, dass Sie den Standardbenutzernamen in einen persönlichen Benutzernamen ändern.
- **Gateway Password** (Gateway-Passwort): Es empfiehlt sich, das Standardpasswort **admin** in ein Passwort Ihrer Wahl zu ändern.
- **Re-enter to confirm** (Zur Bestätigung erneut eingeben): Geben Sie das neue Gateway-Passwort erneut ein, um es zu bestätigen.

Remote Gateway Access (Remote-Gateway-Zugriff): Mit dieser Funktion können Sie auf das Gateway von einem entfernten Standort aus über das Internet zugreifen.

- **Remote Management** (Remote-Verwaltung): Mit dieser Funktion können Sie das Gateway von einem Remote-Standort über das Internet verwalten. Klicken Sie zum Aktivieren von **Remote Management** (Remote-Verwaltung) auf **Enable** (Aktivieren).

WICHTIG: Durch Aktivieren der Option **Remote Management** (Remote-Verwaltung) kann jeder Benutzer, der Ihr Passwort kennt, von jedem beliebigen Standort im Internet das Gateway konfigurieren.

- **Management Port** (Management-Port): Geben Sie die Anschlussnummer ein, die Sie für den entfernten Zugriff auf das Gateway verwenden möchten.

Abbildung 6-46: „Management“ (Verwaltungsfunktionen)

SNMP

SNMP ist ein häufig verwendetes Protokoll zur Netzwerküberwachung und -verwaltung.

- **Device Name** (Gerätename): Geben Sie den Namen des Gateways ein.
- **SNMP**: Klicken Sie zur Verwendung von SNMP auf **Enable** (Aktivieren). Klicken Sie auf **Disabled** (Deaktiviert), um SNMP zu deaktivieren.
- **Get Community** (Get-Gemeinschaft): Geben Sie das Passwort ein, mit dem ein schreibgeschützter Zugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Set Community** (Set-Gemeinschaft): Geben Sie das Passwort ein, mit dem ein Schreib-/Lesezugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Trap Management: Trap to** (Trap-Verwaltung: Trap-Ziel): Geben Sie die IP-Adresse des entfernten Host-Computers ein, der die Trap-Nachrichten erhalten wird.

UPnP

Mit UPnP kann das Gateway unter Windows ME und XP automatisch für verschiedene Internetanwendungen (z. B. Internet-Spiele oder Videokonferenzen) konfiguriert werden.

- **UPnP**: Klicken Sie zur Verwendung von UPnP auf **Enable** (Aktivieren). Klicken Sie andernfalls auf **Disable** (Deaktivieren).

WLAN

- **Management via WLAN** (Verwaltung über WLAN): Mit dieser Funktion kann das Gateway über einen Wireless-Computer des lokalen Netzwerks verwaltet werden, wenn sich dieser beim webbasierten Dienstprogramm des Gateways anmeldet. Klicken Sie zum Aktivieren dieser Funktion auf **Enable** (Aktivieren). Klicken Sie andernfalls auf **Disable** (Deaktivieren).

IGMP

- **IGMP Proxy** (IGMP-Proxy): Wenn die Multimediaanwendung oder das Gerät hinter dem Gateway nicht ordnungsgemäß funktioniert, können Sie mit der IGMP-Proxy-Funktion den Multicast-Datenverkehr durch das Gateway zulassen. Klicken Sie zur Verwendung dieser Funktion auf **Enable** (Aktivieren). Klicken Sie andernfalls auf **Disable** (Deaktivieren).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „Reporting“ (Berichtaufzeichnung)

Im Fenster *Reporting* (Berichtaufzeichnung) wird ein Protokoll angezeigt, in dem alle eingehenden und ausgehenden URLs bzw. IP-Adressen für die Internetverbindung aufgeführt sind. Über diese Registerkarte stehen auch Protokolle für VPN- und Firewall-Ereignisse zur Verfügung.

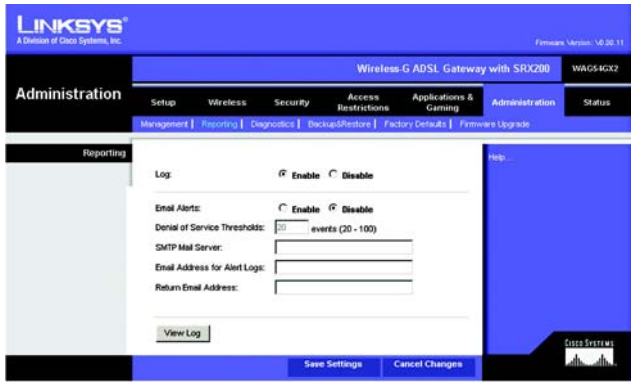


Abbildung 6-48: „Reporting“ (Berichtaufzeichnung)

„Reporting“ (Berichtaufzeichnung)

- **Log** (Protokoll): Klicken Sie zur Verwendung der Berichtaufzeichnung auf **Enable** (Aktivieren).

„Email Alerts“ (E-Mail-Warnungen)

- **Email Alerts** (E-Mail-Warnungen): Klicken Sie auf die Option **Enable** (Aktivieren), um E-Mail-Warnungen zu verwenden.
- **Denial of Service Thresholds** (DoS-Schwellwerte): Geben Sie die Anzahl der DoS-Angriffe (*Denial of Service*) ein, durch die eine E-Mail-Warnung ausgelöst werden soll.
- **SMTP Mail Server** (SMTP-Mailserver): Geben Sie die IP-Adresse des SMTP-Servers ein.
- **E-Mail Address for Alert Logs** (E-Mail-Adresse für Warnungsprotokolle): Geben Sie die E-Mail-Adresse ein, an die Warnungsprotokolle gesendet werden sollen.
- **Return E-Mail address** (E-Mail-Antwortadresse): Geben Sie die Antwortadresse für die E-Mail-Warnungen ein.

Wenn Sie die Protokolle anzeigen möchten, klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen). Es wird ein neues Fenster angezeigt. Wählen Sie im Dropdown-Menü das anzuzeigende Protokoll aus: **ALL** (ALLE), **Access Log** (Zugriffsprotokoll) oder **Firewall Log** (Firewall-Protokoll). Klicken Sie auf die Schaltfläche **pageRefresh** (Seite aktualisieren), um die Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Clear** (Löschen), um die Protokollinformationen zu löschen. Klicken Sie auf die Schaltfläche **Previous Page** (Vorherige Seite), um zur vorherigen Informationsseite zu wechseln. Klicken Sie auf die Schaltfläche **Next Page** (Nächste Seite), um zur nächsten Informationsseite zu wechseln.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

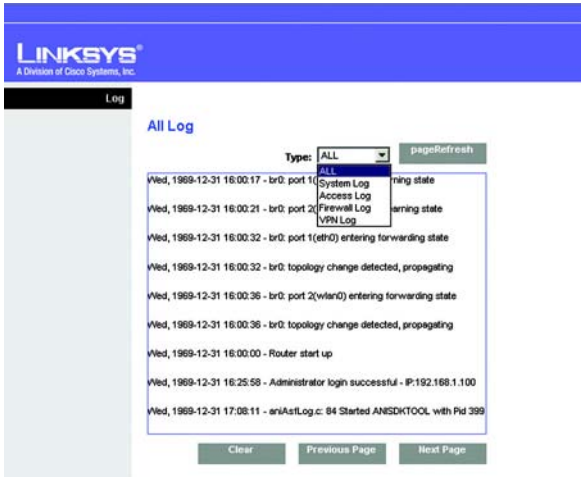


Abbildung 6-49: „System Log“ (Systemprotokoll)

Registerkarte „Diagnostics“ (Diagnose)

In diesem Fenster können Sie Ping-Tests durchführen und die Testergebnisse anzeigen.

„Ping Test“ (Ping-Test)

Ping Test Parameters (Ping-Test-Parameter)

- **Ping Target IP** (Ping-Ziel-IP-Adresse): Geben Sie die IP-Adresse ein, für die Pings durchgeführt werden sollen. Dies kann eine lokale IP-Adresse (LAN) oder eine Internet-IP-Adresse (WAN) sein.
- **Ping Size** (Ping-Größe): Geben Sie die Größe des Pakets an.
- **Number of Pings** (Anzahl der Pings): Geben Sie die Anzahl der Pings an, die durchgeführt werden soll.
- **Ping Interval** (Ping-Intervall): Geben Sie das Ping-Intervall (wie oft Pings für die Ziel-IP-Adresse durchgeführt werden sollen) in Millisekunden ein.
- **Ping Timeout** (Ping-Wartezeit): Geben Sie die Ping-Wartezeit (Zeitraum, nach dem der Ping-Test abläuft) in Millisekunden ein.

Klicken Sie auf die Schaltfläche **Start Test** (Test starten), um den Ping-Test zu starten.

- **Ping Result** (Ping-Ergebnisse): In dieser Zeile werden die Ergebnisse des Ping-Tests angezeigt.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-50: „Diagnostics“ (Diagnose)

Registerkarte „Backup & Restore“ (Sichern & Wiederherstellen)

Auf der Registerkarte **Backup & Restore** (Sichern & Wiederherstellen) können Sie eine Sicherungskopie der Konfigurationsdatei des Gateways erstellen und diese wiederherstellen.

„Backup Configuration“ (Konfiguration sichern)

Klicken Sie zum Erstellen einer Sicherungskopie der Konfigurationsdatei des Gateways auf die Schaltfläche **Backup** (Sichern). Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Abbildung 6-51: „Backup&Restore“ (Sichern & Wiederherstellen)

„Restore Configuration“ (Konfiguration wiederherstellen)

Klicken Sie zum Wiederherstellen der Konfigurationsdatei des Gateways auf die Schaltfläche **Browse** (Durchsuchen). Befolgen Sie dann die Anweisungen auf dem Bildschirm, um nach der Datei zu suchen. Klicken Sie nach Auswahl der Datei auf die Schaltfläche **Restore** (Wiederherstellen).

Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „Factory Defaults“ (Werkseinstellungen)

In diesem Fenster können Sie die Werkseinstellungen des Gateways wiederherstellen.

„Factory Defaults“ (Werkseinstellungen)

Restore Factory Defaults (Werkseinstellungen wiederherstellen): Wenn Sie das Gateway auf die Werkseinstellungen zurücksetzen möchten (Ihre Einstellungen gehen dabei verloren), klicken Sie auf **Restore Factory Defaults** (Werkseinstellungen wiederherstellen). Befolgen Sie dann die Anweisungen auf dem Bildschirm. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-52: „Factory Defaults“ (Werkseinstellungen)

Registerkarte „Firmware Upgrade“ (Aktualisieren der Firmware)

In diesem Fenster können Sie die Firmware des Gateways aktualisieren.

„Firmware Upgrade“ (Aktualisieren der Firmware)

So aktualisieren Sie die Gateway-Firmware:

1. Laden Sie die Aktualisierungsdatei für die Gateway-Firmware unter www.linksys.com/international herunter.
2. Extrahieren Sie die Datei auf dem Computer.
3. Klicken Sie im Fenster *Firmware Upgrade* (Firmware aktualisieren) auf die Schaltfläche **Browse** (Durchsuchen), um die Firmware-Aktualisierungsdatei zu suchen.
4. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben.
5. Klicken Sie auf die Schaltfläche **Start to Upgrade** (Aktualisierung starten), und befolgen Sie die Anweisungen auf dem Bildschirm.

Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-53: „Firmware Upgrade“ (Aktualisieren der Firmware)

Registerkarte „Status“

Registerkarte „Gateway“

In diesem Fenster werden Informationen zum Gateway und zur entsprechenden Internetverbindung angezeigt.

„Gateway Information“ (Gateway-Informationen)

In diesem Bereich wird die Version der Gateway-Firmware, die MAC-Adresse und die aktuelle Uhrzeit angezeigt.

„Internet Connection“ (Internetverbindung)

In diesem Bereich werden folgende Informationen angezeigt: **Login Type** (Anmeldetyp), **Interface** (Schnittstelle), **IP Address** (IP-Adresse), **Subnet Mask** (Subnetzmaske), **Default Gateway** (Standard-Gateway) und die IP-Adressen für die DNS-Server 1 bis 3.

Abbildung 6-54: Gateway

DHCP Renew (DHCP erneuern): Klicken Sie auf die Schaltfläche **DHCP Renew** (DHCP erneuern), sofern diese angezeigt wird, um die aktuelle IP-Adresse des Gateways durch eine neue IP-Adresse zu ersetzen.

DHCP Release (DHCP löschen): Klicken Sie auf die Schaltfläche **DHCP Release** (DHCP löschen), sofern diese angezeigt wird, um die aktuelle IP-Adresse des Gateways zu löschen.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Registerkarte „Local Network“ (Lokales Netzwerk)

In diesem Fenster werden Informationen zum lokalen Netzwerk des Gateways angezeigt.

„Local Network“ (Lokales Netzwerk)

In diesem Fenster wird Folgendes angezeigt: die lokale MAC-Adresse, die IP-Adresse, die Subnetzmaske, der DHCP-Server sowie die erste und die letzte IP-Adresse.

Klicken Sie zum Anzeigen der DHCP-Client-Tabelle auf die Schaltfläche **DHCP Client Table** (DHCP-Client-Tabelle). Klicken Sie zum Anzeigen der ARP/RARP-Tabelle auf die Schaltfläche **ARP/RARP Table** (ARP/RARP-Tabelle).

DHCP Client Table (DHCP-Client-Tabelle): Im Bereich **DHCP Active IP Table** (DHCP – Tabelle zur aktiven IP-Adresse) werden die aktuellen DHCP-Client-Daten angezeigt. Zu diesen Angaben zählen der Computername, die IP-Adresse, die MAC-Adresse und der Zeitpunkt, zu dem die dynamische IP-Adresse für Clients abläuft, die den DHCP-Server verwenden. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Um einen Client vom DHCP-Server zu löschen, wählen Sie den entsprechenden Client aus, und klicken Sie anschließend auf die Schaltfläche **Delete** (Löschen). Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Local Network* (Lokales Netzwerk) zurückzukehren.

ARP/RARP Table (ARP/RARP-Tabelle): Bei einer ARP-Anfrage handelt es sich um eine Anfrage, mit der das Gateway die MAC-Adressen von Clients mit IP-Adressen anfragt, um IP-Adressen den entsprechenden MAC-Adressen zuordnen zu können. Bei RARP geht der Vorgang im Vergleich zu ARP umgekehrt vonstatten. Die ARP/RARP-Tabelle enthält die aktuellen Daten für das lokale Netzwerk des Gateways. Es werden die entsprechenden IP-Adressen und MAC-Adressen aufgeführt. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Local Network* (Lokales Netzwerk) zurückzukehren.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

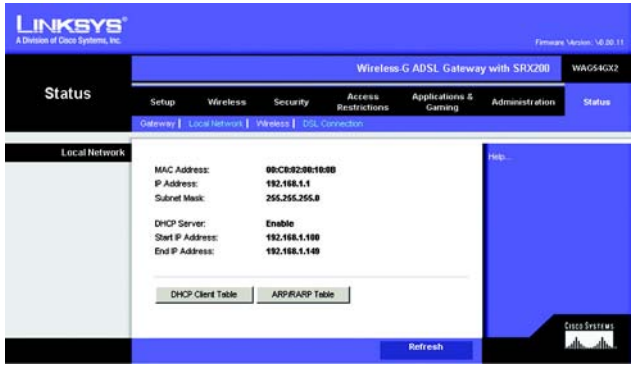


Abbildung 6-55: „Local Network“ Lokales Netzwerk

Abbildung 6-56: DHCP – „DHCP Active IP Table“ (Tabelle zur aktiven IP-Adresse)

Abbildung 6-57: „ARP/RARP Table“ (ARP/RARP-Tabelle)

Registerkarte „Wireless“

In diesem Fenster werden Informationen zum Wireless-Netzwerk des Gateways angezeigt.

Wireless

Dieses Fenster enthält folgende Angaben: die Versionsnummer der Wireless-Firmware, die MAC-Adresse, den Modus, die SSID, den Kanal und die Verschlüsselungsoption.

Klicken Sie auf die Schaltfläche **Wireless Clients Connected** (Angeschlossene Wireless-Clients), um eine Liste der Wireless-Clients anzuzeigen, die an das Gateway angeschlossen sind. Gleichzeitig werden die entsprechenden Computernamen, IP-Adressen und MAC-Adressen angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Wireless* zurückzukehren.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

Abbildung 6-58: Wireless

Abbildung 6-59: „Networked Computers“ (Netzwerk-Computer)

Registerkarte „DSL Connection“ (DSL-Verbindung)

In diesem Fenster sind Informationen zur DSL-Verbindung aufgeführt.

„DSL Status“ (DSL-Status)

Dieser Bereich enthält folgende Angaben: Status sowie Downstream- und Upstream-Rate.

„PVC Connection“ (PVC-Verbindung)

In diesem Bereich werden folgende Informationen angezeigt: **Encapsulation** (Kapselungstyp), **Multiplexing**, **QoS**, **Pcr Rate** (PCR-Rate), **Scr Rate** (SCR-Rate), **Autodetect** (automatische Erkennung), **VPI**, **VCI**, **Enable Status** (Aktivierungsstatus) und **PVC Status** (PVC-Status).

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

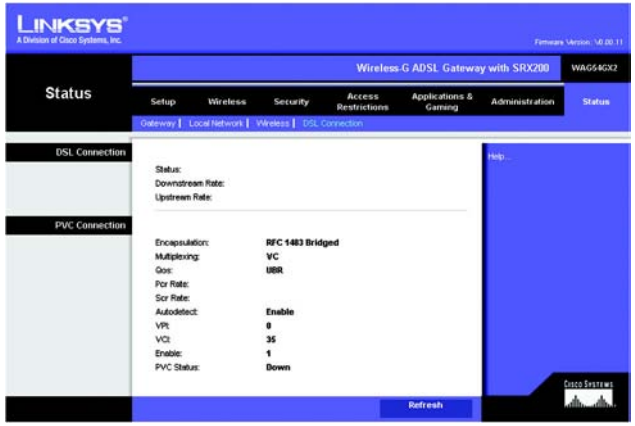


Abbildung 6-60: „DSL Connection“ (DSL-Verbindung)

Anhang A: Fehlerbehebung

Dieser Anhang besteht aus zwei Teilen: „Behebung häufig auftretender Probleme“ und „Häufig gestellte Fragen“. Er enthält Lösungsvorschläge zu Problemen, die während der Installation und des Betriebs des Gateways auftreten können. Lesen Sie sich zur Fehlerbehebung die unten aufgeführten Beschreibungen durch. Wenn hier kein Lösungsvorschlag zu Ihrem Problem aufgeführt ist, finden Sie weitere Informationen auf der Website von Linksys unter www.linksys.com/international.

Behebung häufig auftretender Probleme

1. ***Wie lege ich eine statische IP-Adresse auf einem Computer fest?***
   Führen Sie die folgenden Schritte aus, um einem Computer eine statische IP-Adresse zuzuweisen:
   - Für Benutzer von Windows 98 und ME:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf die Option **Netzwerk**.
     2. Wählen Sie im Feld *Die folgenden Netzwerkkomponenten sind installiert* die mit dem Ethernet-Adapter verbundene Option **TCP/IP->** aus. Falls nur ein Ethernet-Adapter installiert ist, wird nur in einer Zeile **TCP/IP** ohne Verknüpfung mit einem Ethernet-Adapter aufgeführt. Wählen Sie den Eintrag aus, und klicken Sie auf die Schaltfläche **Eigenschaften**.
     3. Wählen Sie im Fenster für die TCP/IP-Eigenschaften auf der Registerkarte **IP-Adresse** die Option **IP-Adresse festlegen** aus. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird. Vergewissern Sie sich, dass für jeden Computer bzw. jedes Netzwerkgerät eine eindeutige IP-Adresse verwendet wird.
     4. Klicken Sie auf die Registerkarte **Gateway**, und geben Sie **192.168.1.1** ein, wenn die Eingabeaufforderung für das neue Gateway angezeigt wird (dies ist die Standard-IP-Adresse für das Gateway). Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Eingabe zu übernehmen.
     5. Klicken Sie auf die Registerkarte **DNS**, und stellen Sie sicher, dass DNS aktiviert ist. Geben Sie den Host- und den Domänenname ein (z. B. „Johann“ als Hostname und „home“ als Domänenname). Geben Sie den DNS-Eintrag ein, den Sie von Ihrem ISP erhalten haben. Falls Sie keine DNS-IP-Adresse von Ihrem ISP erhalten haben, wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
     6. Klicken Sie im Fenster für die TCP/IP-Eigenschaften auf **OK**, und klicken Sie anschließend auf die Schaltfläche **Schließen** bzw. die Schaltfläche **OK**, um das Fenster **Netzwerk** zu schließen.
     7. Wenn Sie dazu aufgefordert werden, starten Sie den Computer neu.
   - Für Benutzer von Windows 2000:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.

2. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
3. Wählen Sie im Feld *Aktivierte Komponenten werden von dieser Verbindung verwendet* die Option **Internetprotokoll (TCP/IP)** aus, und klicken Sie auf die Schaltfläche **Eigenschaften**. Wählen Sie die Option **Folgende IP-Adresse verwenden** aus.
4. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
5. Geben Sie für die Subnetzmaske den Eintrag **255.255.255.0** ein.
6. Geben Sie für das Standard-Gateway den Eintrag **192.168.1.1** ein (die Standard-IP-Adresse des Gateways).
7. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
8. Klicken Sie im Fenster *Internetprotokolleigenschaften (TCP/IP)* auf die Schaltfläche **OK** sowie im Fenster *Eigenschaften von LAN-Verbindung* auf die Schaltfläche **OK**.
9. Wenn Sie dazu aufgefordert werden, starten Sie den Computer neu.

- Für Benutzer von Windows XP:
  Die folgenden Anweisungen gelten, wenn Sie Windows XP mit der Standard-Benutzeroberfläche ausführen. Wenn Sie die klassische Benutzeroberfläche verwenden (bei der die Symbole und Menüs wie in vorherigen Windows-Versionen aussehen), befolgen Sie die Anweisungen für Windows 2000.
  1. Klicken Sie auf **Start** und **Systemsteuerung**.
  2. Klicken Sie auf das Symbol **Netzwerk- und Internetverbindungen** und dann auf **Netzwerkverbindungen**.
  3. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
  4. Wählen Sie im Feld *Diese Verbindung verwendet folgende Elemente* die Option **Internetprotokoll (TCP/IP)** aus. Klicken Sie auf die Schaltfläche **Eigenschaften**.
  5. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
  6. Geben Sie für die Subnetzmaske den Eintrag **255.255.255.0** ein.
  7. Geben Sie für das Standard-Gateway den Eintrag **192.168.1.1** ein (die Standard-IP-Adresse des Gateways).
  8. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
  9. Klicken Sie im Fenster *Internetprotokolleigenschaften (TCP/IP)* auf die Schaltfläche **OK**. Klicken Sie im Fenster *Eigenschaften von LAN-Verbindung* auf die Schaltfläche **OK**.

2. Ich möchte meine Internetverbindung prüfen.

A. Überprüfen Sie Ihre TCP/IP-Einstellungen.

Für Benutzer von Windows 98, ME, 2000 und XP:

- Weitere Informationen finden Sie in der Windows-Hilfe. Stellen Sie sicher, dass in den Einstellungen die Option **IP-Adresse automatisch beziehen** aktiviert ist.

Für Benutzer von Windows NT 4.0:

- Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf das Symbol **Netzwerk**.
- Klicken Sie auf die Registerkarte **Protokoll**, und doppelklicken Sie auf **TCP/IP-Protokoll**.
- Wenn das Fenster angezeigt wird, stellen Sie sicher, dass Sie den richtigen Adapter als Ihren Ethernet-Adapter und die Option **IP-Adresse von einem DHCP-Server beziehen** ausgewählt haben.
- Klicken Sie im Fenster mit den TCP/IP-Protokolleigenschaften auf die Schaltfläche **OK** und im Fenster **Netzwerk** auf die Schaltfläche **Schließen**.
- Wenn Sie dazu aufgefordert werden, starten Sie den Computer neu.

B. Öffnen Sie eine Eingabeaufforderung.

Für Benutzer von Windows 98 und ME:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld *Öffnen* die Zeichenfolge **command** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

Für Benutzer von Windows NT, 2000 und XP:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld *Öffnen* den Eintrag **cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**. Geben Sie an der Eingabeaufforderung die Zeichenfolge **ping 192.168.1.1** ein, und drücken Sie die Eingabetaste.
- Wenn Sie eine Antwort erhalten, kommuniziert der Computer mit dem Gateway.
- Wenn Sie KEINE Antwort erhalten, überprüfen Sie die Kabelverbindung, und stellen Sie sicher, dass in den TCP/IP-Einstellungen für den Ethernet-Adapter die Option **IP-Adresse automatisch beziehen** aktiviert ist.

C. Geben Sie an der Eingabeaufforderung die Zeichenfolge **ping** gefolgt von Ihrer Internet- bzw. WAN-IP-Adresse ein, und drücken Sie die Eingabetaste. Die Internet- bzw. WAN-IP-Adresse wird im Statusfenster des webbasierten Dienstprogramms des Gateways angezeigt. Beispiel: Wenn Ihre Internet- bzw. WAN-IP-Adresse 1.2.3.4 lautet, müssen Sie die Zeichenfolge **ping 1.2.3.4** eingeben und anschließend die Eingabetaste drücken.

- Wenn Sie eine Antwort erhalten, ist der Computer mit dem Gateway verbunden.
- Wenn Sie KEINE Antwort erhalten, geben Sie den Ping-Befehl an einem anderen Computer ein, um so sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

D. Geben Sie an der Eingabeaufforderung die Zeichenfolge **ping www.yahoo.com** ein, und drücken Sie die Eingabetaste.

- Wenn Sie eine Antwort erhalten, ist der Computer mit dem Internet verbunden. Wenn Sie KEINE Webseite öffnen können, geben Sie den Ping-Befehl an einem anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

- Wenn Sie KEINE Antwort erhalten, kann ein Verbindungsproblem vorliegen. Geben Sie den Ping-Befehl an einem anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

3. Mit meiner Internetverbindung erhalte ich keine IP-Adresse im Internet.

- Lesen Sie sich den oben aufgeführten Abschnitt „2. Ich möchte meine Internetverbindung prüfen“ durch, und überprüfen Sie anhand dessen Ihre Verbindung.
  1. Stellen Sie sicher, dass Sie die korrekten Einstellungen für die Internetverbindung verwenden. Wenden Sie sich an Ihren ISP, um die Art Ihrer Internetverbindung zu überprüfen: **RFC 1483 Bridged** (RFC 1483-Überbrückung), **RFC 1483 Routed** (RFC 1483-Weiterleitung), **RFC 2516 PPPoE**, **RFC 2364 PPPoA**, **Bridged Mode Only** (Nur Überbrückungsmodus) oder **IPoA**. Weitere Einzelheiten zu den Einstellungen für die Internetverbindung finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.
  2. Stellen Sie sicher, dass Sie das richtige Kabel verwenden. Überprüfen Sie, ob die LED **ADSL** des Gateways konstant leuchtet.
  3. Stellen Sie sicher, dass das an den Port **ADSL** des Gateways angeschlossene Kabel in den Splitter des ADSL-Anschlusses eingesteckt ist. Überprüfen Sie, ob auf der Statusseite des webbasierten Dienstprogramms des Gateways eine gültige IP-Adresse des ISP aufgeführt ist.
  4. Schalten Sie den Computer und das Gateway aus. Warten Sie 30 Sekunden, und schalten Sie dann das Gateway und den Computer wieder ein. Überprüfen Sie, ob im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Status** eine IP-Adresse angezeigt wird.

4. Ich kann nicht auf die Seite „Setup“ (Einrichtung) des webbasierten Dienstprogramms des Gateways zugreifen.

- Informationen zur Überprüfung einer ordnungsgemäßen Verbindung des Computers mit dem Gateway finden Sie unter „2. Ich möchte meine Internetverbindung prüfen“.
  1. Informationen zur Überprüfung, ob der Computer über eine IP-Adresse, eine Subnetzmaske, ein Gateway und einen DNS verfügt, finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
  2. Legen Sie eine statische IP-Adresse für de Computer fest. Weitere Informationen hierzu finden Sie unter „1. Wie lege ich eine statische IP-Adresse fest?“.
  3. Befolgen Sie die Anweisungen unter „10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?“.

5. Mein VPN (Virtual Private Network) funktioniert nicht über das Gateway.

Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf, und öffnen Sie die Registerkarte **Security** (Sicherheit). Stellen Sie sicher, dass Sie die Option **IPSec Passthrough** (IPSec-Passthrough) und/oder **PPTP Passthrough** (PPTP-Passthrough) aktiviert haben.

- VPNs, in denen IPSec mit der ESP-Authentifizierung (*Encapsulation Security Payload*, auch als Protokoll 50 bezeichnet) verwendet wird, funktionieren einwandfrei. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen. Je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.
- VPNs, in denen IPSec und AH (*Authentication Header*, auch als Protokoll 51 bezeichnet) verwendet werden, sind mit dem Gateway nicht kompatibel. Die Verwendung von AH ist aufgrund gelegentlicher Inkompatibilität mit dem NAT-Standard beschränkt.
- Ändern Sie die IP-Adresse des Gateways auf ein anderes Subnetz, sodass Konflikte zwischen der IP-Adresse des VPNs und Ihrer lokalen IP-Adresse vermieden werden. Wenn Ihr VPN-Server beispielsweise die IP-Adresse 192.168.1.X zuweist (wobei „X“ für eine Zahl zwischen 1 und 254 steht) und die IP-Adresse Ihres LANs 192.168.1.X lautet (wobei „X“ mit der in der IP-Adresse des VPNs verwendeten Zahl identisch ist), werden Informationen vom Gateway u. U. nicht richtig übertragen. Zur Problembehebung ändern Sie die IP-Adresse des Gateways in **192.168.2.1**. Ändern Sie die IP-Adresse des Gateways im webbasierten Dienstprogramm auf der Registerkarte **Setup** (Einrichtung).
- Wenn Sie einem Computer oder einem anderen Gerät in Ihrem Netzwerk eine statische IP-Adresse zugewiesen haben, müssen Sie diese IP-Adresse dementsprechend in **192.168.2.Y** (wobei „Y“ für eine Zahl zwischen 1 und 254 steht) ändern. Beachten Sie, dass jede IP-Adresse im Netzwerk eindeutig sein muss.
- Bei Ihrem VPN ist es u. U. erforderlich, dass Pakete für den UDP-Port 500 an den Computer übertragen werden, der mit dem IPSec-Server verbunden ist. Details hierzu finden Sie unter „7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internetanwendungen verwenden“.
- Weitere Informationen finden Sie auf der Website von Linksys unter www.linksys.com/international.

6. Wie richte ich einen Server hinter dem Gateway ein und gebe ihn für alle Benutzer frei?

Um einen Server als Web-, FTP- oder Mail-Server zu verwenden, muss Ihnen die jeweils verwendete Anschlussnummer bekannt sein. Beispiel: Port 80 (HTTP) wird für Webserver, Port 21 (FTP) für FTP-Server und Port 25 (SMTP-Ausgang) sowie Port 110 (POP3-Eingang) für Mail-Server verwendet. Weitere Informationen finden Sie in der Dokumentation des installierten Servers.

- Befolgen Sie die hier aufgeführten Schritte, um die Anschlussweiterleitung über das webbasierte Dienstprogramm des Gateways einzurichten. Im Folgenden finden Sie Anweisungen zum Einrichten von Web-, FTP- und Mailservern.
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
  2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
  3. Geben Sie den externen Anschlussbereich für den verwendeten Dienst an. Wenn Sie beispielsweise einen Webserver verwenden, legen Sie den Bereich zwischen 80 und 80 fest.
  4. Aktivieren Sie das zu verwendende Protokoll (TCP und/oder UDP).
  5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Port-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert **100** in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Enable** (Aktivieren). Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
Webserver	80 bis 80	X		192.168.1.100	X
FTP-Server	21 bis 21	X		192.168.1.101	X
SMTP (Ausgang)	25 bis25	X		192.168.1.102	X
POP3 (Eingang)	110 bis 110	X		192.168.1.102	X

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internetanwendungen verwenden.

Zum Verwenden von Online-Spielen oder Internetanwendungen ist i. d. R. keine Anschlussweiterleitung bzw. kein DMZ-Hosting notwendig. U. u. möchten Sie jedoch gelegentlich selbst Online-Spiele oder Internetanwendungen hosten. Dazu müssen Sie das Gateway so einrichten, dass eingehende Datenpakete oder Daten an einen bestimmten Computer geliefert werden. Dies trifft auch auf die verwendeten Internetanwendungen zu. Sie erhalten Informationen zu den zu verwendenden Anschlussdiensten auf der Website des betreffenden Online-Spiels bzw. der Anwendung, das bzw. die Sie verwenden möchten. Führen Sie diese Schritte aus, um ein Hosting für ein Online-Spiel auszuführen bzw. um eine bestimmte Internetanwendung zu verwenden:

1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
3. Geben Sie den externen Anschlussbereich für den verwendeten Dienst an. Um beispielsweise Unreal Tournament (UT) auszuführen, müssen Sie den Bereich von 7777 bis 27900 eingeben.
4. Aktivieren Sie das zu verwendende Protokoll (TCP und/oder UDP).
5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Port-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert **100** in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Enable** (Aktivieren). Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
UT	7777 bis 27900	X	X	192.168.1.100	X
Half-Life	27015 bis 27015	X	X	192.168.1.105	X
PCAnywhere	5631 bis 5631		X	192.168.1.102	X
VPN/IPSEC	500 bis 500		X	192.168.1.100	X

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

8. Weder Internetspiele, Internetserver noch Internetanwendungen funktionieren.

Falls Sie Schwierigkeiten haben, Internetspiele, -server und -anwendungen zu verwenden, verbinden Sie einen Computer über das DMZ (*DeMilitarized Zone*)-Hosting mit dem Internet. Diese Option ist verfügbar, wenn für eine Anwendung zu viele Ports erforderlich sind oder Sie nicht sicher sind, welchen Anschlussdienst Sie verwenden sollen. Stellen Sie sicher, dass alle Weiterleitungseinträge deaktiviert sind, um das DMZ-Hosting erfolgreich zu verwenden, da die Weiterleitung Vorrang vor dem DMZ-Hosting hat. (Mit anderen Worten: Für in das Gateway eingehende Daten werden zuerst die Weiterleitungseinstellungen überprüft. Falls die Daten von einer Port-Nummer eingehen, für die keine Anschlussweiterleitung aktiviert ist, sendet das Gateway die Daten an einen beliebigen Computer oder ein beliebiges Netzwerkgerät, der bzw. das für DMZ-Hosting festgelegt wurde.)

- Führen Sie folgende Schritte aus, um DMZ-Hosting festzulegen:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **DMZ** auf. Wählen Sie **Enabled** (Aktiviert) aus, und geben Sie die IP-Adresse des Computers ein.
  2. Überprüfen Sie die Seiten zur Anschlussweiterleitung, und deaktivieren bzw. entfernen Sie die Einträge zur Weiterleitung. Speichern Sie diese Informationen, falls Sie sie zu einem späteren Zeitpunkt verwenden möchten.
- Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

9. Ich habe das Passwort vergessen bzw. die Aufforderung zur Eingabe des Passworts wird jedes Mal angezeigt, wenn ich die Einstellungen für das Gateway speichere.

- Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste 10 Sekunden lang gedrückt halten. Wenn Sie immer noch bei jedem Speichern der Einstellungen zur Eingabe des Passworts aufgefordert werden, führen Sie die folgenden Schritte aus:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Geben Sie den Standardbenutzernamen und das Standardpasswort **admin** ein, und rufen Sie unter **Administration** (Verwaltung) die Registerkarte **Management** (Verwaltungsfunktionen) auf.
  2. Geben Sie im Feld für das Gateway-Passwort ein anderes Passwort ein. Geben Sie anschließend im zweiten Feld das gleiche Passwort ein, um es dadurch zu bestätigen.
  3. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern).

10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?

Wenn Sie Proxy-Einstellungen verwenden, müssen Sie diese auf Ihrem Computer deaktivieren. Da es sich bei dem Gateway um das Gateway für die Internetverbindung handelt, benötigt der Computer keine Proxy-Einstellungen für den Zugriff auf das Internet. Führen Sie die folgenden Anweisungen aus, um sicherzustellen, dass Sie keine Proxy-Einstellungen verwenden und der verwendete Browser direkt eine Verbindung mit dem LAN herstellt.

- Für Benutzer von Microsoft Internet Explorer 5.0 oder höher:
  1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Internetoptionen**.
  2. Klicken Sie auf die Registerkarte **Verbindungen**.
  3. Klicken Sie auf die Schaltfläche **LAN-Einstellungen**, und deaktivieren Sie alle aktivierten Optionen.
  4. Klicken Sie auf die Schaltfläche **OK**, um zum vorherigen Fenster zu wechseln.
  5. Aktivieren Sie die Option **Keine Verbindung wählen**. Dadurch werden alle Popup-Fenster für DFÜ-Verbindungen für PPPoE-Benutzer entfernt.

- Für Netscape 6 oder höher:
  1. Starten Sie **Netscape Navigator**, und klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**.
  2. Stellen Sie sicher, dass in diesem Fenster die Option **Direkte Verbindung zum Internet** ausgewählt ist.
  3. Schließen Sie alle Fenster, um den Vorgang zu beenden.

11. Ich muss das Gateway auf die Werkseinstellungen zurücksetzen, um den Vorgang noch einmal von vorn zu beginnen.

Halten Sie die Reset-Taste 10 Sekunden lang gedrückt. Dadurch werden die Interneteinstellungen, das Passwort, die Weiterleitungsfunktion sowie weitere Einstellungen des Gateways auf die Werkseinstellungen zurückgesetzt. Anders ausgedrückt: Das Gateway verwendet wieder die werkseitige Konfiguration.

12. Ich möchte die Firmware aktualisieren.

Um die Firmware zu aktualisieren und so die neuesten Funktionen zu erhalten, besuchen Sie die internationale Website von Linksys unter www.linksys.com/international, und laden Sie die neueste Firmware herunter.

- Führen Sie die folgenden Schritte aus:
  1. Wählen Sie auf der internationalen Website von Linksys unter http://www.linksys.com/international Ihre Region bzw. Ihr Land aus.
  2. Klicken Sie auf die Registerkarte **Produkt**, und wählen Sie das Gateway aus.
  3. Klicken Sie auf der Website des Gateways auf **Firmware**, und laden Sie anschließend die aktuelle Firmware für das Gateway herunter.

4. Führen Sie zum Aktualisieren der Firmware die Schritte in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“ im Abschnitt „Verwaltung“ aus.

13. Die Aktualisierung der Firmware ist fehlgeschlagen bzw. die Netzstrom-LED blinkt.

Die Aktualisierung der Firmware kann aus mehreren Gründen fehlschlagen. Führen Sie diese Schritte aus, um die Firmware zu aktualisieren bzw. das Blinken der Netzstrom-LED zu stoppen:

- Wenn die Aktualisierung der Firmware fehlgeschlagen ist, verwenden Sie das TFTP-Programm (das Programm wurde zusammen mit der Firmware heruntergeladen). Öffnen Sie die zusammen mit der Firmware und dem TFTP-Programm heruntergeladene PDF-Datei, und befolgen Sie die darin aufgeführten Anweisungen.
- Legen Sie auf dem Computer eine statische IP-Adresse fest. Folgen Sie dazu den Anweisungen unter „1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?“. Verwenden Sie für den Computer die folgenden Einstellungen für die IP-Adresse:
  IP-Adresse: 192.168.1.50
  Subnetzmaske: 255.255.255.0
  Gateway: 192.168.1.1
- Nehmen Sie die Aktualisierung mithilfe des TFTP-Programms oder auf der Registerkarte **Administration** (Verwaltung) im webbasierten Dienstprogramm des Gateways vor.

14. Das PPPoE-Protokoll des DSL-Anbieters wird stets unterbrochen.

PPPoE ist keine dedizierte oder stets aktive Verbindung. Die DSL-Verbindung kann durch den ISP getrennt werden, wenn die Verbindung einige Zeit inaktiv war, ähnlich wie bei einer normalen Telefon-DFÜ-Verbindung zum Internet.

- Es steht eine Setup-Option zur Aufrechterhaltung der Verbindung zur Verfügung. Diese Option funktioniert möglicherweise nicht immer, Sie müssen daher die Verbindung regelmäßig neu herstellen.
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)
  3. Wählen Sie im Fenster *Setup* (Einrichtung) die Option **Keep Alive** (Verbindung aufrechterhalten) aus, und legen Sie für die Option **Redial Period** (Wahlwiederholung) 20 Sekunden fest. (Damit wird die Verbindung zum ISP beibehalten, also nicht getrennt.)
  4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern). Klicken Sie auf die Registerkarte **Status**, und klicken Sie auf Schaltfläche **Connect** (Verbinden).
  5. Möglicherweise wird als Anmeldestatus **Connecting** (Verbindung wird hergestellt) angezeigt. Drücken Sie die Taste F5, um das Fenster zu aktualisieren, bis als Anmeldestatus **Connected** (Verbunden) angezeigt wird.
  6. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.
- Falls die Verbindung wieder unterbrochen wird, führen Sie die Schritte 1 bis 6 aus, um die Verbindung erneut herzustellen.

15. Ich kann weder auf meine E-Mail noch auf das Internet oder auf das VPN zugreifen, oder ich empfange nur beschädigte Daten aus dem Internet.

Sie müssen den Wert für die MTU-Einstellung (*Maximum Transmission Unit*, Maximale Übertragungseinheit) anpassen. Die maximale Übertragungseinheit wird standardmäßig automatisch festgelegt.

- Wenn Sie Schwierigkeiten haben, führen Sie folgende Schritte aus:
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)
  3. Wählen Sie für die MTU-Option **Manual** (Manuell) aus. Geben Sie in das Feld **Size** (Größe) den Wert **1492** ein.
  4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.
- Wenn das Problem weiterhin besteht, ändern Sie den MTU-Wert auf einen anderen Wert. Verwenden Sie aus der folgenden Liste jeweils einen Wert in der angegebenen Reihenfolge, bis das Problem gelöst ist:
  1462
  1400
  1362
  1300

16. Die LED Power (Netzstrom) blinkt ständig.

Die LED **Power** (Netzstrom) leuchtet auf, wenn das Gerät erstmals eingeschaltet wird. Das System wird dann gestartet und auf einen ordnungsgemäßen Betrieb hin geprüft. Nach dem Überprüfungsvorgang leuchtet die LED konstant, wodurch der ordnungsgemäße Betrieb angezeigt wird. Wenn die LED anschließend weiterblinkt, funktioniert das Gerät nicht ordnungsgemäß. Laden Sie die Firmware erneut in den Flash-Speicher, indem Sie dem Computer eine statische IP-Adresse zuweisen und anschließend die Firmware aktualisieren. Verwenden Sie hierfür die folgenden Einstellungen: IP-Adresse **192.168.1.50**, Subnetzmaske **255.255.255.0**.

17. Bei Eingabe einer URL- oder IP-Adresse erhalte ich eine Meldung, dass eine Zeitüberschreitung vorliegt, bzw. die Aufforderung, den Vorgang erneut auszuführen.

- Prüfen Sie, ob Sie den Vorgang auf einem anderen Computer ausführen können. Ist dies der Fall, stellen Sie sicher, dass die IP-Einstellungen Ihres Computers korrekt sind (IP-Adresse, Subnetzmaske, Standard-Gateway und DNS). Starten Sie den Computer neu, bei dem das Problem aufgetreten ist.
- Falls der Computer korrekt konfiguriert ist, jedoch immer noch nicht funktioniert, überprüfen Sie das Gateway. Überprüfen Sie, ob es richtig angeschlossen und eingeschaltet ist. Stellen Sie die Verbindung mit dem Router her, und überprüfen Sie die Einstellungen. (Wenn Sie keine Verbindung herstellen können, prüfen Sie die LAN-Verbindung und die Stromversorgung.)
- Wenn das Gateway korrekt konfiguriert ist, prüfen Sie Ihre Internetverbindung (Kabel-/ADSL-Modem usw.), um den ordnungsgemäßen Betrieb des Gateways zu überprüfen. Sie können das Gateway entfernen, um dadurch die direkte Verbindung zu prüfen.

- Konfigurieren Sie die TCP/IP-Einstellung mithilfe einer von Ihrem ISP zur Verfügung gestellten DNS-Adresse manuell.
- Vergewissern Sie sich, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

18. Beim Versuch, auf das webbasierte Dienstprogramm des Gateways zuzugreifen, wird das Anmeldefenster nicht angezeigt. Stattdessen wird die Meldung „404 Forbidden“ (404 Nicht erlaubt) angezeigt.

Wenn Sie Internet Explorer verwenden, führen Sie die folgenden Schritte aus, bis das Anmeldefenster des webbasierten Dienstprogramms angezeigt wird (bei Verwendung von Netscape Navigator sind ähnliche Schritte erforderlich):

1. Klicken Sie auf **Datei**. Stellen Sie sicher, dass *Offlinebetrieb* NICHT aktiviert ist.
2. Drücken Sie **Strg + F5**. Dadurch wird eine Aktualisierung erzwungen und Internet Explorer veranlasst, neue und nicht gespeicherte Websites zu laden.

- Klicken Sie auf **Extras**. Klicken Sie auf **Internetoptionen**. Klicken Sie auf die Registerkarte **Sicherheit**. Klicken Sie auf die Schaltfläche **Standardstufe**. Stellen Sie sicher, dass die Sicherheitsstufe auf **Mittel** oder niedriger festgelegt ist. Klicken Sie anschließend auf die Schaltfläche **OK**.

Häufig gestellte Fragen

Wie viele IP-Adressen kann das Gateway maximal unterstützen?
Das Gateway unterstützt bis zu 253 IP-Adressen.

Unterstützt das Gateway IPSec-Passthrough?
Ja, dabei handelt es sich um eine integrierte Funktion, die standardmäßig aktiviert ist.

An welcher Stelle im Netzwerk wird das Gateway installiert?
In einer typischen Umgebung wird das Gateway zwischen dem ADSL-Splitter und dem LAN installiert.

Unterstützt das Gateway IPX oder AppleTalk?
Nr. TCP/IP ist der einzige Internetprotokollstandard und ist heutzutage globaler Kommunikationsstandard. IPX ist ein Kommunikationsprotokoll von NetWare, das nur zur Weiterleitung von Nachrichten von einem Knotenpunkt zum nächsten verwendet wird. AppleTalk ist ein Kommunikationsprotokoll, das in Apple- und Macintosh-Netzwerken für LAN-zu-LAN-Verbindungen verwendet wird. Beide Protokolle können jedoch nicht zur Verbindung des Internets an ein LAN verwendet werden.

Unterstützt die LAN-Verbindung des Gateways 100-Mbit/s-Ethernet?
Das Gateway unterstützt über den EtherFast 10/100-Switch mit Auto-Sensing-Funktion auf der LAN-Seite des Gateways auch 100 Mbit/s.

Was ist die Netzwerk-Adressen-Übersetzung, und wofür wird sie verwendet?
Die NAT-Funktion (*Network Address Translation*, Netzwerk-Adressen-Übersetzung) übersetzt mehrere IP-Adressen in einem privaten LAN in eine öffentliche Adresse, die im Internet verwendet wird. Dadurch wird die Sicherheit erhöht, da die Adresse eines mit dem privaten LAN verbundenen Computers nie an das Internet übertragen wird. Darüber hinaus ermöglicht der Einsatz von NAT die Verwendung kostengünstiger Internetverbindungen, wenn nur eine TCP/IP-Adresse vom ISP zur Verfügung gestellt wurde. So können Benutzer mehrere private IP-Adressen hinter einer einzigen vom ISP zur Verfügung gestellten IP-Adresse verwenden.

Unterstützt das Gateway auch andere Betriebssysteme als Windows 98 SE, ME, 2000 oder XP?
Ja. Linksys bietet jedoch derzeit keinen technischen Support hinsichtlich Installation, Konfiguration oder Fehlersuche für andere Betriebssysteme als die Windows-Betriebssysteme an.

Unterstützt das Gateway die ICQ-Dateiübertragung?
Ja, führen Sie dazu folgende Schritte aus: Klicken Sie auf das Menü **ICQ**, **Preferences** (Einstellungen) und auf **Connection Settings** (Verbindungseinstellungen). Aktivieren Sie dann die Option **Using Firewall/Using Proxy** (Verwendung einer Firewall oder eines Proxy). Legen Sie nun in den Firewall-Einstellungen für die Zeitüberschreitung 80 Sekunden fest. Der Internetbenutzer kann nun Dateien an Benutzer hinter dem Gateway senden.

Ich habe einen Unreal Tournament-Server eingerichtet, andere Benutzer im LAN können jedoch keine Verbindung mit dem Server herstellen. Was muss ich tun?
Nach der Installation eines dedizierten Unreal Tournament-Servers müssen Sie eine statische IP-Adresse für jeden Computer im LAN erstellen sowie die Ports 7777, 7778, 7779, 7780, 7781 und 27900 an die IP-Adresse des Servers weiterleiten. Sie können hierfür auch einen Bereich zwischen 7777 und 27900 festlegen. Um die Funktion für UT Server Admin zu verwenden, müssen Sie die Weiterleitung an einen weiteren Port vornehmen. (Das kann Port 8080 sein, der jedoch auch für die Remote-Verwaltung verwendet wird. Sie müssen u. U. diesen Port deaktivieren.) Legen Sie anschließend in der Datei SERVER.INI im Abschnitt [UWeb.WebServer] für „ListenPort“ den Wert 8080 (in Übereinstimmung mit dem oben erwähnten zugeordneten Port) und für „ServerName“ die von Ihrem ISP zur Verfügung gestellte IP-Adresse des Gateways fest.

Können mehrere Spieler im LAN auf einen Spieleserver zugreifen und mit nur einer öffentlichen IP-Adresse gleichzeitig spielen?
Das hängt vom verwendeten Netzwerkspiel bzw. dem verwendeten Server ab. So unterstützt z. B. Unreal Tournament das mehrfache Anmelden mit nur einer öffentlichen IP-Adresse.

Wie kann ich Half-Life – Team Fortress mit dem Gateway verwenden?
Der standardmäßige Client-Port für Half-Life ist 27005. Für die Computer in Ihrem LAN muss in der Befehlszeile für Half-Life-Verknüpfungen „+clientport 2700x“ hinzugefügt werden, wobei „x“ dann 6, 7, 8 usw. entspricht. Dadurch können mehrere Computer mit dem gleichen Server eine Verbindung herstellen. Problem: Bei Version 1.0.1.6 können mehrere Computer, die die gleiche CD-Kennnummer verwenden, nicht gleichzeitig mit dem Server verbunden sein, auch wenn sie sich im gleichen LAN befinden. Dieses Problem tritt bei Version 1.0.1.3 nicht auf. Beim Hosting von Spielen muss sich der Half-Life-Server jedoch nicht in der DMZ befinden. Es muss lediglich der Port 27015 an die lokale IP-Adresse des Server-Computers weitergeleitet werden.

Die Webseite reagiert nicht, heruntergeladene Dateien sind beschädigt, oder es werden nur unleserliche Zeichen auf dem Bildschirm angezeigt. Was muss ich tun?
Legen Sie für den Ethernet-Adapter 10 MBit/s bzw. den Halbduplex-Modus fest, und deaktivieren Sie als vorübergehende Maßnahme für den Ethernet-Adapter die Funktion zur automatischen Verbindungsaushandlung. (Rufen Sie in der Systemsteuerungskomponente **Netzwerk** die Registerkarte für die erweiterten Einstellungen des Ethernet-Adapters auf.) Stellen Sie sicher, dass die Proxy-Einstellung im Browser deaktiviert ist. Weitere Informationen erhalten Sie unter www.linksys.com/international.

Was kann ich tun, wenn alle Maßnahmen bei einer fehlgeschlagenen Installation erfolglos bleiben?
Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Taste **Reset** drücken, bis die LED **Power** (Netzstrom) aufleuchtet und wieder erlischt. Setzen Sie das ADSL-Modem zurück, indem Sie es aus- und erneut einschalten. Laden Sie die neueste Firmware-Version über die internationale Website von Linksys unter www.linksys.com/international herunter, und nehmen Sie die Aktualisierung vor.

Wie erhalte ich Informationen zu neuen Aktualisierungen der Gateway-Firmware?
Sämtliche Aktualisierungen für Firmware von Linksys werden auf der internationalen Website von Linksys unter www.linksys.com/international veröffentlicht und können kostenlos heruntergeladen werden. Verwenden Sie zur Aktualisierung der Gateway-Firmware die Registerkarte **System** des webbasierten Dienstprogramms des Gateways. Wenn die Internetverbindung des Gateways zufriedenstellend funktioniert, besteht keine Notwendigkeit, eine neuere Firmware-Version herunterzuladen, es sei denn, Sie möchten neue Funktionen der aktualisierten Version verwenden.

Funktioniert das Gateway in einer Macintosh-Umgebung?
Ja, Sie können jedoch nur über Internet Explorer 4.0 bzw. Netscape Navigator 4.0 oder höher für Macintosh auf die Setup-Seiten des Gateways zugreifen.

Ich kann die Seite für die Webkonfiguration des Gateways nicht aufrufen. Was kann ich tun?
Sie müssen möglicherweise die Proxy-Einstellungen in Ihrem Internet-Browser, z. B. Netscape Navigator oder Internet Explorer, entfernen. Weitere Anweisungen erhalten Sie in der Dokumentation zu Ihrem Browser. Stellen Sie sicher, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

Was bedeutet DMZ-Hosting?
Mithilfe der DMZ (*Demilitarized Zone*, Entmilitarisierte Zone) kann über eine IP-Adresse (d. h. über einen Computer) eine Verbindung zum Internet hergestellt werden. Für einige Anwendungen ist es erforderlich, dass mehrere TCP/IP-Ports geöffnet sind. Es ist empfehlenswert, dass Sie zur Verwendung des DMZ-Hostings für Ihren Computer eine statische IP-Adresse festlegen. Weitere Informationen zum Ermitteln einer LAN-IP-Adresse finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

Verwenden bei DMZ-Hosting sowohl DMZ-Benutzer als auch Gateway die öffentliche IP-Adresse?
Nr.

Leitet das Gateway PPTP-Datenpakete oder PPTP-Sitzungen aktiv weiter?
Durch das Gateway werden PPTP-Datenpakete weitergeleitet.

Ist das Gateway auch plattformübergreifend einsetzbar?
Jede Plattform, die Ethernet und TCP/IP unterstützt, ist mit dem Gateway kompatibel.

Wie viele Ports können gleichzeitig weitergeleitet werden?
Das Gateway kann theoretisch 520 Sitzungen gleichzeitig ausführen, Sie können jedoch nur 10 Anschlussbereiche weiterleiten.

Über welche erweiterten Funktionen verfügt das Gateway?
Zu den erweiterten Funktionen des Gateways zählen u. a. erweiterte Wireless-Einstellungen, Filter, Port-Forwarding, Routing und DDNS.

Wie kann ich überprüfen, ob ich über statische oder DHCP-IP-Adressen verfüge?
Wenden Sie sich an Ihren ISP, um diese Informationen zu erhalten.

Wie kann ich mIRC mit dem Gateway verwenden?
Legen Sie auf der Registerkarte **Port Forwarding** (Anschlussweiterleitung) den Wert **113** für den Computer fest, auf dem Sie mIRC verwenden möchten.

Kann das Gateway als DHCP-Server eingesetzt werden?
Ja. Das Gateway verfügt über eine integrierte DHCP-Server-Software.

Kann ich Anwendungen von Remote-Computern über das Wireless-Netzwerk ausführen?
Dies ist abhängig davon, ob die Anwendung für die Verwendung in Netzwerken entwickelt wurde. Informationen dazu, ob die Anwendung in Netzwerken verwendet werden kann, finden Sie in der Dokumentation der entsprechenden Anwendung.

Was ist der IEEE 802.11g-Standard?
Dies ist ein IEEE-Standard für Wireless-Netzwerke. Mit dem 802.11g-Standard können Geräte von unterschiedlichen Herstellern im Wireless-Netzwerk miteinander kommunizieren, sofern die Geräte mit dem 802.11g-Standard kompatibel sind. Durch den 802.11g-Standard ist eine maximale Datenübertragungsrate von 54 MBit/s und eine Betriebsfrequenz von 2,4 GHz vorgegeben.

Was ist der IEEE 802.11b-Standard?
Dies ist ein IEEE-Standard für Wireless-Netzwerke. Mit dem 802.11b-Standard können Geräte von unterschiedlichen Herstellern im Wireless-Netzwerk miteinander kommunizieren, sofern die Geräte mit dem 802.11b-Standard kompatibel sind. Durch den 802.11b-Standard ist eine maximale Datenübertragungsrate von 11 MBit/s und eine Betriebsfrequenz von 2,4 GHz vorgegeben.

Welche IEEE 802.11b- und 802.11g-Funktionen werden unterstützt?
Das Produkt unterstützt die folgenden IEEE 802.11b- und IEEE 802.11g-Funktionen:

- CSMA/CA sowie das Acknowledge-Protokoll
- Multi-Channel-Roaming
- Automatische Ratenauswahl
- RTS/CTS
- Fragmentierung
- Energieverwaltung

Es unterstützt zudem die OFDM-Technologie für 802.11g-Netzwerke.

Was bedeutet Ad-hoc-Modus?
Wenn für ein Wireless-Netzwerk der Ad-hoc-Modus festgelegt ist, sind die Wireless-Computer so konfiguriert, dass sie ohne Access Point direkt miteinander kommunizieren (Peer-to-Peer).

Was bedeutet Infrastrukturmodus?
Wenn für ein Wireless-Netzwerk der Infrastrukturmodus festgelegt wurde, ist es so konfiguriert, dass es über einen Wireless Access Point mit Netzwerken kommuniziert.

Was ist Roaming?

Roaming ermöglicht Benutzern von tragbaren Computern einen reibungslosen Datenaustausch beim Zurücklegen von Entfernungen, die nicht von einem einzigen Access Point abgedeckt werden können. Vor Verwendung des Roamings muss der Computer auf die gleiche Kanalnummer wie der Access Point des entsprechenden Empfangsbereichs gesetzt werden.

Um eine dauerhafte nahtlose Verbindung zu erzielen, muss das Wireless-LAN eine Reihe an unterschiedlichen Funktionen besitzen. So müssen z. B. alle Nachrichten von jedem Knoten und jedem Access Point bestätigt werden. Jeder Knoten muss den Kontakt mit dem Wireless-Netzwerk aufrechterhalten, auch wenn keine Datenübertragung stattfindet. Damit diese Funktionen gleichzeitig ausgeführt werden können, ist eine dynamische Funkfrequenz-Netzwerktechnologie erforderlich, mit der Access Points und Knoten miteinander verknüpft werden. In solchen Systemen sucht der Endknoten des Benutzers nach dem jeweils besten Zugriff auf das System. Zunächst werden Faktoren wie Signalstärke und -qualität, die aktuelle Nachrichtenmenge, die von jedem Access Point verarbeitet wird, und die Entfernung zwischen jedem Access Point zum verdrahteten Backbone ausgewertet. Anschließend ermittelt der Knoten auf Grundlage dieser Informationen den geeigneten Access Point und registriert dessen Adresse. Die Kommunikation zwischen Knoten und Host-Computer kann in beide Richtungen des Backbones verlaufen.

Bei fortschreitender Kommunikation prüft der Funkfrequenz-Sender des Endknotens in regelmäßigen Abständen, ob eine Verbindung mit dem ursprünglichen Access Point vorliegt oder ob ein neuer Access Point gesucht werden soll. Wenn ein Knoten keine Bestätigung des ursprünglichen Access Point mehr erhält, wird eine neue Verbindungssuche gestartet. Sobald ein neuer Access Point gefunden wurde, wird dessen Adresse registriert und die Kommunikation fortgesetzt.

Was bedeutet ISM-Band?

Die FCC-Behörde und die jeweiligen Behörden außerhalb der USA haben Bestimmungen hinsichtlich der Bandbreite für eine nicht durch Lizenzen abgedeckte Verwendung im ISM-Band erlassen. Die Frequenz liegt bei ca. 2,4 GHz und kann weltweit genutzt werden. Mit dieser wahrlich revolutionären Maßnahme können nun problemlos High Speed-Wireless-Funktionen von Benutzern weltweit genutzt werden.

Was bedeutet Bandspreizung?

Die Technologie der Bandspreizung (*Spread Spectrum Technology*) ist eine vom Militär entwickelte Breitband-Funkfrequenz-Technologie, die für zuverlässige, sichere und störresistente Kommunikationssysteme eingesetzt werden kann. Bei dieser Technologie werden gewisse Abstriche bei der Bandbreiteneffizienz hingenommen, um eine höhere Zuverlässigkeit, Integrität und Sicherheit zu erreichen. Es wird hier also eine größere Bandbreite als bei der Schmalbandübertragung verwendet. Im Gegenzug wird jedoch ein Signal erreicht, das lauter und einfacher zu lokalisieren ist, allerdings unter der Voraussetzung, dass der Empfänger die Parameter des mittels Bandspreizung übertragenen Signals kennt. Wenn ein Empfänger nicht auf die richtige Frequenz eingestellt ist, scheint ein mittels Bandspreizung übertragenes Signal nichts anderes als ein Hintergrundgeräusch zu sein. Es stehen zwei unterschiedliche Verfahren für die Bandspreizung zur Verfügung: DSSS (*Direct Sequence Spread Spectrum*, Direkte Bandspreizung) und FHSS (*Frequency Hopping Spread Spectrum*, Frequenzsprungverfahren).

Was ist DSSS? Was ist FHSS? Worin liegt der Unterschied?

Bei FHSS wird ein Schmalbandträger verwendet, der nach einem für Sender und Empfänger bekannten Muster die Frequenz ändert. Bei ordnungsgemäßer Synchronisation wird jeweils ein einziger logischer Kanal aufrechterhalten. Unerwünschten Empfängern erscheint das FHSS-Signal als kurzzeitiges Impulsrauschen. DSSS generiert ein redundantes Bitmuster für jedes zu übertragende Bit. Dieses Bitmuster wird „Chip“ oder „Chipping Code“ genannt. Je länger der Chip ist, desto größer ist die Wahrscheinlichkeit, dass die ursprüngliche Information wieder generiert werden kann. Auch wenn ein oder mehrere Bits im Chip während der Übertragung beschädigt wurden, können diese durch eine statistische Technik im Empfänger regeneriert werden und müssen daher nicht nochmals übertragen werden. Unerwünschten Empfängern erscheint das DSSS-Signal als schwaches Breitbandrauschen und wird von den meisten Schmalbandempfängern ignoriert.

Können die Daten bei der Funkübertragung abgefangen werden?

WLAN verfügt über zweifachen Schutz im Sicherheitsbereich. Im Hardwarebereich sorgt DSSS-Technologie (*Direct Sequence Spread Spectrum*, Direkte Bandspreizung) für die integrierte Sicherheitsfunktion der Verschlüsselung. Im Softwarebereich bietet WLAN die WEP-Verschlüsselungsfunktion, um die Sicherheit zu erhöhen und die Zugriffssteuerung zu verbessern.

Was ist WEP?

WEP ist die Abkürzung für *Wired Equivalent Privacy*. Hierbei handelt es sich um einen Datenschutzmechanismus, der auf einem 64-Bit- oder 128-Bit-Algorithmus mit gemeinsam verwendetem Schlüssel basiert und im IEEE 802.11-Standard festgelegt ist.

Was ist eine MAC-Adresse?

Eine MAC-Adresse (*Media Access Control*) ist eine eindeutige Nummer, die jedem Ethernet-Netzwerkgerät, wie z. B. einem Netzwerkadapter, vom Hersteller zugewiesen wird und mit der das Gerät im Netzwerk auf Hardware-Ebene identifiziert werden kann. Aus praktischen Gründen wird diese Nummer dauerhaft vergeben. Im Gegensatz zu IP-Adressen, die sich bei jeder Anmeldung des Computers beim Netzwerk ändern können, bleibt die MAC-Adresse eines Geräts stets gleich und ist dadurch eine äußerst nützliche Kennung im Netzwerk.

Wie setze ich das Gateway zurück?

Halten Sie die Taste **Reset** an der Rückseite des Gateways ca. 10 Sekunden lang gedrückt. Dadurch wird das Gateway auf die Werkseinstellungen zurückgesetzt.

Wie behebe ich Probleme wegen zu schwachen Signals?
Sie können die genaue Reichweite Ihres Wireless-Netzwerks nur durch Testen bestimmen. Jedes Hindernis zwischen dem Gateway und einem Wireless-Computer führt zu Signalverlust. Durch verbleites Glas, Metall, Betonböden, Wasser und Wände werden Signale behindert und die Reichweite vermindert. Verwenden Sie das Gateway und den Wireless-Computer zunächst im gleichen Zimmer, und vergrößern Sie dann schrittweise den Abstand zwischen beiden Geräten, um so die maximale Reichweite in Ihrer Umgebung zu bestimmen.

Verwenden Sie auch unterschiedliche Kanäle, da so Störungen ausgeschlossen werden, die nur einen Kanal betreffen.

Die Signalstärke ist absolut ausreichend, das Netzwerk wird jedoch nicht angezeigt.
Sicherheit im Wireless-Netzwerkbetrieb ist vermutlich im Gateway, jedoch nicht im Wireless-Adapter (oder umgekehrt) aktiviert. Stellen Sie sicher, dass für alle Geräte in Ihrem Wireless-Netzwerk dieselben Wireless-Sicherheitseinstellungen verwendet werden.

Wie viele Kanäle/Frequenzen stehen für das Gateway zur Verfügung?
In weiten Teilen Nord-, Mittel- und Südamerikas sind insgesamt 11 Kanäle (von 1 bis 11) verfügbar. Im Großteil von Europa stehen 13 Kanäle (von 1 bis 13) zur Verfügung. Je nach den regionalen bzw. nationalen Bestimmungen können in anderen Regionen weitere Kanäle verfügbar sein.

Falls Sie hier keine Antworten auf Ihre Fragen erhalten haben, finden Sie weitere Informationen auf der internationalen Website von Linksys unter http://www.linksys.com/international.

Anhang B: Wireless-Sicherheit

Linksys hat es sich zum Ziel gesetzt, den Wireless-Netzwerkbetrieb für Sie so sicher und einfach wie möglich zu gestalten. Die aktuellen Produkte von Linksys bieten verschiedene Netzwerksicherheitsfunktionen. Um diese anzuwenden, müssen Sie jedoch bestimmte Schritte ausführen. Beachten Sie daher Folgendes beim Einrichten bzw. Verwenden Ihres Wireless-Netzwerks.

Vorsichtsmaßnahmen

Bei der folgenden Liste handelt es sich um eine Auflistung aller möglichen Vorsichtsmaßnahmen. Die Schritte 1 bis 5 sollten Sie unbedingt ausführen:

1. Ändern Sie die Standard-SSID.
2. Deaktivieren Sie die SSID-Übertragung.
3. Ändern Sie das Standardpasswort für das Administratorkonto.
4. Aktivieren Sie die MAC-Adressfilterung.
5. Ändern Sie die SSID regelmäßig.
6. Verwenden Sie den stärksten verfügbaren Verschlüsselungsalgorithmus. Verwenden Sie WPA (falls verfügbar). Beachten Sie, dass die Netzwerkleistung hierdurch verringert werden kann.
7. Ändern Sie die WEP-Verschlüsselungsschlüssel regelmäßig.

Informationen zum Umsetzen dieser Sicherheitsmaßnahmen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.

HINWEIS: Einige dieser Sicherheitsfunktionen sind nur über das Netzwerk-Gateway, den Router oder den Access Point verfügbar. Weitere Informationen finden Sie in der Dokumentation zum Gateway, Router bzw. Access Point.

Sicherheitsrisiken bei Wireless-Netzwerken

Wireless-Netzwerke sind einfach zu finden. Hacker wissen, dass Geräte für den Wireless-Netzwerkbetrieb nach so genannten Beacon-Meldungen suchen, bevor sie sich in ein Wireless-Netzwerk einklinken. Diese Meldungen, die umfassende Netzwerkinformationen wie beispielsweise die SSID (*Service Set IDentifier*) des Netzwerks enthalten, lassen sich leicht entschlüsseln. Dagegen können Sie sich folgendermaßen schützen:

Ändern Sie das Administratorpasswort regelmäßig: Bedenken Sie, dass bei jedem im Wireless-Netzwerkbetrieb verwendeten Gerät die Netzwerkeinstellungen (SSID, WEP-Schlüssel usw.) in der Firmware gespeichert sind. Die Netzwerkeinstellungen können nur vom Netzwerkadministrator geändert werden. Wenn einem Hacker das Administratorpasswort bekannt wird, kann auch er diese Einstellungen ändern. Deshalb sollten Sie es ihm so schwer wie möglich machen, an diese Informationen zu gelangen. Ändern Sie das Administratorpasswort regelmäßig:

SSID: Im Zusammenhang mit der SSID ist Folgendes zu beachten:

1. Deaktivieren Sie die Übertragung.
2. Wählen Sie eine individuelle SSID.
3. Ändern Sie sie regelmäßig.

Bei den meisten Geräten für den Wireless-Netzwerkbetrieb gibt es die Option, die SSID zu übertragen. Diese Option ist zwar recht praktisch, bedeutet jedoch, dass sich jeder in Ihr Wireless-Netzwerk einklinken kann. Jeder, auch Hacker. Daher sollten Sie die SSID nicht übertragen.

Geräte für den Wireless-Netzwerkbetrieb sind werkseitig auf eine Standard-SSID eingestellt. (Die Standard-SSID von Linksys lautet „linksys“.) Hacker kennen diese Standardeinstellungen und können Ihr Netzwerk darauf überprüfen. Ändern Sie Ihre SSID in einen eindeutigen Namen, der keinerlei Bezug zu Ihrem Unternehmen oder zu den von Ihnen verwendeten Netzwerkprodukten hat.

Ändern Sie Ihre SSID regelmäßig, damit Hacker, die sich Zugriff auf Ihr Wireless-Netzwerk verschafft haben, erneut das Passwort knacken müssen.

MAC-Adressen: Aktivieren Sie die MAC-Adressfilterung. Durch die MAC-Adressfilterung wird nur Wireless-Knoten mit bestimmten MAC-Adressen der Zugriff auf das Netzwerk ermöglicht. Dies erschwert es Hackern, mit einer zufällig gewählten MAC-Adresse auf Ihr Netzwerk zuzugreifen.

WEP Encryption (WEP-Verschlüsselung): WEP (*Wired Equivalent Privacy*) wird oft als eine Art Allheilmittel im Zusammenhang mit Sicherheitsrisiken bei Wireless-Geräten angesehen. Damit werden die Fähigkeiten von WEP jedoch überschätzt. Auch WEP kann nur soweit zur Sicherheit beitragen, dass es Hackern das Eindringen erschwert.

Es gibt mehrere Methoden, um die Wirksamkeit von WEP zu optimieren:

1. Verwenden Sie die höchste Verschlüsselungsebene.
2. Verwenden Sie die Authentifizierung mit einem gemeinsamen Schlüssel.
3. Ändern Sie Ihren WEP-Schlüssel regelmäßig.

WICHTIG: Jedes Gerät im Wireless-Netzwerk MUSS dasselbe Verschlüsselungsverfahren und denselben Verschlüsselungsschlüssel verwenden, damit das Wireless-Netzwerk ordnungsgemäß funktioniert.

WPA: Bei WPA (Wi-Fi Protected Access) handelt es sich um den neuesten und besten verfügbaren Standard für Wi-Fi-Sicherheit. **WPA2** ist eine neuere Version von WPA (Wi-Fi Protected Access) mit stärkerer Verschlüsselung. Im Modus WPA stehen Ihnen zwei Verschlüsselungsverfahren zur Verfügung: TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption System). TKIP verwendet eine leistungsfähigere Verschlüsselungsmethode sowie MIC (Message Integrity Code), um das System gegen Hacker zu schützen. AES arbeitet mit einer symmetrischen blockweisen Datenverschlüsselung mit 128-Bit-Schlüsseln. WPA Enterprise und WPA2 Enterprise verwenden RADIUS (Remote Authentication Dial-In User Service) für die Authentifizierung.

WPA Personal: Wählen Sie den gewünschten Algorithmus (**TKIP** oder **AES**) aus, geben Sie im Feld **Passphrase** ein Passwort mit einer Länge von 8 bis 63 Zeichen ein, und legen Sie für **Group Key Renewal** (Erneuerung Gruppenschlüssel) einen Zeitraum zwischen 0 und 99.999 Sekunden fest. Diese Zeitangabe teilt dem Gateway bzw. einem anderen Gerät mit, wie oft die Verschlüsselungsschlüssel gewechselt werden sollen.

WPA2 Personal: Bei WPA2 steht Ihnen die Verschlüsselungsmethode TKIP mit dynamischen Verschlüsselungsschlüsseln zur Verfügung. Geben Sie ein Passphrase von 8 bis 63 Zeichen ein. Legen Sie anschließend den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind.

WPA2 Mixed Mode (WPA2 Gemischter Modus): Im gemischten WPA2-Modus stehen TKIP- und AES-Verschlüsselung zur Verfügung. Geben Sie ein Passphrase von 8 bis 63 Zeichen ein. Legen Sie anschließend den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind.

WPA Enterprise: Bei dieser Methode wird WPA in Kombination mit einem RADIUS-Server eingesetzt. Geben Sie die IP-Adresse und die Port-Nummer des RADIUS-Servers ein und dann den Schlüssel, der vom Gateway und dem zugehörigen RADIUS-Server gemeinsam verwendet wird. Legen Sie anschließend den Zeitraum für **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind.

WPA2 Enterprise: Bei dieser Methode wird WPA2 in Kombination mit einem RADIUS-Server eingesetzt. Geben Sie die IP-Adresse und die Port-Nummer des RADIUS-Servers ein und dann den Schlüssel, der vom Gateway und dem zugehörigen RADIUS-Server gemeinsam verwendet wird. Legen Sie anschließend den Zeitraum für **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind.

Die Verwendung von Verschlüsselungsfunktionen kann sich negativ auf die Netzwerkleistung auswirken. Wenn Sie jedoch sensible Daten über das Netzwerk senden, sollten Sie diese verschlüsseln.

Wenn Sie diese Sicherheitsempfehlungen einhalten, können Sie ganz beruhigt arbeiten und die flexible und praktische Technologie von Linksys bedenkenlos einsetzen.

Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters

In diesem Abschnitt wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterungsfunktion des Gateways verwenden zu können. Sie können außerdem die IP-Adresse für den Ethernet-Adapter Ihres Computers ermitteln. Die IP-Adresse wird für die Filterungs-, Weiterleitungs- und DMZ-Funktionen des Gateways verwendet. Führen Sie die in diesem Anhang aufgelisteten Schritte aus, um die MAC- oder IP-Adresse des Adapters unter Windows 98, ME, 2000 bzw. XP zu ermitteln.

Anweisungen für Windows 98/ME

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld *Öffnen* den Eintrag **winipcfg** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

2. Wählen Sie im Fenster *IP-Konfiguration* den Ethernet-Adapter aus, den Sie über ein Ethernet-Netzwerkkabel der Kategorie 5 mit dem Gateway verbunden haben. Siehe Abbildung C-1.

3. Notieren Sie die Adapteradresse so, wie sie am Computer angezeigt wird (siehe Abbildung C-2). Dies ist die MAC-Adresse Ihres Ethernet-Adapters und wird im hexadezimalen Format als Folge von Ziffern und Buchstaben dargestellt.

   Die MAC-Adresse/Adapteradresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-2 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf Ihrem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-2 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf Ihrem Computer angezeigte Adresse kann davon abweichen.

HINWEIS: Die MAC-Adresse wird auch als Adapteradresse bezeichnet.

Abbildung C-1: IP-Konfiguration

Abbildung C-2: MAC-Adresse/ Adapteradresse

Anweisungen für Windows 2000/XP

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld *Öffnen* den Eintrag **cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

HINWEIS: Die MAC-Adresse wird auch als physische Adresse bezeichnet.

2. Geben Sie in die Eingabeaufforderung **ipconfig /all** ein. Drücken Sie die Eingabetaste.

3. Notieren Sie die physische Adresse so, wie sie am Computer anzeigt wird (Abbildung C-3). Diese Adresse stellt die MAC-Adresse des Ethernet-Adapters dar. Sie wird als Folge von Ziffern und Buchstaben dargestellt.

   Die MAC-Adresse/physische Adresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-3 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf Ihrem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-3 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf Ihrem Computer angezeigte Adresse kann davon abweichen.

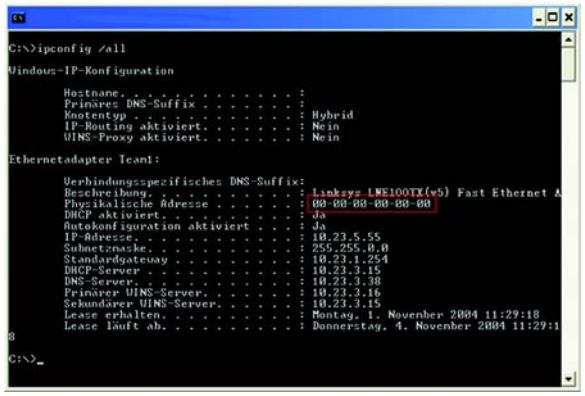


Abbildung C-3: MAC-Adresse/physische Adresse

Anhang D: Aktualisieren der Firmware

So aktualisieren Sie die Gateway-Firmware:

1. Laden Sie die Aktualisierungsdatei für die Gateway-Firmware von der Website unter *www.linksys.com/international* herunter.
2. Extrahieren Sie die Datei auf dem Computer.
3. Öffnen Sie das webbasierte Gateway-Dienstprogramm, und klicken Sie auf die Registerkarte **Administration** (Verwaltung).
4. Klicken Sie auf die Registerkarte **Firmware Upgrade** (Aktualisieren der Firmware).
5. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der extrahierten Datei zu suchen, und doppelklicken Sie auf diese Datei.
6. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren), und befolgen Sie die Anweisungen auf dem Bildschirm.

Abbildung D-1: Aktualisieren der Firmware

Anhang E: Glossar

802.11b: Ein Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 11 MBit/s sowie eine Betriebsfrequenz von 2,4 GHz festlegt.

802.11g: Ein Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 Mbit/s und eine Betriebsfrequenz von 2,4 GHz sowie die Abwärtskompatibilität mit Geräten festlegt, die dem Standard 802.11b entsprechen.

Access Point: Ein Gerät, über das Computer und andere Geräte mit Wireless-Funktionalität mit einem verdrahteten Netzwerk kommunizieren können. Wird auch verwendet, um die Reichweite von Wireless-Netzwerken zu erweitern.

Adapter: Ein Gerät, mit dem Ihr Computer Netzwerkfunktionalität erhält.

Ad-Hoc: Eine Gruppe von Wireless-Geräten, die nicht über einen Access Point, sondern direkt miteinander kommunizieren (Peer-to-Peer).

AES (***A**dvanced **E**ncryption **S**tandard*): Eine Sicherheitsmethode, bei der die symmetrische Datenverschlüsselung mit 128 Bit verwendet wird.

Aktualisierung: Das Ersetzen vorhandener Software oder Firmware durch eine neuere Version.

Backbone: Der Teil des Netzwerks, der die meisten Systeme und Netzwerke miteinander verbindet und die meisten Daten verarbeitet.

Bandbreite: Die Übertragungskapazität eines bestimmten Geräts oder Netzwerks.

Bandspreizung: Weitband-Funkfrequenzmethode, die für eine zuverlässigere und sicherere Datenübertragung verwendet wird.

Beacon-Intervall: Im Wireless-Netzwerk übertragene Daten zur Synchronisierung des Netzwerks.

Bit: Eine binäre Informationseinheit.

Bridge: Ein Gerät, das verschiedene Netzwerke miteinander verbindet.

Breitband: Eine stets aktive, schnelle Internetverbindung.

Browser: Eine Anwendung, mit der auf alle im World Wide Web enthaltenen Informationen interaktiv zugegriffen werden kann.

Byte: Eine Dateneinheit, die üblicherweise aus acht Bit besteht.

CSMA/CA (***C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance*): Eine Datenübertragungsmethode, die verwendet wird, um Datenkollisionen zu verhindern.

CTS (***C**lear **T**o **S**end*): Ein von einem Wireless-Gerät gesendetes Signal, das angibt, dass das Gerät für Daten empfangsbereit ist.

Daisy Chain (Verkettung): Eine Methode, bei der Geräte in Reihe (in einer Kette) miteinander verbunden werden.

Datenbank: Eine Datensammlung, die so organisiert ist, dass die enthaltenen Daten schnell und einfach verwaltet und aktualisiert werden können sowie problemlos abrufbar sind.

DDNS (***D**ynamic **D**omain **N**ame **S**ystem*): Ein System, in dem eine Website, ein FTP- oder E-Mail-Server mit einem festen Domänennamen (z. B. www.xyz.com) eine dynamische IP-Adresse verwenden kann.

DHCP (***D**ynamic **H**ost **C**onfiguration **P**rotocol*): Ein Netzwerkprotokoll, mit dem Administratoren Netzwerkcomputern temporäre IP-Adressen zuweisen können, indem sie IP-Adressen für einen bestimmten Zeitraum an Benutzer „vermieten“ statt ihnen eine permanente IP-Adresse zuzuweisen.

DMZ (***Dem**ilitarized **Z**one*): Hebt den Firewall-Schutz des Routers für einen PC auf, sodass dieser im Internet „sichtbar“ wird.

DNS (***D**omain **N**ame **S**erver*): Die IP-Adresse des Servers Ihres Internetdienstanbieters, der die Namen von Websites in IP-Adressen übersetzt.

Domäne: Ein spezifischer Name für ein Netzwerk aus mehreren Computern.

DSL (***D**igital **S**ubscriber **L**ine*): Eine stets aktive Breitbandverbindung über herkömmliche Telefonleitungen.

DSSS (***D**irect-**S**equence **S**pread-**S**pectrum*): Eine Frequenzübertragungstechnologie, die ein redundantes Bit-Muster verwendet, um die Wahrscheinlichkeit von Datenverlusten bei der Übertragung zu senken.

DTIM (***D**elivery **T**raffic **I**ndication **M**essage*): Eine in Datenpaketen enthaltene Nachricht, die zur Verbesserung der Effizienz von Wireless-Verbindungen beitragen kann.

Durchsatz: Die Datenmenge, die in einem bestimmten Zeitraum erfolgreich von einem Knoten an einen anderen übertragen werden kann.

Dynamische IP-Adresse: Eine von einem DHCP-Server zugewiesene temporäre IP-Adresse.

EAP (***E**xtensible **A**uthentication **P**rotocol*): Ein allgemeines Authentifizierungsprotokoll zur Steuerung des Netzwerkzugriffs. Viele spezielle Authentifizierungsmethoden greifen auf dieses Protokoll zurück.

EAP-PEAP (***E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifizierungsmethode, bei der eine Kombination von digitalen Zertifikaten sowie ein anderes System, z. B. Passwörter, verwendet werden.

EAP-TLS (***E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity*): Eine gegenseitige Authentifizierungsmethode, bei der digitale Zertifikate verwendet werden.

Ethernet: Ein Netzwerkprotokoll, mit dem festgelegt wird, wie Daten auf gängigen Übertragungsmedien gespeichert und von dort abgerufen werden.

Finger: Ein Programm, das Ihnen den Namen angibt, der einer E-Mail-Adresse zugewiesen ist.

Firewall: Eine Gruppe von Programmen, die sich auf einem Netzwerk-Gateway-Server befindet und die Ressourcen des Netzwerks vor unberechtigten Benutzern schützt.

Firmware: Der für den Betrieb eines Netzwerkgeräts verwendete Programmcode.

Fragmentierung: Das Aufteilen von Paketen in kleinere Einheiten bei der Übertragung über Netzwerkmedien, die die ursprüngliche Größe des Pakets nicht unterstützen.

FTP (***F**ile **T**ransfer **P**rotocol*): Ein Protokoll für die Übertragung von Dateien über ein TCP/IP-Netzwerk.

Gateway: Ein Gerät zur Verbindung von Netzwerken mit unterschiedlichen, inkompatiblen Kommunikationsprotokollen.

Halbduplex: Datenübertragung, die über eine Leitung in beide Richtungen erfolgt, jedoch entweder in die eine oder die andere Richtung, nicht gleichzeitig in beide.

Hardware: Als Hardware bezeichnet man die physischen Geräte im Computer- und Telekommunikationsbereich sowie andere Informationstechnologiegeräte.

Herunterladen: Das Empfangen einer Datei, die über ein Netzwerk übertragen wurde.

Hochfahren: Starten von Geräten, sodass diese Befehle ausführen.

HTTP (***H**yper**T**ext **T**ransport **P**rotocol*): Kommunikationsprotokoll, mit dem Verbindungen zu Servern im World Wide Web hergestellt werden.

Infrastruktur: Ein Wireless-Netzwerk, das über einen Access Point mit einem verdrahteten Netzwerk verbunden ist.

IP (***I**nternet **P**rotocol*): Ein Protokoll zum Senden von Daten über Netzwerke.

IP-Adresse: Die Adresse, anhand der ein Computer oder ein Gerät im Netzwerk identifiziert werden kann.

IPCONFIG: Ein Dienstprogramm für Windows 2000 und Windows XP, das die IP-Adresse für ein bestimmtes Netzwerkgerät anzeigt.

IPSec (***I**nternet **P**rotocol **Sec**urity*): Ein VPN-Protokoll, das für den sicheren Austausch von Paketen auf der IP-Ebene verwendet wird.

ISM-Band: Bei Übertragungen im Wireless-Netzwerkbetrieb verwendete Funkbandbreite.

ISP (***I**nternet **S**ervice **P**rovider*): Internetdienstanbieter; ein Anbieter, über den auf das Internet zugegriffen werden kann.

Kabelmodem: Ein Gerät, über das ein Computer mit dem Kabelfernsehnetzwerk verbunden wird, das wiederum eine Verbindung zum Internet herstellt.

Knoten: Ein Netzwerkknotenpunkt bzw. -verbindungspunkt, üblicherweise ein Computer oder eine Arbeitsstation.

Laden: Das Übertragen einer Datei über das Netzwerk.

LAN: Die Computer und Netzwerkprodukte, aus denen sich Ihr lokales Netzwerk zusammensetzt.

LEAP (***L**ightweight **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifizierungsmethode, bei der ein Benutzername- und Passwortsystem verwendet wird.

MAC-Adresse (***M**edia **A**ccess **C**ontrol*): Die eindeutige Adresse, die ein Hersteller jedem einzelnen Netzwerkgerät zuweist.

MBit/s (***M**ega**bit** pro **S**ekunde*): Eine Million Bit pro Sekunde. Maßeinheit für die Datenübertragung.

mIRC: Ein unter Windows verwendetes Internet Relay Chat-Programm.

Multicasting: Das gleichzeitige Senden von Daten an mehrere Ziele.

NAT (***N**etwork **A**ddress **T**ranslation*): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.

Netzwerk: Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam verwenden, speichern und untereinander übertragen können.

NNTP (***N**etwork **N**ews **T**ransfer **P**rotocol*): Das Protokoll, mit dem eine Verbindung zu Usenet-Gruppen im Internet hergestellt wird.

OFDM (***O**rthogonal **F**requency **D**ivision **M**ultiplexing*): Eine Frequenzübertragungstechnologie, die den Datenstrom in mehrere Datenströme von geringerer Geschwindigkeit aufteilt, die dann parallel übertragen werden, um zu verhindern, dass Informationen während der Übertragung verloren gehen.

Paket: Eine Dateneinheit, die über Netzwerke gesendet wird.

Passphrase: Wird wie ein Passwort verwendet und erleichtert die WEP-Verschlüsselung, indem für Linksys Produkte automatisch WEP-Verschlüsselungsschlüssel erstellt werden.

PEAP (***P**rotected **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifzierungsmethode, bei der eine Kombination aus digitalen Zertifikaten und einem anderen System, z. B. Passwörter, verwendet wird.

Ping (***P**acket **IN**ternet **G**roper*): Ein Internetdienstprogramm, mit dem ermittelt werden kann, ob eine bestimmte IP-Adresse online ist.

PoE (***P**ower **o**ver **E**thernet*): Eine Technologie, mit der über Ethernet-Netzwerkkabel sowohl Daten als auch Strom übertragen werden kann.

POP3 (***P**ost **O**ffice **P**rotocol **3***): Ein im Internet verbreitet eingesetzter Standard-Mail-Server.

Port: Der Anschlusspunkt an einem Computer oder Netzwerkbetriebsgerät, an den Kabel oder Adapter angeschlossen werden.

PPPoE (***P**oint to **P**oint **P**rotocol **o**ver **E**thernet*): Eine Art der Breitbandverbindung, die neben der Datenübertragung eine Authentifizierungsmöglichkeit (Benutzername und Passwort) bietet.

PPTP (***P**oint-to-**P**oint **T**unneling **P**rotocol*): Ein VPN-Protokoll, mit dem das Point-to-Point-Protokoll (PPP) über einen Tunnel durch das IP-Netzwerk geleitet werden kann. Dieses Protokoll wird darüber hinaus in Europa als eine Art der Breitbandverbindung verwendet.

Präambel: Teil des Wireless-Signals, mit dem der Netzwerkdatenverkehr synchronisiert wird.

Puffer: Puffer sind freigegebene oder zugewiesene Speicherbereiche zur Unterstützung und Koordinierung von verschiedenen Computer- und Netzwerkaktivitäten, damit sich diese nicht gegenseitig behindern oder aufhalten.

RADIUS (***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*): Ein Protokoll zur Überwachung des Netzwerkzugriffs mithilfe eines Authentifizierungsservers.

RJ-45 (***R**egistered **J**ack-**45***): Ethernet-Anschluss für bis zu acht Drähte.

Roaming: Die Möglichkeit, mit einem Wireless-Gerät aus einem Access Point-Bereich in einen anderen zu wechseln, ohne dass die Verbindung unterbrochen wird.

Router: Ein Netzwerkgerät, mit dem mehrere Netzwerke miteinander verbunden werden.

RTS (***R**equest **T**o **S**end*): Eine Methode zur Koordination von großen Datenpaketen in einem Netzwerk mithilfe der RTS-Schwelle.

Server: Ein beliebiger Computer, der innerhalb eines Netzwerks dafür sorgt, dass Benutzer auf Dateien zugreifen, kommunizieren sowie Druckvorgänge und andere Aktionen ausführen können.

SMTP (***S**imple **M**ail **T**ransfer **P**rotocol*): Das standardmäßige E-Mail-Protokoll im Internet.

SNMP (***S**imple **N**etwork **M**anagement **P**rotocol*): Ein weit verbreitetes und häufig verwendetes Protokoll zur Netzwerküberwachung und -steuerung.

Software: Befehle für den Computer. Ein Satz an Befehlen, mit denen eine bestimmte Aufgabe ausgeführt wird, bezeichnet man als „Programm“.

SOHO (***S**mall **O**ffice/**H**ome **O**ffice*): Marktsegment der Geschäftkunden, die zu Hause oder in kleineren Büros arbeiten.

SPI-Firewall (***S**tateful **P**acket **I**nspection*): Eine Technologie, mit der eingehende Datenpakete vor der Weiterleitung an das Netzwerk überprüft werden.

SSID (***S**ervice **S**et **ID**entifier*): Der Name Ihres Wireless-Netzwerks.

Standard-Gateway: Ein Gerät, über das der Internetdatenverkehr Ihres LANs weitergeleitet wird.

Statische IP-Adresse: Eine feste Adresse, die einem in ein Netzwerk eingebundenen Computer oder Gerät zugewiesen ist.

Statisches Routing: Das Weiterleiten von Daten in einem Netzwerk über einen festen Pfad.

Subnetzmaske: Ein Adressencode, der die Größe des Netzwerks festlegt.

Switch: 1. Ein Daten-Switch, der Rechner mit Host-Computern verbindet, wodurch eine begrenzte Anzahl von Ports von mehreren Geräten gemeinsam genutzt werden kann. 2. Ein Gerät zum Herstellen, Trennen und Ändern der Verbindungen innerhalb von elektrischen Schaltkreisen (Schalter).

TCP (***T**ransmission **C**ontrol **P**rotocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem eine Bestätigung des Empfängers der gesendeten Daten erforderlich ist.

TCP/IP (***T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol*): Ein Satz von Anweisungen, den alle PCs für die Kommunikation über Netzwerke verwenden.

Telnet: Benutzerbefehl und TCP/IP-Protokoll zum Zugriff auf Remote-PCs.

TFTP (***T**rivial **F**ile **T**ransfer **P**rotocol*): Eine Version des TCP/IP-FTP-Protokolls, das über keinerlei Verzeichnis- oder Passwortfunktionalitäten verfügt.

TKIP (***T**emporal **K**ey **I**ntegrity **P**rotocol*): Eine Wireless-Verschlüsselungsmethode, bei der für jedes übertragene Datenpaket dynamische Verschlüsselungsschlüssel zur Verfügung stehen.

Topologie: Die physische Anordnung eines Netzwerks.

TX-Rate: Übertragungsrate.

UDP (***U**ser **D**atagram **P**rotocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem keine Bestätigung vom Empfänger der gesendeten Daten erforderlich ist.

URL (***U**niform **R**esource **L**ocator*): Die Adresse einer im Internet befindlichen Datei.

Verschlüsselung: Die Codierung von Daten, die über Netzwerke übertragen werden.

Vollduplex: Die Fähigkeit eines Netzwerkgeräts, Daten gleichzeitig empfangen und übertragen zu können.

VPN (***V**irtual **P**rivate **N**etwork*): Eine Sicherheitsmaßnahme, mit der Daten geschützt werden, wenn sie über das Internet von einem Netzwerk in ein anderes übertragen werden.

WAN (***W**ide **A**rea **N**etwork*): Das Internet.

WEP (**W***ired **E**quivalent **P**rivacy*): Eine hochgradig sichere Methode zum Verschlüsseln von Netzwerkdaten, die in Wireless-Netzwerken übertragen werden.

WINIPCFG: Ein Dienstprogramm für Windows 98 und Windows ME, das die IP-Adresse für ein bestimmtes Netzwerkgerät anzeigt.

WLAN (***W**ireless **L**ocal **A**rea **N**etwork*): Mehrere Computer und Geräte, die über Wireless-Verbindungen miteinander kommunizieren.

WPA (***W**i-Fi **P**rotected **A**ccess*): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (*Temporal Key Integrity Protocol*) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann.

Anhang F: Spezifikationen

Modellnummer	WAG54GX2
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, IEEE 802.3, g.992.1 (g.dmt), g.992.2 (g.lite), g.992.3, g.992.5, T1.413i2
Ports	Netzstrom, ADSL, Ethernet (1-4)
Tasten	Reset, Ein/Aus-Schalter
Kabeltyp	Kat. 5 UTP
LEDs	Netzstrom, Wireless, Ethernet (1-4), DSL, Internet
Anzahl der Antennen	2
Antennenanschluss-Typ	Fest (nicht abnehmbar)
RF-Leistung (EIRP) in dBm	802.11b: 18, 802.11g: 16, 802.11g MIMO: 17
Antennengewinn in dBi	3,3
UPnP-fähig/ -zertifiziert	UPnP-fähig

Sicherheitsmerkmale	Passwortgeschützte Konfiguration für Web-Zugriff PAP- und CHAP-Authentifizierung DoS-Schutz (*Denial of Service*) URL-Filterung sowie Blockieren von Stichwörtern, Java, ActiveX, Proxy und Cookies ToD-Filter (Blockieren des Zugriffs nach Zeit) VPN-Passthrough für IPSec-, PPTP- und L2TP-Protokolle WEP (128/64 Bit) mit Passphrasen-/WEP-Schlüsselerstellung Deaktivierung der SSID-Übertragung Zugriffsbeschränkung nach MAC- und IP-Adressen Unterstützung von bis zu 5 IPsec VPN-Terminal-Tunneln Unterstützung für WPA und WPA2
WEP-Schlüssel	64 Bit, 128 Bit
Abmessungen	140 mm x 140 mm x 27 mm
Gewicht	0,27 kg
Stromversorgung	12 V=, 1 A
Zertifizierungen	CE
Betriebstemperatur	0 ºC bis 40 ºC
Lagertemperatur	-20 ºC bis 70 ºC
Betriebsfeuchtigkeit	10 % bis 85 %, nicht kondensierend
Lagerfeuchtigkeit	5 % bis 90 %, nicht kondensierend

Anhang G: Garantieinformationen

Linksys sichert Ihnen für einen Zeitraum von drei Jahren (die „Gewährleistungsfrist“) zu, dass dieses Linksys Produkt bei normaler Verwendung keine Material- oder Verarbeitungsfehler aufweist. Im Rahmen dieser Gewährleistung beschränken sich Ihre Rechtsmittel und der Haftungsumfang von Linksys wie folgt: Linksys kann nach eigener Wahl das Produkt reparieren oder austauschen oder Ihnen den Kaufpreis abzüglich etwaiger Nachlässe zurückerstatten. Diese eingeschränkte Gewährleistung gilt nur für den ursprünglichen Käufer.

Sollte sich das Produkt während der Gewährleistungsfrist als fehlerhaft erweisen, wenden Sie sich an den technischen Support von Linksys, um eine so genannte *Return Authorization Number* (Nummer zur berechtigten Rücksendung) zu erhalten. WENN SIE SICH AN DEN TECHNISCHEN SUPPORT WENDEN, SOLLTEN SIE IHREN KAUFBELEG ZUR HAND HABEN. Wenn Sie gebeten werden, das Produkt einzuschicken, geben Sie die Nummer zur berechtigten Rücksendung gut sichtbar auf der Verpackung an, und legen Sie eine Kopie des Originalkaufbelegs bei. RÜCKSENDEANFRAGEN KÖNNEN NICHT OHNE DEN KAUFBELEG BEARBEITET WERDEN. Der Versand fehlerhafter Produkte an Linksys erfolgt auf Ihre Verantwortung. Linksys kommt nur für Versandkosten von Linksys zu Ihrem Standort per UPS auf dem Landweg auf. Bei Kunden außerhalb der USA und Kanadas sind sämtliche Versand- und Abfertigungskosten durch die Kunden selbst zu tragen.

ALLE GEWÄHRLEISTUNGEN UND BEDINGUNGEN STILLSCHWEIGENDER ART HINSICHTLICH DER MARKTÜBLICHEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUF DIE DAUER DER GEWÄHRLEISTUNGSFRIST BESCHRÄNKT. JEGLICHE WEITEREN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN SOWOHL AUSDRÜCKLICHER ALS AUCH STILLSCHWEIGENDER ART, EINSCHLIESSLICH JEGLICHER STILLSCHWEIGENDER GEWÄHRLEISTUNG DER NICHTVERLETZUNG, WERDEN AUSGESCHLOSSEN. Einige Gerichtsbarkeiten gestatten keine Beschränkungen hinsichtlich der Gültigkeitsdauer einer stillschweigenden Gewährleistung; die oben genannte Beschränkung findet daher unter Umständen auf Sie keine Anwendung. Die vorliegende Gewährleistung sichert Ihnen bestimmte gesetzlich verankerte Rechte zu. Darüber hinaus stehen Ihnen je nach Gerichtsbarkeit unter Umständen weitere Rechte zu.

Diese Gewährleistung gilt nicht, wenn das Produkt (a) von einer anderen Partei als Linksys verändert wurde, (b) nicht gemäß den von Linksys bereitgestellten Anweisungen installiert, betrieben, repariert oder gewartet wurde oder (c) unüblichen physischen oder elektrischen Belastungen, Missbrauch, Nachlässigkeit oder Unfällen ausgesetzt wurde. Darüber hinaus kann Linksys angesichts der ständigen Weiterentwicklung neuer Methoden zum unerlaubten Zugriff und Angriff auf Netzwerke nicht gewährleisten, dass das Produkt keinerlei Schwachstellen für unerlaubte Zugriffe oder Angriffe bietet.

SOWEIT NICHT GESETZLICH UNTERSAGT, SCHLIESST LINKSYS JEGLICHE HAFTUNG FÜR VERLOREN GEGANGENE DATEN, ENTGANGENE EINNAHMEN, ENTGANGENE GEWINNE ODER SONSTIGE SCHÄDEN BESONDERER, INDIREKTER, MITTELBARER, ZUFÄLLIGER ODER BESTRAFENDER ART AUS, DIE SICH AUS DER VERWENDUNG BZW. DER NICHTVERWENDBARKEIT DES PRODUKTS (AUCH DER SOFTWARE) ERGEBEN ODER MIT DIESER ZUSAMMENHÄNGEN, UNABHÄNGIG VON DER HAFTUNGS-THEORIE (EINSCHLIESSLICH NACHLÄSSIGKEIT), AUCH WENN LINKSYS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. DIE HAFTUNG VON LINKSYS IST STETS AUF DEN FÜR DAS PRODUKT GEZAHLTEN BETRAG BESCHRÄNKT. Die oben genannten Beschränkungen kommen auch dann zur Anwendung, wenn eine in diesem Abschnitt aufgeführte Gewährleistung oder Zusicherung ihren wesentlichen Zweck verfehlt. Einige Gerichtsbarkeiten gestatten keinen Ausschluss von bzw. keine Beschränkungen auf zufällige oder Folgeschäden; die oben genannte Beschränkung oder der oben genannte Ausschluss findet daher unter Umständen auf Sie keine Anwendung.

Die vorliegende Gewährleistung ist nur in dem Land gültig bzw. kann nur in dem Land verarbeitet werden, in dem das Produkt erworben wurde.

Richten Sie alle Anfragen direkt an: Linksys, P.O. Box 18558, Irvine, CA 92623, USA

Anhang H: Zulassungsinformationen

FCC-Bestimmungen

Dieses Gerät wurde geprüft und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Die Grenzwerte wurden so festgelegt, dass ein angemessener Schutz gegen Störungen in einer Wohngegend gewährleistet ist. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese abstrahlen. Wird es nicht gemäß den Angaben des Herstellers installiert und betrieben, kann es sich störend auf den Rundfunk- und Fernsehempfang auswirken. Es besteht jedoch keine Gewähr, dass bei einer bestimmten Installation keine Störungen auftreten. Sollte dieses Gerät Störungen des Radio- und Fernsehempfangs verursachen (was durch Ein- und Ausschalten des Geräts feststellbar ist), wird der Benutzer aufgefordert, die Störungen durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus, oder stellen Sie sie an einem anderen Ort auf.
- Increase the separation between the equipment or devices.
- Schließen Sie das Gerät an eine anderen Anschluss als den des Empfängers an.
- Wenden Sie sich bei Fragen an Ihren Händler oder an einen erfahrenen Funk-/Fernsehtechniker.

FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung

Dieses Gerät erfüllt die FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung in einer nicht gesteuerten Umgebung. Dieses Gerät sollte so installiert und betrieben werden, dass der Abstand zwischen dem Radiator und Personen mindestens 20 cm beträgt.

INDUSTRY CANADA (CANADA)

Dieses Gerät erfüllt die kanadischen Bestimmungen der Richtlinien ICES-003 und RSS210.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry Canada.

Informationen zur Einhaltung gesetzlicher Vorschriften bei 2,4-GHz-Wireless-Produkten für den Bereich der EU und anderer Länder gemäß EU-Richtlinie 1999/5/EG (R&TTE-Richtlinie)

Konformitätserklärung zur EU-Richtlinie 1999/5/EG (R&TTE-Richtlinie)

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

HINWEIS: Für alle Produkte ist die Konformitätserklärung in folgender Form verfügbar:

- PDF-Datei auf der Produkt-CD.
- Druckversion im Lieferumfang des Produkts.
- PDF-Datei auf der Produkt-Webseite. Rufen Sie www.linksys.com/international auf, und wählen Sie das für Sie zutreffende Land bzw. die entsprechende Region aus. Wählen Sie dann Ihr Produkt aus.

Wenn Sie weitere technische Dokumente benötigen, finden Sie entsprechende Hinweise im Abschnitt „Technische Dokumente unter www.linksys.com/international“ weiter hinten in diesem Anhang.

Bei der Bewertung des Produkts hinsichtlich der Anforderungen der Richtlinie 1999/5/EG kamen die folgenden Standards zur Anwendung:

- Funkausrüstung: EN 300 328
- EMV: EN 301 489-1, EN 301 489-17
- Sicherheit: EN 60950

CE-Kennzeichnung

Die Wireless-B- und Wireless-G-Produkte von Linksys sind mit der folgenden CE-Kennzeichnung, der Nummer der Überwachungs- und Zertifizierungsstelle (sofern zutreffend) und der Kennung der Klasse 2 versehen.

CE 0560 ! oder CE 0678 ! oder CE !

Überprüfen Sie das CE-Etikett auf dem Produkt, um die Überwachungs- und Zertifizierungsstelle zu ermitteln, die in die Bewertung einbezogen wurde.

Nationale Beschränkungen

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU-Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten, die der EU-Richtlinie 1999/5/EG folgen), mit Ausnahme der folgenden Staaten:

Belgien

Wireless-Verbindungen im Freien mit einer Reichweite über 300 m müssen beim Belgischen Institut für Postdienste und Telekommunikation (BIPT) angemeldet werden. Weitere Informationen finden Sie unter http://www.bipt.be.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Frankreich

Bei Verwendung des Produkts im Freien gelten für die Ausgangsleistung in bestimmten Bandbereichen Beschränkungen. Weitere Informationen finden Sie in Tabelle 1 oder unter http://www.art-telecom.fr/.

Dans le cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez http://www.art-telecom.fr/ pour de plus amples détails.

Tabelle 1: In Frankreich zulässige Leistungspegel

Standort	**Frequenzbereich (MHz)**	**Leistung (EIRP; *Effective Isotropic Radiated Power*)**
In Gebäuden (keine Beschränkungen)	2400-2483,5	100 mW (20 dBm)
Im Freien	2400-2454 2454-2483,5	100 mW (20 dBm) 10 mW (10 dBm)

Italien

Dieses Produkt entspricht den nationalen Vorschriften für Funkschnittstellen und den in der nationalen Frequenzzuweisungstabelle für Italien aufgeführten Anforderungen. Für den Betrieb dieses 2,4-GHz-Wireless-LAN-Produkts außerhalb der Grundstücksgrenzen des Eigentümers ist eine allgemeine Genehmigung erforderlich. Weitere Informationen finden Sie unter http://www.comunicazioni.it/it/.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Beschränkungen hinsichtlich der Verwendung des Produkts

Dieses Produkt wurde ausschließlich für die Verwendung in Gebäuden entwickelt. Die Verwendung im Freien wird nicht empfohlen.

Dieses Produkt wurde für die Verwendung mit der im Lieferumfang enthaltenen standardmäßigen, integrierten bzw. externen (speziell für diesen Zweck vorgesehenen) Antenne entwickelt. Manche Anwendungen setzen jedoch unter Umständen voraus, dass Sie die Antenne(n) vom Produkt trennen (sofern diese abnehmbar sind) und mithilfe eines Verlängerungskabels an einem anderen Ort als das Gerät installieren. Für diese Anwendungen bietet Linksys ein R-SMA-Verlängerungskabel (AC9SMA) und ein R-TNC-Verlängerungskabel (AC9TNC). Beide Kabel sind neun Meter lang. Der Verlust durch das Kabel (die Abschwächung) liegt bei 5 dB. Zur Kompensation der Abschwächung bietet Linksys außerdem die Hochleistungsantennen HGA7S (mit R-SMA-Stecker) und HGA7T (mit R-TNC-Stecker). Diese Antennen verfügen über einen Antennengewinn von 7 dBi und dürfen nur mit dem R-SMA- oder R-TNC-Verlängerungskabel eingesetzt werden.

Kombinationen von Verlängerungskabeln und Antennen, die zu einem ausgestrahlten Leistungspegel von mehr als 100 mW EIRP (*Effective Isotropic Radiated Power*) führen, sind unzulässig.

Ausgangsleistung des Geräts

Zur Einhaltung der jeweiligen nationalen Vorschriften müssen Sie u. U. die Ausgangsleistung Ihres Wireless-Geräts anpassen. Fahren Sie mit dem entsprechenden Abschnitt für Ihr Gerät fort.

HINWEIS: Die Einstellungen für die Ausgangsleistung sind u. U. nicht für alle Wireless-Produkte verfügbar. Weitere Informationen finden Sie in der Dokumentation auf der Produkt-CD oder unter http://www.linksys.com/international.

Wireless-Adapter

Bei Wireless-Adaptern ist die Ausgangsleistung standardmäßig auf 100 % eingestellt. Die Ausgangsleistung der einzelnen Adapter beträgt maximal 20 dBm (100 mW), liegt aber gewöhnlich bei 18 dBm (64 mW) oder darunter. Wenn Sie die Ausgangsleistung Ihres Wireless-Adapters anpassen müssen, befolgen Sie die entsprechenden Anweisungen für das Windows-Betriebssystem Ihres Computers:

Windows XP
1. Doppelklicken Sie auf dem Desktop in der Taskleiste auf das Symbol **Drahtlose Verbindung**.
2. Öffnen Sie das Fenster *Drahtlose Netzwerkverbindung*.
3. Klicken Sie auf die Schaltfläche **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Allgemein** und dann auf die Schaltfläche **Konfigurieren**.
5. Klicken Sie im Fenster *Eigenschaften* auf die Registerkarte **Erweitert**.
6. Wählen Sie **Ausgangsleistung** aus.
7. Wählen Sie aus dem rechts angezeigten Pulldown-Menü den Prozentsatz für die Ausgangsleistung des Wireless-Adapters aus.

Windows 2000

1. Öffnen Sie das Fenster *Systemsteuerung*.
2. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.
3. Wählen Sie Ihre aktuelle Wireless-Verbindung aus, und wählen Sie dann **Eigenschaften**.
4. Klicken Sie im Fenster *Eigenschaften* auf die Schaltfläche **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Erweitert**, und wählen Sie **Ausgangsleistung** aus.
6. Wählen Sie aus dem rechts angezeigten Pulldown-Menü die Leistungseinstellung für den Wireless-Adapter aus.

Wenn auf Ihrem Computer Windows ME oder Windows 98 ausgeführt wird, finden Sie in der Windows-Hilfe Anweisungen zum Aufrufen der erweiterten Einstellungen von Netzwerkadaptern.

Wireless Access Points, Router und andere Wireless-Produkte

Wenn Sie über einen Wireless Access Point, einen Router oder ein anderes Wireless-Produkt verfügen, verwenden Sie das zugehörige webbasierte Dienstprogramm, um die Einstellungen für die Ausgangsleistung zu konfigurieren (weitere Informationen finden Sie in der Dokumentation zum jeweiligen Produkt).

Technische Dokumente unter www.linksys.com/international

Führen Sie die folgenden Schritte aus, um auf die gewünschten technischen Dokumente zuzugreifen:

1. Navigieren Sie mit dem Browser zur Website http://www.linksys.com/international.
2. Klicken Sie auf Ihre Region.
3. Klicken Sie auf den Namen Ihres Landes.
4. Klicken Sie auf **Produkt**.
5. Klicken Sie auf die entsprechende Produktkategorie.
6. Wählen Sie ein Produkt aus.
7. Klicken Sie auf den gewünschten Dokumentationstyp. Das Dokument wird automatisch im PDF-Format geöffnet.

HINWEIS: Wenn Sie Fragen zur Einhaltung gesetzlicher Vorschriften in Bezug auf diese Produkte haben oder die gewünschten Informationen nicht finden können, wenden Sie sich an die Vertriebsniederlassung vor Ort. Weitere Informationen finden Sie unter http://www.linksys.com/international.

Anhang I: Kontaktinformationen

Möchten Sie sich persönlich an Linksys wenden?
Informationen zu den aktuellen Produkten und Aktualisierungen für bereits installierte Produkte finden Sie online unter:
http://www.linksys.com/international

Wenn Sie im Zusammenhang mit Linksys Produkten auf Probleme stoßen, können Sie uns unter folgenden Adressen eine E-Mail senden:

In Europa	E-Mail-Adresse
Belgien	support.be@linksys.com
Dänemark	support.dk@linksys.com
Deutschland	support.de@linksys.com
Frankreich	support.fr@linksys.com
Großbritannien & Irland	support.uk@linksys.com
Italien	support.it@linksys.com
Niederlande	support.nl@linksys.com
Norwegen	support.no@linksys.com
Österreich	support.at@linksys.com
Portugal	support.pt@linksys.com
Schweden	support.se@linksys.com
Schweiz	support.ch@linksys.com
Spanien	support.es@linksys.com

Außerhalb von Europa	E-Mail-Adresse
Asien-Pazifik	asiasupport@linksys.com (nur Englisch)
Lateinamerika	support.portuguese@linksys.com oder support.spanish@linksys.com
Naher Osten und Afrika	support.mea@linksys.com (nur Englisch)
USA und Kanada	support@linksys.com

LINKSYS®
A Division of Cisco Systems, Inc.

2,4 GHz 802.11g

Sans fil - G

Sans fil

Modem routeur ADSL avec SRX200

Guide utilisateur

Modèle **WAG54GX2 (FR)**

CISCO SYSTEMS

Copyright et marques commerciales

Les spécifications peuvent être modifiées sans préavis. Linksys est une marque déposée ou une marque commerciale de Cisco Systems, Inc. et/ou ses filiales aux Etats-Unis et dans certains autres pays.

Comment utiliser le présent Guide de l'utilisateur ?

Ce guide présentant le modem routeur ADSL sans fil G avec SRX200 a été conçu pour faciliter au maximum votre compréhension de la mise en réseau à l'aide du modem routeur. Les symboles suivants sont contenus dans ce guide de l'utilisateur :

Cette coche indique un élément qui mérite une attention plus particulière lors de l'utilisation de votre votre modem routeur.

Ce point d'exclamation indique un avertissement et vous avertit de la possibilité d'endommagement de votre installation ou de votre modem routeur.

Ce point d'interrogation indique un rappel concernant quelque chose que vous êtes susceptible de devoir faire pour utiliser votre modem routeur.

Outre ces symboles, des définitions concernant des termes techniques sont présentées de la façon suivante :

mot : *définition.*

Chaque figure (diagramme, capture d'écran ou toute autre image) est accompagnée d'un numéro et d'une description, comme ceci : **Figure 0-1 : Exemple de description de figure**

Les numéros de figures et les descriptions sont également répertoriés dans la section « Liste des figures » de la « Table des matières ».

Table des matières

Liste des Figures

Chapitre 1 : Introduction

Bienvenue

Merci d'avoir choisi le modem routeur ADSL sans fil G avec SRX200. Avec cette ce modem routeur, vous êtes en mesure d'équiper vos ordinateurs d'une connexion Internet haut débit et d'autres ressources, telles que fichiers et imprimantes.

Comment le modem routeur peut-elle vous offrir tous ces avantages ? Une fois le modem routeur connectée à Internet, ainsi qu'à vos ordinateurs et périphériques, elle est en mesure de diriger et de contrôler les communications de votre réseau. En outre, s'agissant d'un modem routeur sans fil, vous pouvez partager cet accès Internet sur le réseau câblé ou via la diffusion sans fil.

le modem routeur sans fil G avec SRX200 associe la technologie d'antenne intelligente SRX et la mise en réseau standard sans fil G (802.11g). En superposant les signaux de deux émissions radio sans fil G, la technologie MIMO (Multiple In, Multiple Out) double efficacement le débit des données. Contrairement aux technologies de mise en réseau sans fil ordinaire qui sont brouillées par les réflexions de signaux, la technologie MIMO utilise ces réflexions pour augmenter l'étendue et réduire les zones inaccessibles dans la zone de couverture sans fil. Ce signal fort voyage plus loin, tout en assurant une portée des connexions sans fil deux fois plus grande par rapport au signal sans fil G standard. Plus vous vous trouvez loin, plus vous tirez profit de cette technologie. Dans certains cas, le débit de données plus élevé et la technologie se basant sur la réflexion assurent un débit six fois plus rapide qu'avec la technologie sans fil G. le modem routeur évite les interférences en basculant automatiquement vers le canal disponible le moins encombré. Même votre équipement sans fil G ou B standard fonctionnera mieux lors de vos communications avec des périphériques équipés de la technologie SRX.

La norme WPA offre des options de sécurité sans fil accrues tandis que la totalité du réseau est protégée par un pare-feu SPI (Stateful Packet Inspection) et la technologie NAT. Vous pouvez en outre protéger votre famille grâce aux fonctions de contrôle parental telles que les restrictions d'accès à Internet et le blocage par mot clé. Facile à utiliser, l'utilitaire Web vous permet d'accéder à ces fonctions de sécurité et aux autres paramètres du modem routeur.

Que signifie tout cela ?

Les réseaux permettent de partager un accès à Internet et des ressources informatiques. Vous pouvez connecter plusieurs ordinateurs à une même imprimante et accéder à des données stockées sur le disque dur d'un autre ordinateur. Les réseaux sont même utilisés pour les jeux vidéo multijoueurs. Outre leur utilité à la maison et au bureau, ils peuvent donc servir à des activités plus ludiques.

802.11b *: norme de mise en réseau sans fil IEEE qui spécifie un débit de transfert de données maximal de 11 Mbit/s et une fréquence de 2,4 GHz.*

802.11g *: norme de mise en réseau sans fil IEEE qui spécifie un débit de transfert de données maximum de 54 Mbit/s, une fréquence de 2,4 GHz et une rétro-compatibilité avec les périphériques 802.11b.*

wpa *(wi-fi protected access) : protocole de sécurité sans fil faisant appel au cryptage TKIP (Temporal Key Integrity Protocol) et pouvant être utilisé en association avec un serveur RADIUS.*

pare-feu spi *(stateful packet inspection) : technologie inspectant les paquets d'informations entrants avant de les autoriser à pénétrer le réseau.*

pare-feu *: mesures de sécurité protégeant les ressources d'un réseau local contre toute intrusion.*

nat *(network address translation) : la technologie NAT permet de convertir les adresses IP d'un réseau local en une adresse IP distincte sur Internet.*

réseau *: plusieurs ordinateurs ou périphériques reliés entre eux dans le but de partager et de stocker des données, ainsi que transmettre des données entre des utilisateurs.*

lan *(réseau local) : ordinateurs et produits composant le réseau que vous installez chez vous ou dans vos locaux professionnels.*

Les ordinateurs reliés à un réseau câblé constituent un réseau local ou LAN. Ils sont connectés par l'intermédiaire de câbles Ethernet, d'où le terme de réseau « câblé ». Les ordinateurs équipés de cartes sans fil peuvent communiquer sans la présence de câbles encombrants. En partageant les mêmes paramètres sans fil conformément à leur rayon de transmission, ils forment un réseau sans fil. On parle parfois de réseau local sans fil ou WLAN. Les fonctions sans fil du modem routeur permettent de relier vos réseaux câblé et sans fil et d'établir une communication entre eux.

Grâce à vos réseaux connectés, câblés et sans fil, et Internet, vous pouvez alors partager des fichiers et l'accès à Internet et même jouer. Simultanément, le modem routeur ADSL sans fil G avec SRX200 protège vos réseaux et empêche tout utilisateur non autorisé et indésirable d'y accéder.

Linksys vous recommande d'utiliser le CD-ROM d'installation pour la première installation du modem routeur. Si vous ne souhaitez pas exécuter l'assistant de configuration disponible sur le CD-ROM d'installation, suivez les instructions de ce Guide pour connecter, installer et configurer le modem routeur pour relier vos différents réseaux. Ces instructions devraient s'avérer suffisantes pour vous permettre de tirer le meilleur parti du modem routeur ADSL sans fil G avec SRX200.

Contenu de ce Guide de l'utilisateur

Ce Guide de l'utilisateur présente les procédures d'installation et d'utilisation du modem routeur ADSL sans fil G avec SRX200.

- Chapitre 1 : Introduction
  Ce chapitre décrit les applications du modem routeur ADSL sans fil G ainsi que le présent Guide de l'utilisateur.

- Chapitre 2 : Planification de la configuration de votre réseau
  Ce chapitre décrit les éléments de base nécessaires à la mise en place d'un réseau.

- Chapitre 3 : Présentation du modem routeur ADSL sans fil - G avec SRX200
  Ce chapitre décrit les caractéristiques physiques du modem routeur.

- Chapitre 4 : Connexion du modem routeur ADSL sans fil - G avec SRX200
  Ce chapitre vous explique pas à pas comment connecter le modem routeur à votre réseau.

- Chapitre 5 : Installation du modem routeur ADSL sans fil - G avec SRX200
  Ce chapitre vous explique comment installer le modem routeur à l'aide de l'assistant de configuration.

- Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200
  Ce chapitre vous explique comment configurer le modem routeur à l'aide de l'utilitaire Web.

- Annexe A : Dépannage
  Cette annexe expose quelques problèmes et leurs solutions, ainsi que les questions fréquemment posées au sujet de l'installation et de l'utilisation du modem routeur ADSL sans fil G avec SRX200.

- Annexe B : Sécurité sans fil
  Cette annexe décrit les risques liés aux réseaux sans fil et propose quelques solutions en vue de réduire ces risques.

- Annexe C : Recherche des adresses MAC et IP de votre carte Ethernet
  Cette annexe explique comment rechercher l'adresse MAC de la carte Ethernet de votre ordinateur pour être en mesure d'utiliser la fonctionnalité de filtrage MAC et/ou la fonctionnalité de clonage des adresses MAC du modem routeur.

- Annexe D : Mise à niveau du micrologiciel
  Cette annexe vous explique comment mettre à niveau le micrologiciel sur votre modem routeur si cette opération s'avère nécessaire.

- Annexe E : Glossaire
  Cette annexe propose un glossaire des termes fréquemment utilisés dans le cadre des réseaux.

- Annexe F : Spécifications
  Cette annexe décrit les spécifications techniques du modem routeur.

- Annexe G : Informations de garantie
  Cette annexe fournit des informations relatives à la garantie du modem routeur.

- Annexe H : Réglementation
  Cette annexe fournit des informations relatives à la réglementation qui régit l'utilisation du modem routeur.

- Annexe I : Contacts
  Cette annexe fournit des informations sur diverses ressources Linksys que vous pouvez contacter, notamment le Support technique.

Chapitre 2 : Planification de la configuration de votre réseau

Les fonctions du modem routeur

Un modem routeur est un périphérique réseau qui connecte deux réseaux entre eux.

Dans ce cas, le modem routeur connecte à Internet votre réseau local (LAN) ou un groupe d'ordinateurs situés à votre bureau ou à votre domicile. le modem routeur traite et régule les données transmises entre ces deux réseaux.

La fonctionnalité NAT du modem routeur protège votre réseau d'ordinateurs, de manière à ce que les utilisateurs Internet publics ne puissent pas « voir » vos ordinateurs. De cette façon, votre réseau reste privé. le modem routeur protège votre réseau en inspectant chaque paquet entrant via le port Internet avant qu'il soit transmis vers la machine appropriée du réseau. le modem routeur inspecte les services du port Internet tels que le serveur Web, le serveur FTP ou toute autre application Internet. S'il est autorisé à le faire, il transmet ensuite le paquet à l'ordinateur approprié du réseau local.

N'oubliez pas que les ports du modem routeur sont connectés à deux « côtés ». Les ports LAN sont connectés à votre réseau local (LAN) et le port ADSL est connecté à Internet. Les ports LAN transmettent les données à un débit de 10/100 Mbit/s.

Figure 2-1 : Réseau

Adresses IP

Qu'est ce qu'une adresse IP ?

IP signifie Internet Protocol. Chaque périphérique d'un réseau basé sur des adresses IP, comprenant des ordinateurs, des serveurs d'impression et des modems routeurs, requiert une adresse IP pour l'identification de son « emplacement » ou adresse sur le réseau. Elle s'applique aux connexions LAN et Internet. Il existe deux façons d'attribuer une adresse IP à vos périphériques réseau. Vous pouvez attribuer des adresses IP statiques ou utiliser le modem routeur pour attribuer dynamiquement ces adresses IP.

Adresses IP statiques

Une adresse IP statique est une adresse IP fixe que vous attribuez manuellement à un ordinateur ou à un autre périphérique du réseau. Etant donné qu'une adresse IP statique reste valide jusqu'à ce que vous la désactiviez, l'utilisation d'une adresse IP statique permet de s'assurer que le périphérique correspondant aura toujours la même adresse IP tant que vous ne la changez pas. Les adresses IP statiques doivent être uniques et sont

***ip** (internet protocol) : protocole utilisé pour transmettre des données sur un réseau.*

REMARQUE : Etant donné que le modem routeur est un périphérique connecté à deux réseaux, il requiert deux adresses IP : une pour le réseau local et une pour Internet. Dans ce Guide de l'utilisateur, vous trouverez des références à « l'adresse IP Internet » et à « l'adresse IP LAN ».

Puisque le modem routeur utilise la technologie NAT, la seule adresse IP de votre réseau qui peut être « vue » à partir d'Internet est l'adresse IP Internet du modem routeur. Néanmoins, même cette adresse IP peut être bloquée, afin que le modem routeur et le réseau soient invisibles sur Internet. Reportez-vous à l'onglet Security - Firewall (Sécurité - Pare-feu) du « Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200 ».

généralement utilisées avec des périphériques réseau tels que les serveurs d'ordinateurs ou les serveurs d'impression.

Etant donné que vous utilisez le modem routeur pour partager votre connexion Internet DSL, contactez votre fournisseur d'accès Internet pour savoir si une adresse IP statique a été attribuée à votre compte. Si c'est le cas, vous aurez besoin de cette adresse IP statique lors de la configuration du modem routeur. Vous pouvez obtenir cette information en contactant votre fournisseur d'accès Internet.

Adresses IP dynamiques

Une adresse IP dynamique est automatiquement attribuée à un périphérique du réseau, tel que des ordinateurs et des serveurs d'impression. Ces adresses IP sont dites « dynamiques » car elles sont attribuées temporairement à l'ordinateur ou au périphérique. Après un certain temps, elles expirent et peuvent être modifiées. Si un ordinateur se connecte au réseau (ou à Internet) et que son adresse IP dynamique a expiré, le serveur DHCP lui attribue automatiquement une nouvelle adresse IP dynamique.

Serveurs DHCP (Dynamic Host Configuration Protocol)

Les ordinateurs et tous les autres périphériques réseau utilisant des adresses IP dynamiques se voient attribuer une nouvelle adresse IP par un serveur DHCP. L'ordinateur ou le périphérique réseau qui obtient une adresse IP est appelé le client DHCP. DHCP vous évite d'avoir à attribuer des adresses IP manuellement dès qu'un nouvel utilisateur est ajouté à votre réseau.

Un serveur DHCP peut être soit un ordinateur dédié du réseau, soit un autre périphérique réseau, telle que le modem routeur. Par défaut, la fonction de serveur DHCP du modem routeur est activée.

Si vous disposez déjà d'un serveur DHCP sur votre réseau, vous devez désactiver l'un des deux serveurs DHCP. Si vous exécutez plusieurs serveurs DHCP sur votre réseau, des erreurs se produisent, telles que des conflits d'adresses IP. Pour désactiver la fonction DHCP sur le modem routeur, reportez-vous à la section DHCP du « Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200 ».

Chapitre 3 : Présentation du modem routeur ADSL sans fil - G avec SRX200

Ports et bouton Reset (Réinitialisation) du panneau latéral

Les ports et le bouton Reset (Réinitialisation) sont situés sur un côté latéral du modem routeur.

Figure 3-1 : Ports et bouton Reset (Réinitialisation) du panneau latéral

Line (Ligne)	Le port **Line** (Ligne) permet de connecter la ligne ADSL.
Ethernet (1-4)	Les ports **Ethernet** permettent de connecter l'appareil à vos ordinateurs et à d'autres périphériques réseau.
Bouton Reset appuyez (Réinitialisation)	Il existe deux façons de réinitialiser les paramètres d'usine de votre modem routeur : sur le bouton **Reset** (Réinitialiser) pendant environ cinq secondes ou restaurez les paramètres par défaut à partir de l'écran *Factory Defaults* (Paramètres usine) de l'onglet Administration de l'utilitaire Web du modem routeur.
Power (Alimentation)	Le port **Power** (Alimentation) doit être raccordé à l'adaptateur électrique.

IMPORTANT : La réinitialisation du modem routeur vers les paramètres d'usine supprime tous les paramètres personnalisés (connexion Internet, sans fil et autres). Ne réinitialisez pas les paramètres du modem routeur si vous souhaitez les conserver.

Voyants du panneau latéral

Les voyants du modem routeur qui indiquent l'activité du réseau se trouvent sur le panneau latéral.

Figure 3-2 : Voyants du panneau latéral

Bouton (POWER) (Alimentation) — Lorsque vous souhaitez mettre sous/hors tension le modem routeur, appuyez sur ce bouton.

POWER (Alimentation) — Vert. Le voyant **POWER** (Alimentation) s'allume lorsque le modem routeur est sous tension.

WIRELESS (sans fil) — Vert. Le voyant **WIRELESS** (Sans fil) s'allume lorsqu'une connexion sans fil est établie. Si le voyant clignote, cela signifie que le modem routeur traite actuellement l'envoi ou la réception de données avec l'un des périphériques du réseau.

ETHERNET (1-4) — Vert. Le voyant **ETHERNET** a deux fonctions. S'il est allumé en permanence, cela signifie que le modem routeur est connectée correctement à un périphérique via le port Ethernet. S'il clignote, il indique une activité réseau.

DSL — Vert. Le voyant **DSL** s'allume lorsqu'une connexion DSL est réalisée avec succès. Il clignote lorsque le modem routeur établit la connexion ADSL.

INTERNET — Vert. Le voyant **INTERNET** est vert lorsqu'une connexion au fournisseur d'accès Internet (FAI) a été établie. Le voyant INTERNET est rouge si la connexion au fournisseur d'accès Internet (FAI) a échoué.

Chapitre 4 : Connexion du modem routeur ADSL sans fil - G avec SRX200

Présentation

Le technicien de votre fournisseur d'accès Internet doit vous avoir communiqué les données concernant le modem après avoir installé votre connexion large bande. Dans le cas contraire, contactez votre FAI.

Si vous disposez des informations de configuration correspondant à votre type de connexion Internet, vous pouvez commencer l'installation et la configuration de votre modem routeur.

Si vous souhaitez utiliser un ordinateur équipé d'une carte Ethernet pour configurer le modem routeur, passez à la rubrique « Connexion câblée à un ordinateur ». Si vous souhaitez utiliser un ordinateur équipé d'une carte sans fil pour configurer le modem routeur, passez à la rubrique « Connexion sans fil à un ordinateur ».

Connexion câblée à un ordinateur

1. Assurez-vous que tous les appareils du réseau sont hors tension, y compris le modem routeur et tous les ordinateurs.
2. Branchez un câble téléphonique entre le port Line (Ligne) du panneau latéral du modem routeur et la prise murale de la ligne ADSL. Il peut être nécessaire de placer un petit périphérique appelé microfiltre (non fourni) entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.

REMARQUE : Il peut être nécessaire de placer un petit périphérique appelé microfiltre (non fourni) entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.

IMPORTANT : Dans les pays où les prises téléphoniques sont utilisées avec des connecteurs RJ-11, veillez à placer les microfiltres entre le téléphone et la prise murale et **non pas** entre le modem routeur et la prise murale. Sinon, la connexion ADSL ne pourra pas être établie.

Dans les pays où les prises téléphoniques **ne sont pas** utilisées avec des connecteurs RJ-11 (par exemple, France, Suède, Suisse, Royaume-Uni, etc.), sauf pour les utilisateurs RNIS, le microfiltre doit être placé entre le modem routeur et la prise murale, car il contient le connecteur RJ-11.

Les utilisateurs de Annex B (versions E1 et DE du modem routeur) doivent utiliser le câble spécial fourni pour connecter le modem routeur à la prise murale (RJ-45 vers RJ-12). Si vous avez besoin

Figure 4-1 : Connexion d'une ligne ADSL

3. Reliez une extrémité d'un câble réseau Ethernet à l'un des ports Ethernet (numérotés de 1 à 4) situés sur le panneau arrière du modem routeur et l'autre extrémité au port Ethernet d'un ordinateur.

   Procédez de même pour relier d'autres ordinateurs, un commutateur ou des périphériques réseau au modem routeur.

Figure 4-2 : Connexion d'un ordinateur

4. Connectez l'adaptateur électrique fourni au port Power (Alimentation) du modem routeur, puis branchez-le sur une prise secteur.

REMARQUE : Branchez toujours l'adaptateur électrique du modem routeur sur une barrette de connexion protégée contre les surtensions.

   Le voyant d'alimentation (Power) situé sur le panneau avant s'illumine en vert dès que l'adaptateur électrique est correctement connecté. Le voyant d'alimentation clignote pendant quelques secondes puis reste allumé une fois le test d'autodiagnostic terminé. Si le voyant clignote pendant au moins une minute, reportez-vous à l'« Annexe A : Dépannage ».

Figure 4-3 : Connexion de l'alimentation

5. Allumez un des ordinateurs connectés au modem routeur.

Allez au « Chapitre 5 : Installation du modem routeur ADSL sans fil - G avec SRX200. »

Connexion sans fil à un ordinateur

Si vous souhaitez utiliser une connexion sans fil pour accéder au modem routeur, procédez comme suit :

1. Assurez-vous que tous les appareils du réseau sont hors tension, y compris le modem routeur et tous les ordinateurs.
2. Branchez un câble téléphonique entre le port Line (Ligne) du panneau arrière du modem routeur et la prise murale de la ligne ADSL. Il peut être nécessaire de placer un petit périphérique appelé microfiltre (non fourni) entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.

REMARQUE : Il peut être nécessaire de placer un petit périphérique appelé microfiltre (non fourni) entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.

IMPORTANT : Dans les pays où les prises téléphoniques sont utilisées avec des connecteurs RJ-11, veillez à placer les microfiltres entre le téléphone et la prise murale et **non pas** entre le modem routeur et la prise murale. Sinon, la connexion ADSL ne pourra pas être établie.

Dans les pays où les prises téléphoniques **ne sont pas** utilisées avec des connecteurs RJ-11 (par exemple, France, Suède, Suisse, Royaume-Uni, etc.), sauf pour les utilisateurs RNIS, le microfiltre doit être placé entre le modem routeur et la prise murale, car il contient le connecteur RJ-11.

Les utilisateurs de Annex B (versions E1 et DE du modem routeur) doivent utiliser le câble spécial fourni pour connecter le modem routeur à la prise murale (RJ-45 vers RJ-12). Si vous avez besoin de

Figure 4-4 : Connexion d'une ligne ADSL

3. Connectez l'adaptateur électrique fourni au port Power (Alimentation), puis branchez-le sur une prise secteur.

REMARQUE : Branchez toujours l'adaptateur électrique du modem routeur sur une barrette de connexion protégée contre les surtensions.

Le voyant d'alimentation (Power) situé sur le panneau avant s'illumine en vert dès que l'adaptateur électrique est correctement connecté. Le voyant d'alimentation clignote pendant quelques secondes puis reste allumé une fois le test d'autodiagnostic terminé. Si le voyant clignote pendant au moins une minute, reportez-vous à l'« Annexe A : Dépannage ».

Figure 4-5 : Connexion de l'alimentation

4. Allumez un des ordinateurs de votre/vos réseau(x) sans fil.
5. Pour accéder initialement au modem routeur via une connexion sans fil, assurez-vous que le SSID de la carte sans fil est défini à « **linksys** » (paramètre par défaut du modem routeur) et que sa fonction de sécurité sans fil est désactivée. Après avoir accédé au modem routeur, vous pouvez modifier les paramètres du modem routeur et de la carte de cet ordinateur pour qu'ils correspondent à vos paramètres réseau habituels.

REMARQUE : Veillez à toujours modifier le paramètre par défaut, **linksys**, et à activer la sécurité sans fil.

Allez au « Chapitre 5 : Installation du modem routeur ADSL sans fil - G avec SRX200. »

Chapitre 5 : Installation du modem routeur ADSL sans fil G avec SRX200

Présentation

L'assistant de configuration du modem routeur ADSL sans fil G avec SRX200 vous guidera tout au long de la procédure d'installation. Il parcourra les instructions de configuration des paramètres réseau et sans fil du modem routeur.

Utilisation de l'assistant de configuration

1. Insérez le **CD-ROM de l'assistant de configuration** dans le lecteur de CD-ROM. L'assistant de configuration démarre automatiquement et l'écran *Welcome* (Bienvenue) apparaît. Si ce n'est pas le cas, ouvrez le menu **Démarrer** de Windows, puis cliquez sur **Exécuter**. Dans le champ qui apparaît, saisissez **D:\setup.exe** (« D » représentant votre lecteur de CD-ROM).

2. L'assistant de configuration détecte automatiquement les paramètres de langue de votre ordinateur ; si tel n'est pas le cas, sélectionnez une langue parmi les langues disponibles dans le menu déroulant *Language* (Langue). Dans l'écran *Welcome* (Bienvenue) initial, cliquez sur le bouton **Next** (Suivant) pour poursuivre l'exécution de l'assistant de configuration dans la langue en cours. Pour utiliser une autre langue, sélectionnez la langue appropriée, puis cliquez sur le bouton **Next** (Suivant).

3. Dans l'écran *Welcome* (Bienvenue) suivant, cliquez sur le bouton **Click Here to Start** (Cliquez ici pour démarrer). Voici les autres possibilités :

   Norton Internet Security : cliquez sur le bouton **Norton Internet Security** pour installer le logiciel Norton Internet Security.

   User Guide (Guide de l'utilisateur) : cliquez sur ce bouton pour ouvrir le guide de l'utilisateur au format PDF.

   Exit (Quitter) : cliquez sur ce bouton pour quitter l'assistant de configuration.

Figure 5-1 : Ecran Welcome - Language Selection (Bienvenue - Sélection de la langue) de l'assistant de configuration

Figure 5-2 : Ecran Welcome - Start Wizard (Bienvenue - Lancer l'assistant) de l'assistant de configuration

4. Après avoir lu l'accord de licence, cliquez sur **Next** (Suivant) si vous l'acceptez ou sur **Exit** (Quitter) pour terminer l'installation. Cliquez sur **Back** (Précédent) pour revenir à l'écran précédent.

Figure 5-3 : Ecran License Agreement (Accord de licence) de l'assistant de configuration

5. L'assistant de configuration vous demande de déconnecter le modem haut débit de votre ordinateur et la prise murale ADSL. Une fois cette opération terminée, cliquez sur le bouton **Next** (Suivant).

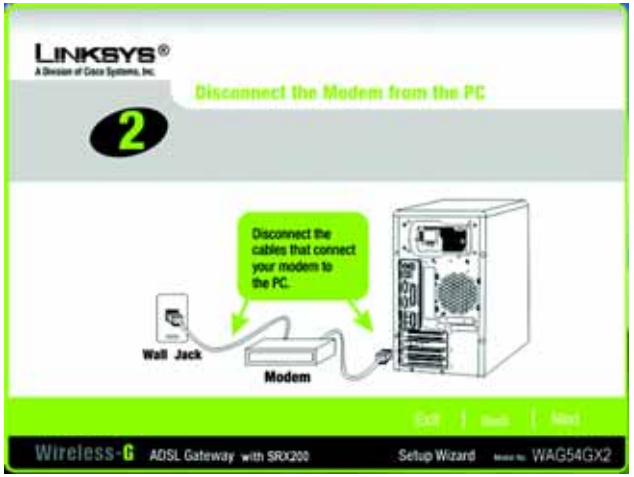


Figure 5-4 : Ecran Disconnect the Modem from the PC and ADSL Wall Jack (Déconnexion du modem du PC et de la prise murale ADSL) de l'assistant de configuration

6. L'assistant de configuration vous demande de connecter votre modem routeur à la prise murale ADSL. Une fois cette opération terminée, cliquez sur le bouton **Next** (Suivant).

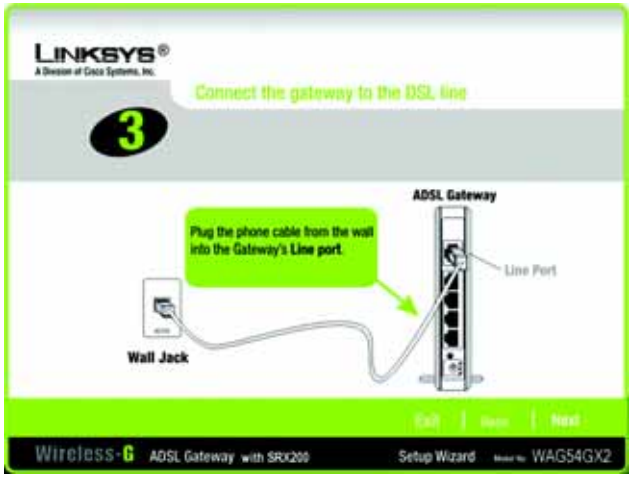


Figure 5-5 : Ecran Connect the Gateway to the ADSL Wall Jack (Connexion du modem routeur à la prise murale ADSL) de l'assistant de configuration

7. L'assistant de configuration vous demande de connecter un câble réseau à votre ordinateur. Une fois cette opération terminée, cliquez sur le bouton **Next** (Suivant).

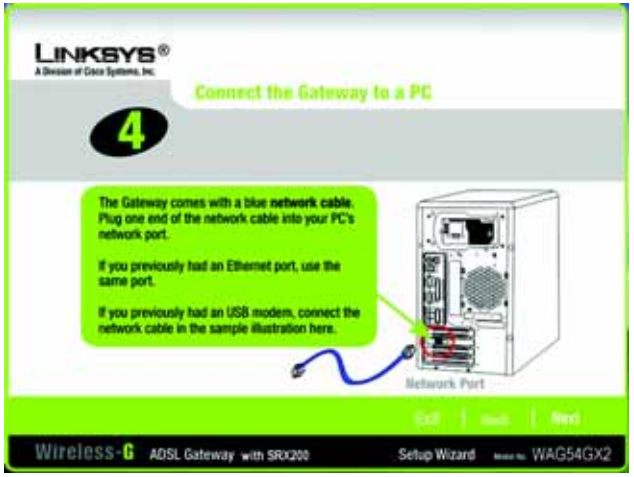


Figure 5-6 : Ecran Connect a Network Cable to a PC (Connexion d'un câble réseau à un ordinateur) de l'assistant de configuration

8. L'assistant de configuration vous demande de connecter l'autre extrémité du câble réseau au modem routeur.

   Vous pouvez alors également connecter d'autres ordinateurs au modem routeur.

   Une fois cette opération terminée, cliquez sur le bouton **Next** (Suivant).

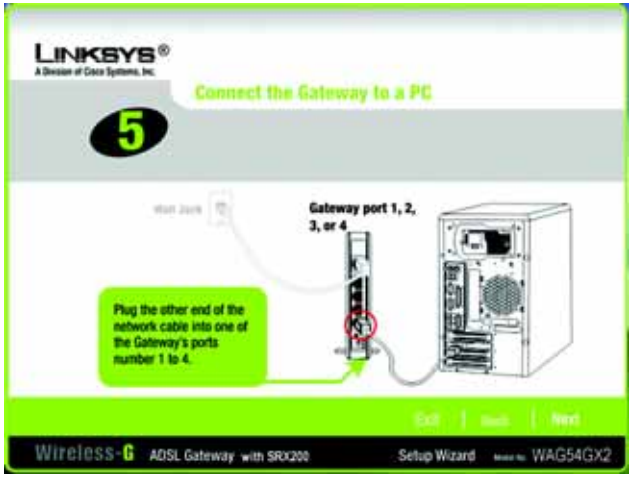


Figure 5-7 : Ecran Connect the Network Cable to the Gateway (Connecter le câble réseau au modem routeur) de l'assistant de configuration

9. L'assistant de configuration vous demande de mettre le modem routeur sous tension. Une fois cette opération terminée, cliquez sur le bouton **Next** (Suivant).

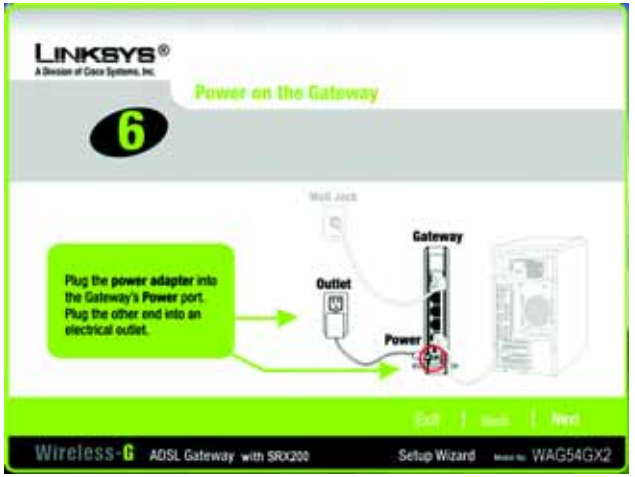


Figure 5-8 : Ecran Power on the Gateway (Mise sous tension du modem routeur) de l'assistant de configuration

10. Veillez à ce que les voyants Power (Alimentation), DSL et numérotés du modem routeur (en fonction du nombre d'ordinateurs connectés) soient allumés sur le panneau avant. Une fois cette opération terminée, cliquez sur le bouton **Next** (Suivant).

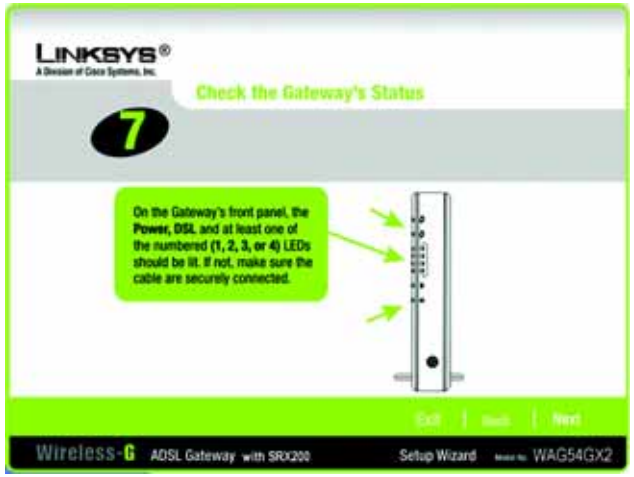


Figure 5-9 : Ecran Check the Gateway's Status (Vérification de l'état du modem routeur) de l'assistant de configuration

11. Il vous est demandé où vous résidez. Sélectionnez le pays souhaité dans le menu déroulant. Cliquez ensuite sur le bouton **Next** (Suivant).

REMARQUE : Si votre pays n'est pas répertorié, configurez vos paramètres à l'aide de l'utilitaire Web du modem routeur. Reportez-vous au « Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200 » pour plus d'instructions.

Figure 5-10 : Ecran Select Your Country (Sélectionner votre pays) de l'assistant de configuration

12. Les fournisseurs d'accès Internet (FAI) de votre pays sont répertoriés. (Les options à l'écran varient en fonction du pays sélectionné dans l'écran précédent.) Cliquez sur le bouton de votre FAI.

    Si votre FAI n'est pas répertorié, cliquez sur le bouton **Next** (Suivant) pour saisir manuellement vos paramètres.

Figure 5-11 : Ecran Select Your Internet Service Provider (Sélection de votre fournisseur d'accès Internet) (Royaume-Uni) de l'assistant de configuration

13. Si besoin est, l'assistant de configuration détecte automatiquement le type d'encapsulation que vous utilisez : 1483 Bridged, 1483 Routed, PPPoA ou PPPoE. Pour saisir manuellement vos paramètres, sélectionnez votre type d'encapsulation : **1483 Bridged**, **1483 Routed**, **PPPoA** ou **PPPoE**.

    REMARQUE : Si votre type d'encapsulation est IPoA ou Bridged Mode Only (Bridged Mode uniquement), vous devez le configurer à l'aide de l'utilitaire Web du modem routeur. Reportez-vous au « Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200 » pour plus d'instructions.

    Reportez-vous à la section consacrée à votre type d'encapsulation.

1483 Bridged

Si vous avez sélectionné votre FAI, l'assistant de configuration sélectionne automatiquement les paramètres d'encapsulation, de VPI, de VCI et de multiplexage. Sélectionnez ensuite le paramètre IP approprié pour votre connexion DSL.

Si vous devez saisir manuellement vos paramètres, utilisez cet écran.

VPI/VCI : si vous devez saisir manuellement vos paramètres, saisissez les paramètres VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier) fourni par votre FAI.

Multiplexing (Multiplexage) : si vous devez saisir manuellement vos paramètres, sélectionnez **LLC** ou **VC**, en fonction de votre FAI.

Auto IP (Adresse IP automatique) : si vous utilisez une adresse IP dynamique, cliquez sur le bouton d'option **Auto IP** (Adresse IP automatique).

Static IP (Adresse IP statique) : si vous utilisez une adresse IP statique, cliquez sur le bouton d'option **Static IP** (Adresse IP statique). Renseignez les champs *IP Address* (Adresse IP), *Subnet Mask* (Masque de sous-réseau), *Default Gateway* (Passerelle par défaut), *Primary DNS* (Domain Name System) (Nom de domaine primaire) et *Secondary DNS* (Nom de domaine secondaire). (Vous devez saisir au moins une adresse IP de serveur DNS.)

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

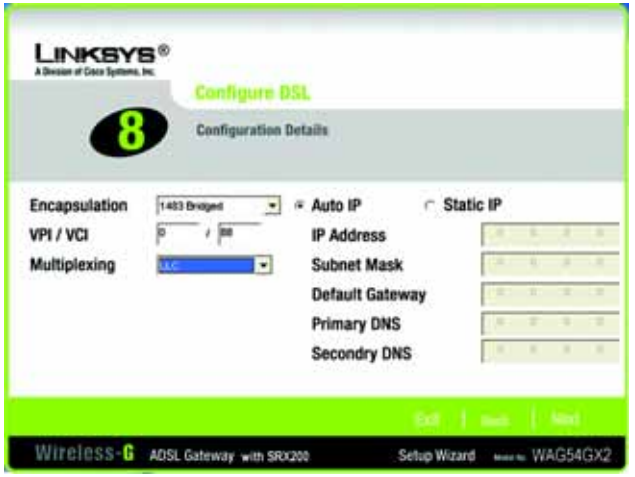


Figure 5-12 : Ecran Configure DSL - 1483 Bridged (Configuration DSL - 1483 Bridged) de l'assistant de configuration

1483 Routed

Si vous avez sélectionné votre FAI, l'assistant de configuration sélectionne automatiquement les paramètres d'encapsulation, de VPI, de VCI et de multiplexage. Saisissez ensuite les paramètres IP appropriés pour votre connexion DSL.

Si vous devez saisir manuellement vos paramètres, utilisez cet écran.

VPI/VCI : si vous devez saisir manuellement vos paramètres, saisissez les paramètres VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier) fourni par votre FAI.

Multiplexing (Multiplexage) : si vous devez saisir manuellement vos paramètres, sélectionnez **LLC** ou **VC**, en fonction de votre FAI.

Static IP (Adresse IP statique) : renseignez les champs *IP Address* (Adresse IP), *Subnet Mask* (Masque de sous-réseau), *Default Gateway* (Passerelle par défaut), *Primary DNS* (Domain Name System) (Nom de domaine primaire) et *Secondary DNS* (Nom de domaine secondaire). (Vous devez saisir au moins une adresse IP de serveur DNS.)

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

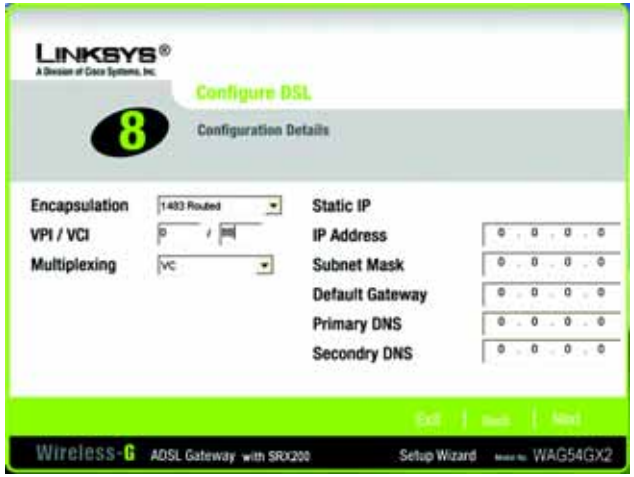


Figure 5-13 : Ecran Configure DSL - 1483 Routed (Configuration DSL - 1483 Routed) de l'assistant de configuration

PPPoA

Si vous avez sélectionné votre FAI, l'assistant de configuration sélectionne automatiquement les paramètres d'encapsulation, de VPI, de VCI et de multiplexage. Saisissez ensuite l'ID d'utilisateur et le mot de passe pour votre connexion DSL.

Si vous devez saisir manuellement vos paramètres, utilisez cet écran.

VPI/VCI : si vous devez saisir manuellement vos paramètres, saisissez les paramètres VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier) fourni par votre FAI.

Multiplexing (Multiplexage) : si vous devez saisir manuellement vos paramètres, sélectionnez **LLC** ou **VC**, en fonction de votre FAI.

User ID (ID d'utilisateur) et **Password** (Mot de passe) : saisissez l'ID d'utilisateur et le mot de passe fournis par votre FAI.

Connection (Connexion) : choisissez l'option **Keep Alive** (Maintien de la connexion) si vous souhaitez toujours être connecté à votre fournisseur d'accès Internet (FAI) ou sélectionnez **Connect on Demand** (Connexion à la demande) si vous êtes facturé pour la durée de connexion à votre FAI.

Keep Alive (Maintien de la connexion) : pour cette option, le modem routeur maintiendra votre connexion Internet et active. Dans le champ *Redial Period* (Rappel après), spécifiez la fréquence à laquelle le modem routeur doit vérifier votre connexion Internet (la valeur par défaut est **5** minutes).

Connect on Demand (Connexion à la demande) : si vous sélectionnez cette option, le modem routeur met fin à votre accès Internet à l'issue d'un laps de temps spécifique, que vous pouvez spécifier dans le champ *Max Idle Time* (Délai d'inactivité maximal). La valeur par défaut est **30** secondes.

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

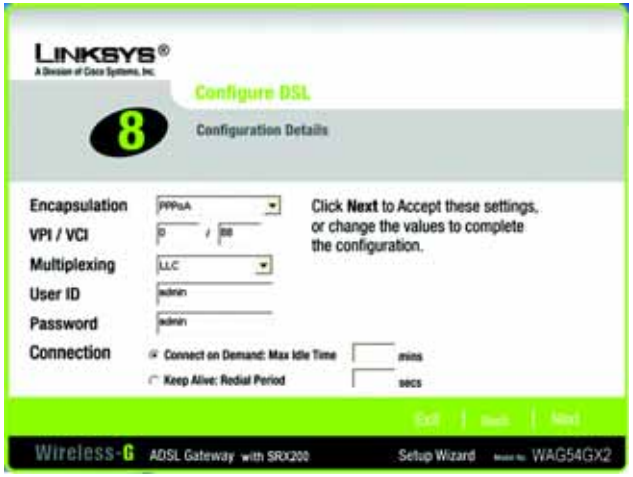


Figure 5-14 : Ecran Configure DSL - PPPoA (Configuration DSL - PPPoA) de l'assistant de configuration

PPPoE

Si vous avez sélectionné votre FAI, l'assistant de configuration sélectionne automatiquement les paramètres d'encapsulation, de VPI, de VCI et de multiplexage. Saisissez ensuite l'ID d'utilisateur et le mot de passe pour votre connexion DSL.

Si vous devez saisir manuellement vos paramètres, utilisez cet écran.

VPI/VCI : si vous devez saisir manuellement vos paramètres, saisissez les paramètres VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier) fourni par votre FAI.

Multiplexing (Multiplexage) : si vous devez saisir manuellement vos paramètres, sélectionnez **LLC** ou **VC**, en fonction de votre FAI.

User ID (ID d'utilisateur) et **Password** (Mot de passe) : saisissez l'ID d'utilisateur et le mot de passe fournis par votre FAI.

Connection : choisissez l'option **Keep Alive** (Maintien de la connexion) si vous souhaitez toujours être connecté à votre fournisseur d'accès Internet (FAI) ou sélectionnez **Connect on Demand** (Connexion à la demande) si vous êtes facturé pour la durée de connexion à votre FAI.

Keep Alive (Maintien de la connexion) : pour cette option, le modem routeur maintiendra votre connexion Internet et active. Dans le champ *Redial Period* (Rappel après), spécifiez la fréquence à laquelle le modem routeur doit vérifier votre connexion Internet (la valeur par défaut est **5** minutes).

Connect on Demand (Connexion à la demande) : si vous sélectionnez cette option, le modem routeur met fin à votre accès Internet à l'issue d'un laps de temps spécifique, que vous pouvez spécifier dans le champ *Max Idle Time* (Délai d'inactivité maximal). La valeur par défaut est **30** secondes.

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

14. Pour configurer le modem routeur à partir de n'importe quel ordinateur du réseau, vous pouvez utiliser l'utilitaire Web qui l'accompagne. L'accès à l'utilitaire est protégé par un mot de passe.

    Password (Mot de passe) : le mot de passe par défaut est **admin**. Remplacez-le par un mot de passe de votre choix.

    Confirm (Confirmer) : saisissez à nouveau le mot de passe dans le champ *Confirm* (Confirmer).

    Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

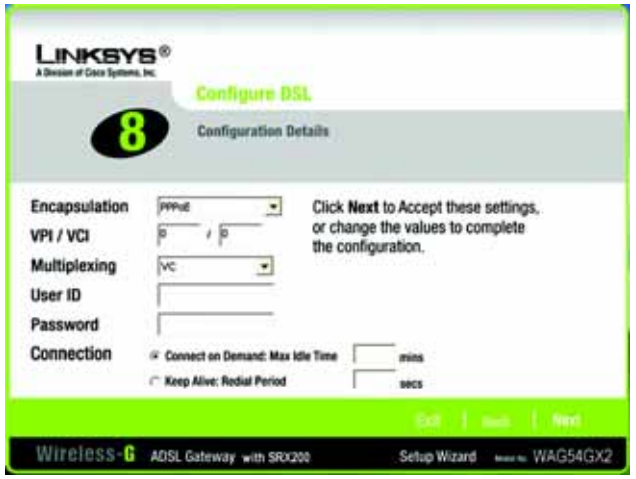


Figure 5-15 : Ecran Configure DSL - PPPoE (Configuration DSL - PPPoE) de l'assistant de configuration

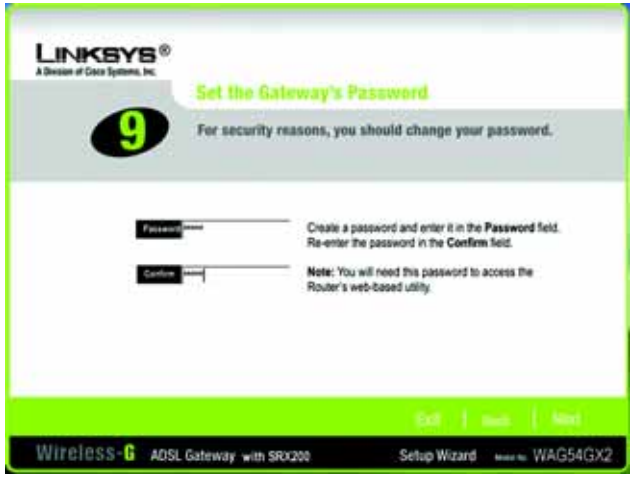


Figure 5-16 : Ecran Set the Gateway's Password (Définition du mot de passe du modem routeur) de l'assistant de configuration

15. L'assistant de configuration vous demande de saisir les paramètres de votre réseau sans fil.

SSID : dans le champ *SSID*, saisissez le nom de votre réseau sans fil. Le SSID doit être identique pour tous les périphériques du réseau. Le paramètre par défaut est **linksys** (en minuscules).

REMARQUE : Un SSID est le nom de réseau que partagent tous les périphériques d'un réseau sans fil. Le SSID de votre réseau devrait être propre à votre réseau et identique pour tous ses périphériques.

Channel (Canal) : sélectionnez le canal d'utilisation de votre réseau sans fil. Tous vos périphériques communiqueront sur ce canal.

Network Mode (Mode réseau) : dans le menu déroulant *Network Mode* (Mode réseau), sélectionnez les normes sans fil en vigueur sur votre réseau. Si vous disposez à la fois des périphériques 802.11g et 802.11b sur votre réseau, conservez le paramètre par défaut **Mixed** (Mixte). Si vous utilisez uniquement des périphériques 802.11g, sélectionnez **G-Only** (G uniquement). Si vous travaillez uniquement avec des périphériques 802.11b, sélectionnez **B-Only** (B uniquement). Si vous souhaitez désactiver votre réseau sans fil, sélectionnez **Disable** (Désactiver).

Device Name (Nom du périphérique) : saisissez un nom pour le modem routeur dans le champ *Device Name* (Nom du périphérique).

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

16. Sélectionnez la méthode de sécurité que vous souhaitez utiliser : **WPA Personal**, **WPA2 Personal**, **WPA2 Mixed Mode**, **WEP (64-Bit)** ou **WEP (128-Bit)**. WPA signifie Wi-Fi Protected Access et WEP Wired Equivalent Privacy. La méthode WPA2 est une version plus sécurisée de la méthode WPA qui est elle-même plus sécurisée que la méthode WEP. Reportez-vous à la section correspondant à votre méthode de sécurité.

Si vous ne souhaitez utiliser aucune méthode de sécurité sans fil, sélectionnez **Disabled** (Désactivée), puis cliquez sur le bouton **Next** (Suivant). Passez à l'étape 17.

REMARQUE : Si vous souhaitez utiliser la sécurité WPA Enterprise ou WPA2 Enterprise, sélectionnez **Disabled** (Désactivé), puis cliquez sur le bouton **Next** (Suivant). Une fois l'assistant de configuration terminé, utilisez l'utilitaire Web du modem routeur pour configurer les paramètres de sécurité sans fil. Reportez-vous au « Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200 » pour plus d'instructions.

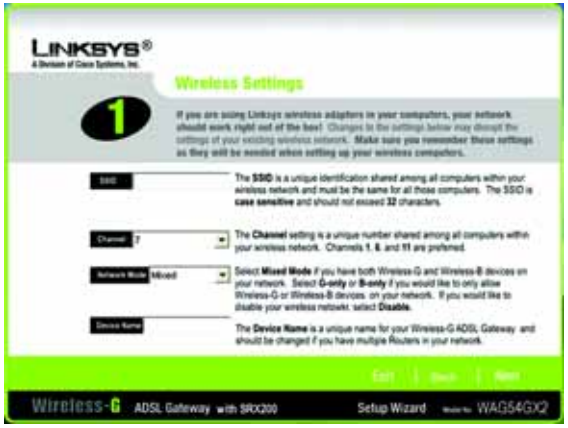


Figure 5-17 : Ecran Wireless Settings (Paramètres sans fil) de l'assistant de configuration

wpa *(wi-fi protected access) : protocole de sécurité sans fil faisant appel au cryptage TKIP (Temporal Key Integrity Protocol) et pouvant être utilisé en association avec un serveur RADIUS.*

wep *(Wired Equivalent Privacy) : méthode permettant de crypter des données transmises sur un réseau sans fil pour une sécurité accrue.*

Figure 5-18 : Ecran Configure Wireless Security Settings (Configuration des paramètres de sécurité sans fil) de l'assistant de configuration

WPA Personal (WPA personnel)

Encryption (Cryptage) : sélectionnez le type d'algorithme que vous souhaitez utiliser (**TKIP** ou **AES**).

Passphrase (Phrase de passe) : saisissez une phrase de passe, également appelée une clé pré-partagée de 8 à 32 caractères. Plus votre phrase de passe est longue et complexe, meilleure est la sécurité de votre réseau.

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

cryptage : *codage de données transmises sur un réseau.*

Figure 5-19 : Ecran Wireless Security - WPA Personal (Sécurité sans fil - WPA personnel) de l'assistant de configuration

WPA2 Personal (WPA2 personnel)

Encryption (Cryptage) : AES est automatiquement sélectionné pour WPA2 Personal mode.

Passphrase (Phrase de passe) : saisissez une phrase de passe, également appelée une clé pré-partagée de 8 à 32 caractères. Plus votre phrase de passe est longue et complexe, meilleure est la sécurité de votre réseau.

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

Figure 5-20 : Ecran Wireless Security - WPA2 Personal (Sécurité sans fil - WPA2 personnel) de l'assistant de configuration

WPA2 Mixed Mode (WPA2 mode mixte)

Encryption (Cryptage) : TKIP + AES sont automatiquement sélectionnés et les deux méthodes peuvent donc être utilisées.

Passphrase (Phrase de passe) : saisissez une phrase de passe, également appelée une clé pré-partagée de 8 à 32 caractères. Plus votre phrase de passe est longue et complexe, meilleure est la sécurité de votre réseau.

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

Figure 5-21 : Ecran Wireless Security - WPA2 Mixed Mode (Sécurité sans fil - WPA2 mode mixte) de l'assistant de configuration

WEP (64 bits)

Saisissez une phrase de passe ou une clé WEP.

Passphrase (Phrase de passe) : saisissez une phrase de passe dans le champ *Passphrase* (Phrase de passe). Une clé WEP est alors générée automatiquement. La phrase de passe est sensible à la casse et ne doit pas comporter plus de 16 caractères alphanumériques. Elle doit correspondre à celle des autres périphériques sans fil du réseau et n'est compatible qu'avec les produits sans fil Linksys. (Si vos produits sans fil ne sont pas des produits Linksys, saisissez la clé WEP manuellement sur ces produits.)

Key 1 (Clé 1) : la clé WEP saisie doit correspondre à celle de votre réseau sans fil. Pour un mode de cryptage à 64 bits, saisissez exactement 10 caractères hexadécimaux. Les caractères hexadécimaux valides sont : « 0 » à « 9 » et « A » à « F ».

Cliquez sur le bouton **Next** (Suivant) pour continuer ou sur **Back** (Précédent) pour revenir à l'écran précédent.

Figure 5-22 : Ecran Wireless Security - WEP (64-Bit) (Sécurité sans fil - WEP (64 bits)) de l'assistant de configuration

WEP (128 bits)

Saisissez une phrase de passe ou une clé WEP.

Passphrase (Phrase de passe) : saisissez une phrase de passe dans le champ *Passphrase* (Phrase de passe). Une clé WEP est alors générée automatiquement. La phrase de passe est sensible à la casse et ne doit pas comporter plus de 16 caractères alphanumériques. Elle doit correspondre à celle des autres périphériques sans fil du réseau et n'est compatible qu'avec les produits sans fil Linksys. (Si vos produits sans fil ne sont pas des produits Linksys, saisissez la clé WEP manuellement sur ces produits.)

Key 1 (Clé 1) : la clé WEP que vous entrez doit correspondre à celle de votre réseau sans fil. Pour un mode de cryptage à 128 bits, saisissez exactement 26 caractères hexadécimaux. Les caractères hexadécimaux valides sont : « 0 » à « 9 » et « A » à « F ».

Cliquez sur le bouton Next (Suivant) pour continuer ou sur Back (Précédent) pour revenir à l'écran précédent.

Figure 5-23 : Ecran Wireless Security - WEP (128-Bit) (Sécurité sans fil - WEP (128 bits)) de l'assistant de configuration

17. L'assistant de configuration vous demande de vérifier vos paramètres avant qu'il les enregistre. Cliquez sur le bouton **Yes** (Oui) si vous êtes satisfait de vos paramètres ou sur le bouton **No** (Non) si vous ne souhaitez pas enregistrer vos nouveaux paramètres.

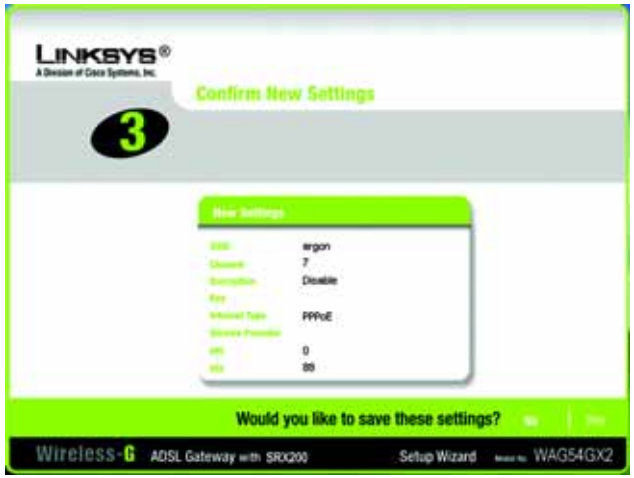


Figure 5-24 : Ecran Confirm New Settings (Confirmation des nouveaux paramètres) de l'assistant de configuration

18. Une fois les paramètres enregistrés, l'écran *Safe Surfing* (Surf sécurisé) apparaît. Cliquez sur le bouton **Norton Internet Security Suite** (Suite Norton Internet Security) pour installer l'édition spéciale de Norton Internet Security sur votre ordinateur ou cliquez sur le bouton **Finish** (Terminer) pour terminer l'assistant de configuration.

Figure 5-25 : Ecran Safe Surfing (Surf sécurisé) de l'assistant de configuration

19. L'écran *Congratulations* (Félicitations) s'affiche. Cliquez sur le bouton **Online Registration** (Enregistrement en ligne) pour enregistrer le modem routeur ou sur le bouton **Exit** (Quitter) pour quitter l'assistant de configuration.

Félicitations ! L'installation du modem routeur ADSL sans fil G avec SRX200 est terminée.

Pour effectuer des modifications de la configuration avancée, passez au « Chapitre 6 : Configuration de le modem routeur ADSL sans fil - G avec SRX200 ».

Figure 5-26 : Ecran Congratulations (Félicitations) de l'assistant de configuration

Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200

Présentation

Suivez les étapes contenues dans ce chapitre et configurez le modem routeur en utilisant son utilitaire Web. Ce chapitre décrit les pages Web de l'utilitaire ainsi que leurs fonctions clés. Vous pouvez accéder à l'utilitaire à partir de votre navigateur Web par l'intermédiaire d'un ordinateur connecté au modem routeur. Dans le cadre d'une configuration réseau de base, la plupart des utilisateurs pourront effectuer leurs opérations uniquement à partir des écrans de l'utilitaire suivants :

- Basic Setup (Configuration de base). Dans l'écran Basic Setup (Configuration de base), saisissez les paramètres fournis par votre FAI.
- Management (Gestion). Cliquez sur l'onglet **Administration**, puis sur l'onglet **Management** (Gestion). Le nom d'utilisateur et le mot de passe par défaut du modem routeur est **admin**. Pour sécuriser le modem routeur, modifiez le nom d'utilisateur et le mot de passe par défaut.

Sept onglets principaux sont disponibles : Setup (Configuration), Wireless (Sans fil), Security (Sécurité), Access Restrictions (Restrictions d'accès), Applications & Gaming (Applications et jeux), Administration et Status (Etat). D'autres onglets apparaissent lorsque vous cliquez sur les onglets principaux. Pour plus d'informations, cliquez sur **Help** (Aide).

AVEZ-VOUS ? : Avez-vous activé TCP/IP sur vos ordinateurs ? Les ordinateurs utilisent ce protocole pour communiquer sur le réseau. Pour obtenir plus d'informations sur TCP/IP, consultez l'aide de Windows.

REMARQUE : Pour plus de sécurité, modifiez vos nom d'utilisateur et mot de passe à partir de l'onglet Administration.

Configuration

- Basic Setup (Configuration de base). Saisissez les paramètres de connexion Internet et de réseau dans cet écran.
- DDNS. Pour activer la fonctionnalité DDNS (Dynamic Domain Name System) du modem routeur, renseignez les champs à l'écran.
- Advanced Routing (Routage avancé). Dans cet écran, vous pouvez configurer les options NAT et de routage.

Sans fil

- Basic Wireless Settings (Paramètres sans fil de base). Dans cet écran, vous pouvez sélectionner les paramètres de réseau sans fil.
- Wireless Security (Sécurité sans fil). Dans cet écran, vous pouvez configurer les paramètres de sécurité sans fil.
- Wireless Access (Accès sans fil). Dans cet écran, vous pouvez contrôler l'accès à votre réseau sans fil.
- Advanced Wireless Settings (Paramètres sans fil avancés). Dans cet écran, vous pouvez accéder aux paramètres de réseau sans fil avancés.

Sécurité

- Firewall (Pare-feu). Utilisez cet écran pour activer/désactiver le pare-feu, définir des filtres et bloquer des requêtes Internet anonymes.
- VPN Passthrough (Intercommunication VPN). Vous pouvez activer ou désactiver l'intercommunication VPN (Virtual Private Network) dans cet écran.
- VPN. Cet écran vous permet de configurer jusqu'à cinq tunnels VPN.

__vpn__ (virtual private network) : mesure de sécurité visant à protéger des données lorsqu'elles quittent un réseau et s'acheminent vers un autre via Internet.

Restrictions d'accès

- Internet Access Policy (Stratégie d'accès à Internet). Dans cet écran, vous pouvez contrôler l'exploitation et le trafic Internet de votre réseau local.

Applications et jeux

- Single Port Range Forwarding (Transfert de connexion unique). Dans cet écran, vous pouvez définir des services ou des applications fréquemment utilisés qui exigent un transfert de connexion unique.
- Port Range Forwarding (Transfert de connexion). Dans cet écran, vous pouvez définir des services publics ou autres applications Internet spécialisées qui exigent le transfert d'une série de connexions.
- Port Triggering (Déclenchement de connexion). Cet onglet vous permet de configurer des connexions déclenchées et des connexions transférées pour des applications Internet.
- DMZ. Cet écran vous permet d'autoriser l'exposition à Internet d'un ordinateur local, pour l'accès à des services spécifiques.
- QoS (QS, qualité de service). Utilisez Quality of Service (Qualité de service) pour attribuer différents degrés de priorité à différents types de transmissions de données.

Administration

- Management (Gestion). Cet écran vous permet de modifier les paramètres de gestion d'accès au modem routeur, SNMP (Simple Network Management Protocol), UPnP (Universal Plug and Play) et les paramètres de proxy IGMP.
- Reporting (Rapports). Cet onglet vous permet de visualiser ou d'enregistrer des fichiers journaux d'activités.
- Diagnostics. Cet écran vous permet d'effectuer un test Ping.
- Backup&Restore (Sauvegarde&restauration). Cet écran vous permet de sauvegarder ou restaurer la configuration du modem routeur.
- Factory Defaults (Paramètres d'usine). Cet écran vous permet de restaurer les paramètres d'usine (par défaut) du modem routeur.
- Firmware Upgrade (Mise à niveau du micrologiciel). Cet onglet vous permet de mettre à niveau le micrologiciel du modem routeur.

Etat

- Gateway (Modem routeur). Cet écran contient des informations sur l'état du modem routeur.
- Local Network (Réseau local). Cet écran contient des informations sur l'état du réseau local.
- Wireless (Sans fil). Cet écran contient des informations sur l'état du réseau sans fil.
- DSL Connection (Connexion DSL). Cet écran contient des informations sur l'état de la connexion DSL.

Comment accéder à l'utilitaire Web ?

Pour accéder à l'utilitaire Web, démarrez Internet Explorer ou Netscape Navigator, puis saisissez l'adresse IP par défaut du modem routeur, **192.168.1.1**, dans le champ *Address* (Adresse). Appuyez ensuite sur la touche **Entrée**.

Un écran de connexion apparaît (les utilisateurs de Windows XP voient apparaître un écran semblable). Saisissez **admin** (nom d'utilisateur par défaut) dans le champ *Nom d'utilisateur* et **admin** (mot de passe par défaut) dans le champ *Mot de passe*. Cliquez sur le bouton **OK**.

Figure 6-1 : Ecran Login (Connexion)

Onglet Setup (Configuration)

Onglet Basic Setup (Configuration de base)

Le premier écran qui s'affiche est l'onglet Basic Setup (Configuration de base). Les options de cet onglet vous permettent de modifier les paramètres généraux du modem routeur. Modifiez ces paramètres comme décrit ici et cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

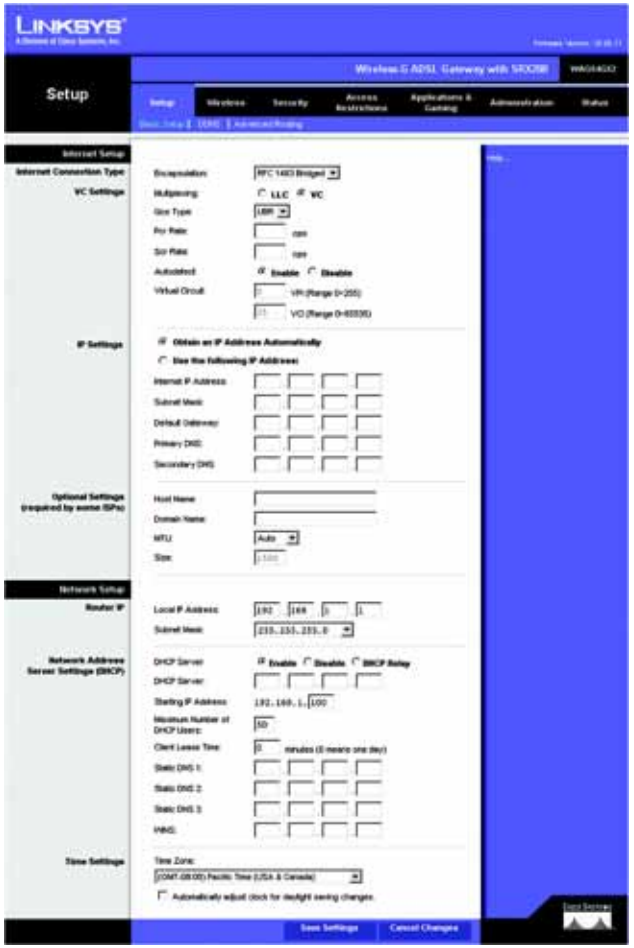


Figure 6-2 : Basic Setup (Configuration de base)

Internet Setup (Configuration Internet)

- Internet Connection Type (Type de connexion Internet). le modem routeur prend en charge six méthodes d'encapsulation : RFC 1483 Bridged, RFC 1483 Routed, IPoA, RFC 2516 PPPoE, RFC 2364 PPPoA et Bridged Mode Only (Bridged Mode uniquement). Sélectionnez le type d'encapsulation qui convient dans le menu déroulant. Les écrans *Basic Setup* (Configuration de base) et les options disponibles varient selon le type d'encapsulation sélectionné.
- VC Settings (Paramètres VC). Cette section permet de configurer les paramètres VC.
  - Multiplexing (Multiplexage) : sélectionnez **LLC** ou **VC** en fonction de votre FAI.
  - QoS Type (Type QS) : sélectionnez dans le menu déroulant : **CBR** (Continuous Bit Rate) pour spécifier une bande passante fixe pour les transmissions vocales ou de données, **UBR** (Unspecific Bit Rate) pour les applications qui ne sont pas sensibles au temps comme la messagerie ou **VBR** (Variable Bite Rate) pour le trafic en rafales et le partage de bande passante avec d'autres applications.

- Pcr Rate (Taux Pcr) : pour calculer le taux Pcr, divisez le taux de la ligne DSL par 424. Vous obtenez le taux maximal d'envoi de cellules par l'expéditeur. Saisissez le taux dans ce champ (s'il est requis par votre FAI).
- Scr Rate (Taux Scr) : maintient la vitesse de cellule, définit le taux moyen de cellules pouvant être transmises. Cette valeur est normalement inférieure au taux Pcr. Saisissez le taux dans ce champ (s'il est requis par votre FAI).
- Autodetect (Détection automatique) : sélectionnez **Enable** (Activer) pour que les paramètres soient saisis automatiquement ou **Disable** (Désactiver) pour saisir les valeurs manuellement.
- Virtual Circuit (Circuit Virtuel) : ces champs se rapportent à deux éléments : VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier). Votre FAI vous indiquera le paramétrage approprié de chacun de ces deux champs.

- IP Settings (Paramètres IP). Suivez les instructions de la section correspondant au type d'encapsulation choisi.

RFC 1483 Bridged

Adresse IP dynamique

IP Settings (Paramètres IP). Sélectionnez **Obtain an IP Address Automatically** (Obtenir une adresse IP automatiquement) si votre FAI vous indique que vous êtes connecté via une adresse IP dynamique.

Adresse IP statique

Si vous devez utiliser une adresse IP permanente (statique) pour vous connecter à Internet, sélectionnez **Use the following IP Address** (Utiliser l'adresse IP suivante).

- Internet IP Address (Adresse IP Internet). Il s'agit de l'adresse IP du modem routeur, vue par le WAN ou Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.
- Subnet Mask (Masque de sous-réseau). Il s'agit du masque de sous-réseau du modem routeur. Votre FAI peut vous fournir le masque de sous-réseau.
- Default Gateway (Passerelle par défaut). Votre FAI peut vous fournir l'adresse par défaut du modem routeur. Il s'agit en fait de l'adresse IP du serveur du FAI.
- Primary DNS (Nom de domaine primaire) (obligatoire) et Secondary DNS (Nom de domaine secondaire) (facultatif). Votre FAI peut vous fournir au moins une adresse IP de serveur DNS (Domain Name System).

Figure 6-3 : RFC 1483 Bridged

RFC 1483 Routed

Si vous devez utiliser RFC 1483 Routed, sélectionnez **RFC 1483 Routed**.

- Internet IP Address (Adresse IP Internet). Il s'agit de l'adresse IP du modem routeur, vue par le WAN ou Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.
- Subnet Mask (Masque de sous-réseau). Il s'agit du masque de sous-réseau du modem routeur. Votre FAI peut vous fournir le masque de sous-réseau.
- Default Gateway (Passerelle par défaut). Votre FAI peut vous fournir l'adresse par défaut du modem routeur. Il s'agit en fait de l'adresse IP du serveur du FAI.
- Primary DNS (Nom de domaine primaire) (obligatoire) et Secondary DNS (Nom de domaine secondaire) (facultatif). Votre FAI peut vous fournir au moins une adresse IP de serveur DNS (Domain Name System).

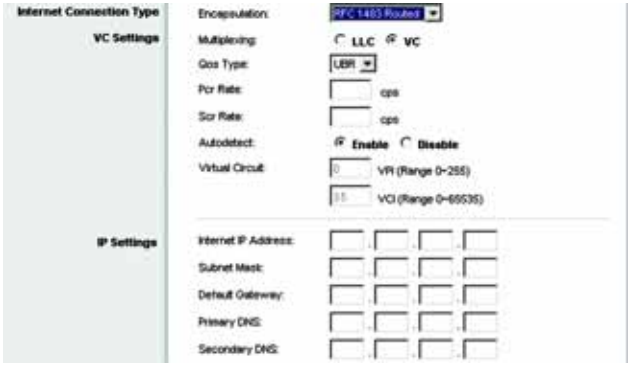


Figure 6-4 : RFC 1483 Routed

IPoA

Si vous devez utiliser IPoA (IP over ATM), sélectionnez **IPoA**.

- Internet IP Address (Adresse IP Internet). Il s'agit de l'adresse IP du modem routeur, vue par le WAN ou Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.
- Subnet Mask (Masque de sous-réseau). Il s'agit du masque de sous-réseau du modem routeur. Votre FAI peut vous fournir le masque de sous-réseau.
- Default Gateway (Passerelle par défaut). Votre FAI peut vous fournir l'adresse par défaut du modem routeur. Il s'agit en fait de l'adresse IP du serveur du FAI.
- Primary DNS (Nom de domaine primaire) (obligatoire) et Secondary DNS (Nom de domaine secondaire) (facultatif). Votre FAI peut vous fournir au moins une adresse IP de serveur DNS (Domain Name System).

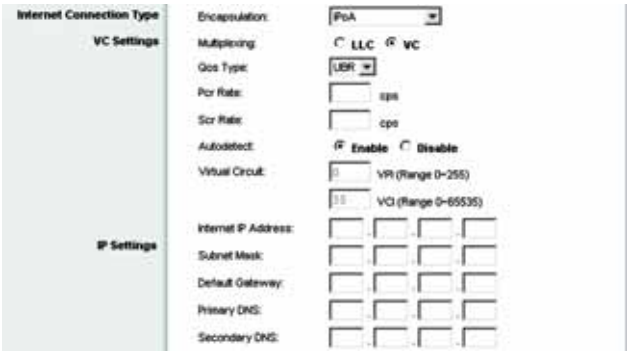


Figure 6-5 : IPoA

RFC 2516 PPPoE

Certains fournisseurs d'accès à Internet DSL utilisent le protocole PPPoE (Point-to-Point Protocol over Ethernet) pour établir des connexions Internet. Si vous êtes connecté à Internet par l'intermédiaire d'une ligne DSL, demandez à votre FAI s'il utilise le protocole PPPoE. Si tel est le cas, vous devrez sélectionner l'option PPPoE.

- User Name and Password (Nom d'utilisateur et mot de passe). Saisissez le nom d'utilisateur et le mot de passe fournis par votre FAI.
- Connect on Demand: Max Idle Time (Connexion à la demande : délai d'inactivité maximal). Vous pouvez configurer le modem routeur afin qu'elle désactive la connexion Internet après une période donnée d'inactivité. Si votre connexion Internet a été désactivée suite à son inactivité, l'option Connect on Demand (Connexion à la demande) permet au modem routeur de rétablir automatiquement votre connexion dès que vous tentez d'accéder de nouveau à Internet. Si vous souhaitez sélectionner cette option, cliquez sur le bouton d'option **Connect on Demand** (Connexion à la demande). Dans le champ *Max Idle Time* (Délai d'inactivité maximal), saisissez le nombre de minutes que vous souhaitez voir s'écouler avant la désactivation de votre connexion Internet.
- Keep Alive: Redial Period (Activée : rappel après). Si vous sélectionnez cette option, le modem routeur procède régulièrement à une vérification de votre connexion Internet. Si vous êtes déconnecté, le modem routeur rétablit automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton d'option **Keep Alive** (Activée). Dans le champ *Redial Period* (Rappel après), spécifiez la fréquence à laquelle le modem routeur doit vérifier votre connexion Internet. Le temps devant s'écouler par défaut avant rappel est de **30** secondes.

RFC 2364 PPPoA

Certains fournisseurs d'accès Internet (FAI) DSL utilisent le protocole PPPoA (protocole de point-à-point sur ATM) pour établir des connexions Internet. Si vous êtes connecté à Internet par l'intermédiaire d'une ligne DSL, demandez à votre FAI s'il utilise le protocole PPPoA. Si tel est le cas, vous devrez sélectionner l'option PPPoA.

- User Name and Password (Nom d'utilisateur et mot de passe). Saisissez le nom d'utilisateur et le mot de passe fournis par votre FAI.
- Connect on Demand: Max Idle Time (Connexion à la demande : délai d'inactivité maximal). Vous pouvez configurer le modem routeur afin qu'elle désactive la connexion Internet après une période donnée d'inactivité. Si votre connexion Internet a été désactivée suite à son inactivité, l'option Connect on Demand (Connexion à la demande) permet au modem routeur de rétablir automatiquement votre connexion dès que vous tentez d'accéder de nouveau à Internet. Si vous souhaitez sélectionner cette option, cliquez sur le bouton d'option **Connect on Demand** (Connexion à la demande). Dans le champ *Max Idle Time* (Délai d'inactivité maximal), saisissez le nombre de minutes que vous souhaitez voir s'écouler avant la désactivation de votre connexion Internet.

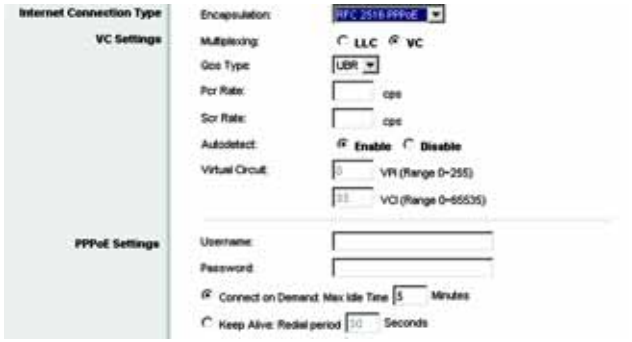


Figure 6-6 : RFC 2516 PPPoE

IMPORTANT : Pour que l'option Connect on Demand (Connexion à la demande) fonctionne correctement, fermez toutes les applications Internet, sans quoi le modem routeur risque de ne pas abandonner la connexion selon la fréquence à laquelle l'application tente de se connecter à Internet (par exemple, programmes de messagerie instantanée).

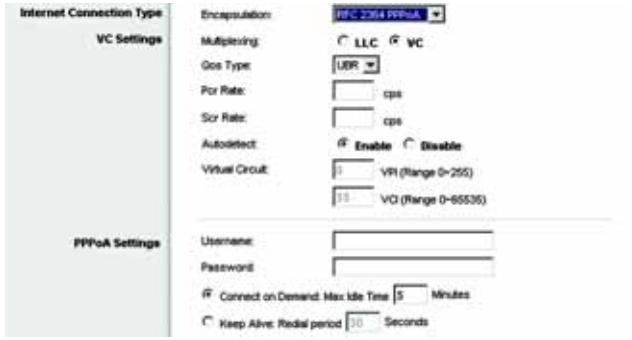


Figure 6-7 : RFC 2364 PPPoA

Keep Alive: Redial Period (Activée : rappel après). Si vous sélectionnez cette option, le modem routeur procède régulièrement à une vérification de votre connexion Internet. Si vous êtes déconnecté, le modem routeur rétablit automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton d'option **Keep Alive** (Activée). Dans le champ *Redial Period* (Rappel après), spécifiez la fréquence à laquelle le modem routeur doit vérifier votre connexion Internet. Le temps devant s'écouler par défaut avant rappel est de **30** secondes.

Bridged Mode Only (Bridged Mode uniquement)

Si vous utilisez votre modem routeur en tant que pont (il fonctionne comme un modem autonome), sélectionnez **Bridged Mode Only** (Bridged Mode uniquement). Les paramètres NAT et de routage sont désactivés dans ce mode.

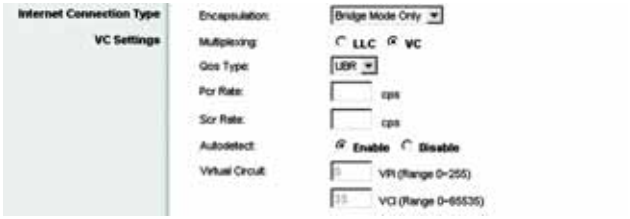


Figure 6-8 : Bridged Mode Only (Bridged Mode uniquement)

Optional Settings (Paramètres facultatifs) (Requis par certains FAI)

- Host Name (Nom d'hôte) et Domain Name (Nom de domaine). Saisissez les noms d'hôte et de domaine du modem routeur dans ces deux champs. Certains FAI requièrent ces noms pour l'authentification. Vous devrez peut-être contacter votre FAI et vérifier si votre service Internet haut débit a été configuré avec un nom d'hôte et un nom de domaine. Dans la plupart des cas, vous pourrez laisser ces champs vides.

- MTU et Size (Taille). Le paramètre MTU (Maximum Transmission Unit) spécifie la taille de paquet maximale autorisée pour la transmission réseau. Sélectionnez **Manual** (Manuel) et saisissez la valeur souhaitée dans le champ *Size* (Taille). Il est recommandé d'entrer une valeur comprise entre 1200 et 1500. Par défaut, le paramètre MTU est configuré automatiquement.

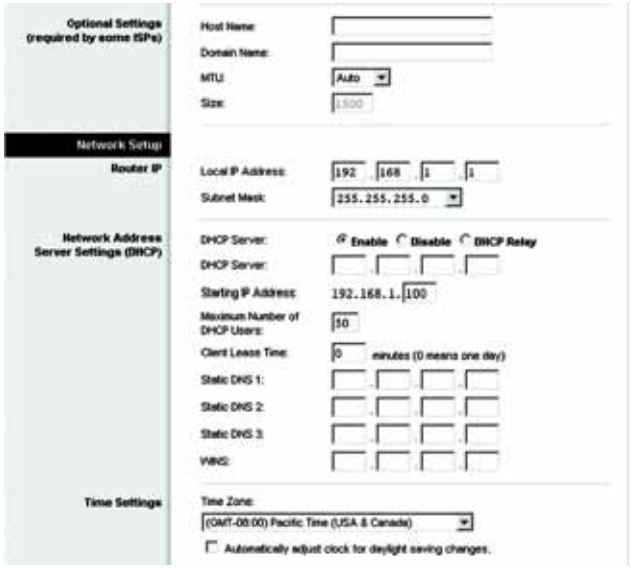


Figure 6-9 : Optional Settings (Paramètres facultatifs)

Network Setup (Configuration du réseau)

- Router IP (Adresse IP du routeur). Les valeurs d'adresse IP locale et de masque de sous-réseau du modem routeur sont spécifiées dans ces champs. Dans la plupart des cas, il est recommandé de conserver les valeurs par défaut.
  - Local IP Address (Adresse IP locale). La valeur par défaut est **192.168.1.1**.
  - Subnet Mask (Masque de sous-réseau). La valeur par défaut est **255.255.255.0**.
- Network Address Server Settings (DHCP) (Paramètres du serveur d'adresse de réseau (DHCP)). Cette section permet de configurer les paramètres DHCP (Dynamic Host Configuration Protocol) du modem routeur.

- DHCP Server (Serveur DHCP). Un serveur Dynamic Host Configuration Protocol (DHCP) attribue automatiquement une adresse IP à chaque ordinateur du réseau. A moins que vous ne disposiez déjà d'un serveur DHCP, il est recommandé de laisser la fonction de serveur DHCP activée pour le modem routeur. Le modem routeur peut également être utilisée en mode Relais DHCP. (Ce paramètre n'est pas disponible pour tous les types d'encapsulation.)

- DHCP Server (Serveur DHCP). Si vous activez le paramètre Relais DHCP du *serveur DHCP*, saisissez l'adresse IP du serveur DHCP dans les champs. (Ce paramètre n'est pas disponible pour tous les types d'encapsulation.)

- Starting IP Address (Adresse IP de début). Saisissez une valeur de début pour la publication d'adresses IP sur le serveur DHCP. L'adresse IP par défaut du modem routeur étant **192.168.1.1**, cette valeur doit être égale à 192.168.1. 2 ou supérieure.

- Maximum Number of DHCP Users (Nombre maximal d'utilisateurs DHCP). Saisissez le nombre maximal d'utilisateurs/clients pouvant obtenir une adresse IP. Ce nombre varie en fonction de l'adresse IP de début spécifiée.

- Client Lease Time (Durée de connexion du client). Cette option détermine la période pendant laquelle un ordinateur est autorisé à se connecter au modem routeur à l'aide de son adresse IP dynamique actuelle. Saisissez la durée (en minutes) pendant laquelle l'adresse IP dynamique est allouée à l'ordinateur.

- Static DNS 1-3 (DNS statique, 1 à 3). Le système DNS (Domain Name System) est le service adopté par Internet pour convertir des noms de domaine ou de site Web en adresses Internet ou URL. Votre FAI peut vous fournir au moins une adresse IP de serveur DNS. Vous pouvez saisir jusqu'à trois adresses IP de serveur DNS. le modem routeur utilise alors ces trois adresses IP pour accéder en un clin d'œil aux serveurs DNS en cours d'utilisation.

- WINS. Le système WINS (Windows Internet Naming Service) convertit des noms NetBIOS en adresses IP. Si vous optez pour un serveur WINS, saisissez son adresse IP dans ce champ. Autrement, laissez-le vide.

- Time Setting (Réglage de l'heure). Sélectionnez le fuseau horaire correspondant à l'emplacement de votre modem routeur. Vous pouvez activer la case à cocher **Automatically adjust clock for daylight saving changes** (Régler automatiquement l'horloge en fonction des modifications de l'heure d'été).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet DDNS

le modem routeur inclut une fonction DDNS (Dynamic Domain Name System) qui vous permet d'attribuer un nom de domaine et d'hôte fixe à une adresse IP Internet dynamique. Cela peut s'avérer utile si vous hébergez votre propre site Web, un serveur FTP ou tout autre type de serveur derrière le modem routeur.

Avant d'opter pour cette fonctionnalité, vous devez obtenir la connexion à un service DDNS auprès de fournisseurs spécialisés, tels que DynDNS.org ou TZO.com.

DDNS

DDNS Service (Service DDNS). Si votre service DDNS est fourni par DynDNS.org, sélectionnez **DynDNS.org** dans le menu déroulant. Si votre service DDNS est fourni par TZO.com, sélectionnez **TZOcom** dans le menu déroulant. Pour désactiver le service DDNS, sélectionnez **Disabled** (Désactiver).

DynDNS.org

- User Name (Nom d'utilisateur), Password (Mot de passe) et Host Name (Nom d'hôte). Saisissez le nom d'utilisateur, le mot de passe et le nom d'hôte du compte configuré avec DynDNS.org.
- Status (Etat). L'état de la connexion du service DDNS est spécifié dans ce champ.
- Connect (Connecter). Cliquez sur le bouton **Connect** (Connecter) pour lancer la connexion au service DDNS.

Figure 6-10 : DDNS - DynDNS.org

TZO.com

- Email Address (Adresse électronique), Password (Mot de passe) et Domain Name (Nom de domaine). Saisissez l'adresse électronique, le mot de passe et le nom de domaine du compte configuré avec TZO.
- Status (Etat). L'état de la connexion du service DDNS est spécifié dans ce champ.
- Connect (Connecter). Cliquez sur le bouton **Connect** (Connecter) pour lancer la connexion au service DDNS.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-11 : DDNS - TZO.com

Onglet Advanced Routing (Routage avancé)

L'écran *Advanced Routing* (Routage avancé) vous permet de configurer les paramètres NAT, de routage dynamique et de routage statique.

Figure 6-12 : Advanced Routing (Routage avancé)

Advanced Routing (Routage avancé)

- Operating Mode (Mode opérationnel). Cette section permet de configurer les paramètres de routage généraux du modem routeur.
  - NAT. NAT est une fonction de sécurité activée par défaut. Elle permet au modem routeur de convertir les adresses IP d'un réseau local en une adresse IP distincte sur Internet. Pour désactiver NAT, cliquez sur le bouton d'option **Disabled** (Désactivé).
- Dynamic Routing (Routage dynamique). Le routage dynamique vous permet d'exiger du modem routeur qu'elle s'adapte aux modifications physiques de la configuration du réseau. le modem routeur, à l'aide du protocole RIP, détermine l'itinéraire des paquets du réseau en fonction du plus petit nombre de sauts relevés entre la source et la destination. Le protocole RIP transmet régulièrement les informations de routage aux autres modems routeurs du réseau.
  - RIP. Si votre réseau comporte plusieurs routeurs, vous pouvez utiliser le protocole RIP (Routing Information Protocol) de façon à ce que les routeurs échangent des informations de routage. Pour utiliser le protocole RIP, sélectionnez le bouton d'option **Enabled** (Activé). Sinon, conservez la valeur par défaut, **Disabled** (Désactivé).
  - RIP Send Packet Version (RIP - Version Envoi de paquets). Sélectionnez le protocole de version souhaité : **RIPv1** ou **RIPv2**.
  - RIP Recv Packet Version (RIP - Version Réception de paquets). Sélectionnez le protocole de version souhaité : **RIPv1** ou **RIPv2**.
- Static Routing (Routage statique). Si le modem routeur est connectée à plusieurs réseaux, il peut être nécessaire de définir un itinéraire statique entre eux. Un itinéraire statique est une voie prédéfinie que les informations du réseau doivent emprunter pour atteindre un hôte ou un réseau spécifique. Pour créer un itinéraire statique, modifiez les paramètres suivants :
  - Sélectionner le numéro de jeu (set number). Sélectionnez le numéro de l'itinéraire statique dans le menu déroulant. le modem routeur peut prendre en charge jusqu'à 20 entrées d'itinéraires statiques. Si vous souhaitez supprimer un itinéraire, une fois l'entrée sélectionnée, cliquez sur le bouton **Delete This Entry** (Supprimer cette entrée).
  - Destination IP Address (Adresse IP de destination). Cette option identifie l'adresse du réseau distant, ou hôte, auquel vous souhaitez attribuer un itinéraire statique. Saisissez l'adresse IP de l'hôte pour lequel vous souhaitez créer un itinéraire statique. Si vous créez un itinéraire pour l'intégralité du réseau, assurez-vous que la portion de réseau de l'adresse IP est définie à 0.

- Subnet Mask (Masque de sous-réseau). Saisissez le masque de sous-réseau (également appelé Masque de réseau), qui détermine la portion de l'adresse IP qui correspond au réseau et la portion de l'adresse IP qui correspond à l'hôte.
- Gateway (Passerelle). Saisissez l'adresse IP du périphérique du modem routeur qui permet le contact entre le modem routeur et le réseau distant ou hôte.
- Hop Count (Nombre de sauts). Il s'agit du nombre de sauts entre un noeud et la destination (16 tronçons au maximum). Saisissez le nombre de sauts dans ce champ.

- Show Routing Table (Afficher la table de routage). Cliquez sur le bouton **Show Routing Table** (Afficher la table de routage) pour afficher un écran indiquant l'itinéraire des données sur le réseau local. Pour chaque itinéraire, l'adresse IP du réseau local de destination, le masque de sous-réseau, le modem routeur et l'interface sont affichés. Cliquez sur le bouton **Refresh** (Actualiser) pour mettre à jour les informations. Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran précédent.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-13 : Routing Table (Table de routage)

Onglet Wireless (Sans fil)

Onglet Basic Wireless Settings (Paramètres sans fil de base)

Cet écran vous permet de sélectionner votre mode réseau sans fil ainsi que votre sécurité sans fil.

Wireless Network (Réseau sans fil)

- Wireless Network Mode (Mode réseau sans fil). Si votre réseau comporte des périphériques 802.11g et 802.11b, conservez le paramètre par défaut, **Mixed** (Mixte). Si vous utilisez uniquement des périphériques 802.11g, sélectionnez **G-Only** (G uniquement). Si vous travaillez uniquement avec des périphériques 802.11b, sélectionnez **B-Only** (B uniquement). Si vous souhaitez désactiver le réseau sans fil, sélectionnez **Disabled** (Désactivé).

- Wireless Network Name (SSID) (Nom du réseau sans fil [SSID]). Saisissez le nom de votre réseau sans fil dans ce champ. Il s'agit du nom de réseau que partagent tous les périphériques interconnectés à un réseau sans fil. Il doit être identique pour tous les périphériques du réseau sans fil. Ce paramètre est sensible à la casse et ne doit pas comprendre plus de 32 caractères alphanumériques. Tous les caractères du clavier peuvent être utilisés. Linksys vous recommande de remplacer le nom SSID par défaut (linksys) par un nom unique de votre choix.

- Wireless Channel (Canal sans fil). Sélectionnez le canal approprié dans la liste fournie en fonction de vos paramètres réseau. Tous les périphériques de votre réseau sans fil doivent utiliser le même canal pour fonctionner correctement. Les ordinateurs ou clients sans fil détecteront automatiquement le canal sans fil du modem routeur.

- Wireless SSID Broadcast (Diffusion SSID sans fil). Lorsque des ordinateurs ou des clients sans fil recherchent sur le réseau local des réseaux sans fil auxquels s'associer, ils détectent le SSID diffusé par le modem routeur. Pour diffuser le SSID du modem routeur, conservez le paramètre par défaut, **Enable** (Activer). Si vous ne souhaitez pas diffuser le SSID du modem routeur, sélectionnez **Disable** (Désactiver).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-14 : Basic Wireless Settings (Paramètres sans fil de base)

Onglet Wireless Security (Sécurité sans fil)

Les paramètres de cette section permettent de configurer la sécurité de votre réseau sans fil. le modem routeur prend en charge six options en mode Sécurité sans fil : WPA-Personal, WPA2-Personal, WPA2-Mixed, WPA Enterprise, WPA2 Enterprise et WEP. WPA, acronyme de Wi-Fi Protected Access, désigne une norme de sécurité plus puissante que le système de cryptage WEP (Wired Equivalent Privacy). WPA2 est une version plus avancée et plus sécurisée de WPA. WPA/WPA2 Entreprise utilisent un serveur RADIUS (Remote Authentication Dial-In User Service) pour l'authentification. Ces deux options font l'objet d'une description sommaire ci-après. Pour obtenir des instructions plus détaillées sur la configuration de la sécurité sans fil du modem routeur, consultez l'« Annexe B : Sécurité sans fil ».

Pour désactiver la sécurité sans fil, sélectionnez **Disable** (Désactiver) dans le menu déroulant du mode de sécurité.

- Security Mode (Mode de sécurité). Sélectionnez le mode que votre réseau doit utiliser, **WPA-Personal**, **WPA2-Personal**, **WPA2-Mixed**, **WPA Enterprise**, **WPA2 Enterprise** ou **WEP**. Si vous travaillez avec des périphériques utilisant WPA-Personal et WPA2-Personal, sélectionnez **WPA2-Mixed**.

WPA-Personnal (WPA personnel)

- Encryption (Cryptage). Sélectionnez la méthode à utiliser, **TKIP** ou **AES**. (AES est une méthode de cryptage plus puissante que la méthode TKIP.)
- Passphrase (Phrase de passe). Saisissez la clé partagée par le modem routeur et par vos autres périphériques réseau. Elle doit comporter entre 8 et 63 caractères.
- Key Renewal (Renouvellement des clés). Saisissez ensuite le Key Renewal (Renouvellement des clés) pour indiquer au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage dynamiques.

Lorsque vous avez terminé d'apporter des modifications dans cet écran, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer les modifications ou le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

WPA2-Personal (WPA2 personnel)

- Encryption (Cryptage). AES est automatiquement sélectionné.
- Passphrase (Phrase de passe). Saisissez la clé partagée par le modem routeur et par vos autres périphériques réseau. Elle doit comporter entre 8 et 63 caractères.
- Key Renewal (Renouvellement des clés). Saisissez ensuite le Key Renewal (Renouvellement des clés) pour indiquer au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage dynamiques.

Lorsque vous avez terminé d'apporter des modifications dans cet écran, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer les modifications ou le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-15 : Wireless Security - WPA-Personal (Sécurité sans fil - WPA-Personal)

IMPORTANT : Si vous utilisez une sécurité sans fil, gardez toujours à l'esprit que votre réseau sans fil DOIT utiliser la même méthode de sécurité sans fil et la même clé partagée, sans quoi le réseau ne fonctionnera pas correctement. Si vous travaillez avec des périphériques utilisant WPA-Personal et WPA2-Personal, vous devez utiliser WPA2-Mixed. Vous pouvez basculer entre WPA et WPA2 Enterprise sans problème, mais cela est impossible entre Personal et Enterprise, Personal et WEP ou Enterprise et WEP.

Figure 6-16 : Wireless Security - WPA2-Personal (Sécurité sans fil - WPA2-Personal)

WPA2-Mixed (WPA2 mixte)

- Encryption (Cryptage). TKIP + AES est automatiquement sélectionné et les deux méthodes sont donc disponibles.
- Passphrase (Phrase de passe). Saisissez la clé partagée par le modem routeur et par vos autres périphériques réseau. Elle doit comporter entre 8 et 63 caractères.
- Key Renewal (Renouvellement des clés). Saisissez ensuite le Key Renewal (Renouvellement des clés) pour indiquer au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage dynamiques.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-17 : Wireless Security - WPA2-Mixed (Sécurité sans fil - WPA2-Mixed)

WPA Enterprise (WPA entreprise)

Cette option associe le système WPA à l'utilisation d'un serveur WPA. Cette méthode est à utiliser uniquement lorsqu'un serveur RADIUS est connecté au modem routeur.

- RADIUS Server Address (Adresse du serveur RADIUS). Saisissez l'adresse IP du serveur RADIUS.
- RADIUS Port (Port RADIUS). Saisissez l'adresse IP du serveur RADIUS.
- Shared Key (Clé partagée). Saisissez la clé partagée par le modem routeur et le serveur RADIUS.
- Key Renewal Timeout (Délai de renouvellement des clés). Saisissez ensuite le Key Renewal (Renouvellement des clés) pour indiquer au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage dynamiques.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-18 : Wireless Security - WPA Enterprise (Sécurité sans fil - WPA entreprise)

WPA2 Enterprise (WPA2 entreprise)

Cette option associe le système WPA2 à l'utilisation d'un serveur WPA2. Cette méthode est à utiliser uniquement lorsqu'un serveur RADIUS est connecté au modem routeur.

- RADIUS Server Address (Adresse du serveur RADIUS). Saisissez l'adresse IP du serveur RADIUS.
- RADIUS Port (Port RADIUS). Saisissez l'adresse IP du serveur RADIUS.
- Shared Key (Clé partagée). Saisissez la clé partagée par le modem routeur et le serveur RADIUS.
- Key Renewal Timeout (Délai de renouvellement des clés). Saisissez ensuite le Key Renewal (Renouvellement des clés) pour indiquer au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage dynamiques.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-19 : Wireless Security - WPA2 Enterprise (Sécurité sans fil - WPA2 entreprise)

WEP

- Encryption (Cryptage). Sélectionnez le niveau approprié de cryptage **64 bits** ou **128 bits**. Plus le niveau de cryptage est élevé, plus il est sécurisé.
- Passphrase (Phrase de passe). Au lieu de saisir manuellement les clés WEP, vous pouvez saisir une phrase de passe. Ce paramètre sensible à la casse ne doit pas comporter plus de 32 caractères alphanumériques. Cette fonction est compatible avec les produits sans fil Linksys uniquement et ne peut pas être utilisée avec l'utilitaire de configuration automatique de réseau sans fil de Windows XP. Si vous souhaitez communiquer avec des produits sans fil autres que des produits Linksys ou avec l'utilitaire de configuration automatique de réseau sans fil de Windows XP, notez les clés WEP générées et saisissez la clé appropriée manuellement dans l'ordinateur ou le client sans fil. Si vous voulez utiliser une phrase de passe, saisissez-la dans le champ *Passphrase* (Phrase de passe) et cliquez sur le bouton **Generate** (Générer).
- WEP Keys 1-4 (Clés 1-4). Si vous n'utilisez pas de phrase de passe, saisissez manuellement un ensemble de valeurs. (Ne laissez aucun champ vierge et ne saisissez pas de zéro ; ce ne sont pas des valeurs de clés valides.) Si vous utilisez un cryptage WEP 40/64 bits, la clé doit être constituée d'exactement 10 caractères hexadécimaux. Si vous utilisez un cryptage WEP 128 bits, la clé doit être constituée d'exactement 26 caractères hexadécimaux. Les caractères hexadécimaux valides sont : « 0 à 9 » et « A à F ».
- TX Key (Clé de transmission). Pour indiquer la clé WEP à utiliser, sélectionnez un nombre de clé de transmission (TX) par défaut.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-20 : Wireless Security - WEP (Sécurité sans fil - WEP)

Onglet Wireless Access (Accès sans fil)

Wireless Network Access (Accès réseau sans fil)

Wireless Network Access (Accès réseau sans fil). Sélectionnez **Allow All** (Tout autoriser) pour autoriser tous les ordinateurs à accéder au réseau sans fil. Pour restreindre l'accès au réseau, sélectionnez **Restrict Access** (Restreindre l'accès), puis sélectionnez **Prevent** (Interdire) pour interdire l'accès aux ordinateurs désignés ou **Permit only** (Autoriser uniquement) pour autoriser l'accès des ordinateurs désignés. Cliquez sur le bouton **Update Filter List** (Mettre à jour la liste des filtres) et l'écran *MAC Address Filter List* (Liste de filtrage des adresses MAC) s'affiche.

Saisissez les adresses MAC des ordinateurs que vous souhaitez désigner. Pour consulter une liste d'adresses MAC d'ordinateurs ou de clients sans fil, cliquez sur le bouton **Wireless Client MAC List** (Liste MAC des clients sans fil).

L'écran *Wireless Client List* (Liste des clients sans fil) répertorie les adresses MAC pour vos périphériques sans fil. Cliquez sur le bouton **Refresh** (Actualiser) pour afficher les informations les plus récentes. Pour ajouter un ordinateur spécifique à la liste de filtrage des adresses MAC, cliquez sur la case à cocher **Enable MAC Filter** (Activer le filtre MAC) puis sur le bouton **Update Filter List** (Mettre à jour la liste des filtres). Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran *MAC Address Filter List* (Liste de filtrage des adresses MAC).

Sur l'écran *MAC Address Filter List* (Liste de filtrage des adresses MAC), cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer cette liste ou sur le bouton **Cancel Changes** (Annuler les modifications) pour les supprimer.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-21 : Wireless Access (Accès sans fil)

Figure 6-22 : MAC Address Filter List (Liste de filtrage des adresses MAC)

Figure 6-23 : Wireless Client MAC List (Liste MAC des clients sans fil)

Onglet Advanced Wireless Settings (Paramètres sans fil avancés)

Cet écran vous permet d'accéder aux paramètres sans fil avancés.

Advanced Wireless (Paramètres sans fil avancés)

Wireless-G Settings (Paramètres sans fil - G)

Vous pouvez utiliser les options de cet onglet pour définir les fonctions sans fil avancées du modem routeur. Il est préférable de réserver cette tâche à un administrateur chevronné, car des paramètres mal définis pourraient diminuer les performances de votre infrastructure sans fil.

- Basic Rate Set (Taux de base défini). Le paramètre Basic Rate Set (Taux de base défini) désigne une série de taux selon lesquels le modem routeur peut transmettre des données. [Pour préciser le taux de transmission des données du modem routeur, utilisez l'option Transmission Rate (Taux de transmission).] le modem routeur publie son taux de base aux autres périphériques sans fil de votre réseau afin qu'ils connaissent les taux appliqués. Elle informe également qu'elle sélectionnera automatiquement le meilleur taux de transmission. Vous devez généralement conserver le paramètre par défaut, **Default (1-2-5.5-11)** [Par défaut (1-2-5.5-11)]. D'autres options disponibles sont **1-2 Mbps** (1-2 Mbit/s), utilisées dans le cadre de technologies sans fil plus anciennes, et **All** (Tous) lorsque le modem routeur prend en charge tous les taux disponibles pour la transmission sans fil de données.

- Transmission Rate (Taux de transmission). Vous devez définir le taux de transmission des données en fonction de la vitesse de votre réseau sans fil. Vous pouvez faire votre choix parmi les diverses vitesses de transmission proposées ou sélectionner l'option **Auto** pour demander au modem routeur d'adopter automatiquement le taux de transmission le plus rapide possible et activer la fonctionnalité de reconnexion automatique. Cette fonctionnalité est alors chargée de définir la meilleure vitesse de connexion possible entre le modem routeur et un client sans fil. La valeur par défaut est **Auto**.

- CTS Protection Mode (Mode de protection CTS). Ce mode doit rester défini sur son paramètre par défaut, **Auto**. Ainsi, si vos produits sans fil G sont dans l'incapacité de transmettre de données au modem routeur dans un environnement à trafic 802.11b surchargé, ce mode sera utilisé. Cette fonction augmente la capacité du modem routeur à capter toutes les transmissions sans fil G, mais réduit considérablement les performances.

- Beacon Interval (Intervalle de transmission de balise). Une balise désigne un paquet diffusé par le modem routeur pour synchroniser le réseau sans fil. La valeur par défaut est **100**. Saisissez une valeur comprise entre 1 et 65 535 millisecondes. La valeur Beacon Interval (Intervalle de transmission de balise) indique l'intervalle de fréquence de la balise. Une balise désigne un paquet diffusé par le modem routeur pour synchroniser le réseau sans fil.

Figure 6-24 : Advanced Wireless Settings (Paramètres sans fil avancés)

- DTIM Interval (Intervalle DTIM). Cette valeur, comprise entre 1 et 255, indique l'intervalle du message d'indication de transmission de données (DTIM). Un champ DTIM est un champ de compte à rebours chargé d'informer les clients sur la prochaine fenêtre à utiliser pour écouter des messages de diffusion ou de multidiffusion. Après avoir mis en mémoire tampon les messages de diffusion ou de multidiffusion des clients qui lui sont associés, le modem routeur transmet le DTIM suivant avec une valeur d'intervalle DTIM. Ses clients sont informés par les balises et se préparent à recevoir les messages de diffusion et de multidiffusion. La valeur par défaut est **1**.

- Fragmentation Threshold (Seuil de fragmentation). Cette valeur permet de spécifier la taille maximale d'un paquet avant de fragmenter les données en plusieurs paquets. Si le taux d'erreurs de paquet que vous rencontrez est élevé, vous pouvez légèrement augmenter le seuil de fragmentation. Un seuil de fragmentation trop bas peut se traduire par des performances faibles du réseau. Seule une légère diminution de la valeur par défaut est recommandée. Dans la plupart des cas, il est préférable de conserver la valeur par défaut, **2 346**.

- RTS Threshold (Seuil RTS). Si vous êtes confrontés à un flux de données incohérent, seules des réductions légères sont conseillées. Si un paquet du réseau apparaît plus petit que la taille pré-définie du seuil RTS, le mécanisme RTS/CTS n'est pas activé. le modem routeur transmet des trames RTS (Request To Send, demande d'émission) à une station de réception donnée et négocie l'envoi d'une trame de données. Après réception d'un signal RTS, la station sans fil répond par une trame CTS (Clear To Send, prêt pour émission) pour autoriser le lancement de la transmission. Il faut de préférence conserver le paramètre par défaut de cette valeur, soit **2 346**.

- Preamble Type (Type de préambule). Le préambule définit la longueur du bloc CRC pour la communication entre le modem routeur et le client d'itinérance sans fil. (Les zones dans lesquelles le trafic réseau est élevé doivent utiliser le type de préambule le plus court.) Sélectionnez le type de préambule approprié, **Long (default)** [Long (par défaut)] ou **Short** (Court).

- Network Density (Densité réseau). Ce paramètre détermine la portée de transmission et de réception du modem routeur. Sélectionnez l'un de ces paramètres, **Low** [(Basse), la portée est plus grande], **Medium** [(Moyenne), la portée moyenne] ou **High** [(Haute), la portée est plus petite]. Le paramètre Low (Basse) est recommandé lorsque vous disposez de peu de réseaux sans fil dans votre zone, tandis que le paramètre High (Haute) est recommandé lorsque vous avez un trafic réseau élevé dans votre zone. Vous pouvez utiliser le paramètre Medium (Moyenne) lorsque vous souhaitez un paramètre moyen. La valeur par défaut est **Low** (Basse).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet Security (Sécurité)

Onglet Firewall (Pare-feu)

Vous pouvez activer ou désactiver le pare-feu, définir des filtres pour bloquer des types de données Internet spécifiques et bloquer les requêtes Internet anonymes. Ces fonctions permettent d'améliorer la sécurité du réseau.

Firewall (Pare-feu)

- SPI Firewall Protection (Protection par pare-feu SPI). La fonctionnalité pare-feu SPI (Stateful Packet Inspection) renforce la sécurité de votre réseau. Pour utiliser cette fonctionnalité, cliquez sur **Enable** (Activer). Si vous ne souhaitez pas l'utiliser, cliquez sur **Disable** (Désactiver).

Filtres supplémentaires

- Filter Proxy (Filtrer le proxy). L'utilisation de serveurs proxy WAN peut compromettre la sécurité du modem routeur. La suppression du filtre de proxy désactive l'accès aux serveurs de proxy WAN. Pour activer le filtre de proxy, activez la case à cocher.
- Filter Cookies (Filtrer les cookies). Un cookie est un ensemble de données stocké sur votre ordinateur et utilisé par les sites Internet lorsque vous consultez des pages Web. Pour activer le filtrage des cookies, sélectionnez la case à cocher.
- Filter Java Applets (Filtrer les Applets Java). Java est un langage de programmation pour sites Web. Si vous supprimez le filtrage des applets Java, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation. Pour activer le filtrage des Applets Java, activez la case à cocher.
- Filter ActiveX (Filtrer ActiveX). ActiveX est un langage de programmation pour sites Web. Si vous supprimez le filtrage ActiveX, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation. Pour activer le filtrage ActiveX, activez la case à cocher.

Blocage des requêtes WAN

- Block Anonymous Internet Requests (Bloquer les requêtes Internet anonymes). Cette option permet à votre réseau de ne pas être détecté et renforce votre sécurité en cachant vos ports réseau. Les intrus auront ainsi plus de difficultés à découvrir votre réseau. Pour bloquer les requêtes Internet anonymes, activez l'option **Block Anonymous Internet Requests**. Pour autoriser ces requêtes, désactivez cette option.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-25 : Firewall (Pare-feu)

Onglet VPN Passthrough (Intercommunication VPN)

VPN (Virtual Private Networking) est une mesure de sécurité qui crée une connexion sécurisée entre deux emplacements distants. Si vous configurez ces paramètres, le modem routeur autorisera le passage de tunnels VPN.

VPN Passthrough (Intercommunication VPN)

- IPSec Passthrough (Intercommunication IPSec). La technologie IPSec (Internet Protocol Security) désigne une série de protocoles utilisés pour la mise en place d'un échange sécurisé des paquets au niveau de la couche IP. Pour activer l'option Intercommunication IPSec, cliquez sur le bouton **Enable** (Activer). Pour désactiver l'option Intercommunication IPSec, cliquez sur le bouton **Disable** (Désactiver).

- PPTP Passthrough (Intercommunication PPTP). L'intercommunication PPTP (Point-to-Point Tunneling Protocol) est la méthode utilisée pour activer les sessions VPN dans un serveur Windows NT 4.0 ou 2000. Pour activer l'option Intercommunication PPTP, cliquez sur le bouton **Enable** (Activer). Pour désactiver l'option Intercommunication PPTP, cliquez sur le bouton **Disable** (Désactiver).

- L2TP Passthrough (Intercommunication L2TP). L'Intercommunication L2TP (Layer 2 Tunneling Protocol) est une extension de PPTP (Point-to-Point Tunneling Protocol) utilisée pour activer le fonctionnement d'un VPN sur Internet. Pour activer l'intercommunication L2TP, cliquez sur le bouton **Enable** (Activer). Pour désactiver l'option Intercommunication L2TP, cliquez sur le bouton **Disable** (Désactiver).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-26 : VPN Passthrough (Intercommunication VPN)

Onglet VPN

VPN (Virtual Private Networking) est une mesure de sécurité qui crée une connexion sécurisée entre deux emplacements distants. Si vous configurez ces paramètres, le modem routeur créera le passage de tunnels VPN, avec un maximum de cinq.

VPN Tunnel (Tunnel VPN)

- Select Tunnel Entry (Sélectionner une entrée de tunnel). Pour établir ce tunnel, sélectionnez **New** (Nouveau). Pour modifier les paramètres d'un tunnel, sélectionnez le tunnel que vous souhaitez modifier.
- Delete (Supprimer). Pour supprimer un tunnel, sélectionnez-le dans le menu déroulant et cliquez sur le bouton **Delete** (Supprimer).
- Summary (Récapitulatif). Pour voir les paramètres d'un tunnel, sélectionnez-le dans le menu déroulant et cliquez sur le bouton **Summary** (Récapitulatif).
- IPSec VPN Tunnel (Tunnel VPN IPSec). Sélectionnez **Enable** (Activer) pour activer le tunnel VPN actuel. Pour désactiver le son, sélectionnez **Disable** (Désactiver).
- Tunnel Name (Nom du tunnel). Une fois le tunnel activé, attribuez-lui un nom. Les noms uniques vous permettent d'identifier divers tunnels. Il n'est pas nécessaire que le nom donné de ce côté du tunnel corresponde au nom utilisé à l'autre bout du tunnel.

Local Secure Group (Groupe sécurisé local)

Local Secure Group (Groupe sécurisé local) correspond à l'ordinateur ou aux ordinateurs de votre réseau local pouvant accéder au tunnel. Dans le menu déroulant, sélectionnez **IP Addr.** (Adresse IP) ou **Subnet** (Sous-réseau)

- IP Addr. (Adresse IP). Sélectionnez **IP Addr.** (Adresse IP) si vous souhaitez désigner un ordinateur spécifique. Saisissez ensuite l'adresse IP de l'ordinateur dans le champ *IP*.
- Subnet (Sous-réseau). Sélectionnez **Subnet** (Sous-réseau) si vous souhaitez inclure la totalité du réseau pour le tunnel. Saisissez ensuite l'adresse IP du modem routeur dans le champ *IP* et le masque de sous-réseau dans le champ *Mask* (Masque).

Remote Secure Group (Groupe sécurisé distant)

Remote Secure Group (Groupe sécurisé distant) correspond à l'ordinateur ou aux ordinateurs du côté distant du tunnel ; ordinateurs pouvant accéder au tunnel. Dans le menu déroulant, sélectionnez **IP Addr.** (Adresse IP), **Subnet** (Sous-réseau) ou **Any** (Tous).

- IP Addr. (Adresse IP). Sélectionnez **IP Addr.** (Adresse IP) si vous souhaitez désigner un ordinateur spécifique. Saisissez ensuite l'adresse IP de l'ordinateur dans le champ *IP*.
- Subnet (Sous-réseau). Sélectionnez **Subnet** (Sous-réseau) si vous souhaitez inclure la totalité du réseau pour le tunnel. Dans le champ *IP*, saisissez l'adresse IP du périphérique VPN distant, telle que le routeur, puis saisissez son masque de sous-réseau dans le champ *Mask* (Masque).
- Any (Tous). Sélectionnez **Any** (Tous) si vous souhaitez que le modem routeur accepte les requêtes de toutes les adresses IP.

Figure 6-27 : VPN

Figure 6-28 : VPN Settings Summary (Récapitulatif des paramètres VPN)

Remote Secure Gateway (Passerelle sécurisée distante)

Remote Security Gateway (Passerelle de sécurité distante) correspond au périphérique VPN du côté distant du tunnel VPN. Le périphérique VPN distant peut être un autre routeur VPN, un serveur VPN, ou un ordinateur exécutant un logiciel client VPN prenant en charge IPSec. Dans le menu déroulant, sélectionnez **IP Addr.** (Adresse IP) ou **Any** (Tous).

- IP Addr. (Adresse IP). Sélectionnez **IP Addr.** (Adresse IP) si vous souhaitez désigner une adresse IP statique. Saisissez ensuite l'adresse IP du VPN dans le champ *IP*.
- Any (Tous). Sélectionnez **Any** (Tous) si vous souhaitez que le modem routeur accepte les requêtes de toutes les adresses IP.

Key Management (Gestion de clé)

- Key Exchange Method (Méthode d'échange de clés). Sélectionnez **Auto (IKE)** ou **Manual** (Manuelle) pour la méthode d'échange de clés. Les deux côtés du tunnel VPN doivent utiliser le même mode de gestion de clé. Les deux méthodes sont décrites ci-dessous. Après avoir sélectionné la méthode, les paramètres disponibles sur cet écran peuvent varier, en fonction de la sélection effectuée.

Auto (IKE)

IKE est un protocole d'échange de clés Internet utilisé pour négocier des éléments clé pour une association de sécurité (SA). IKE utilise la clé pré-partagée pour authentifier la détection IDE distante.

- Encryption (Cryptage). Lorsque vous sélectionnez Auto (IKE), le cryptage 3DES (168 bits) est automatiquement sélectionné. Le même type de cryptage doit être utilisé par le périphérique VPN à l'autre bout du tunnel.
- Authentication (Authentification). Sélectionnez l'une des deux méthodes d'authentification disponibles, **SHA1** ou **MD5**. MD5 est un algorithme de hachage unidirectionnel qui produit une assimilation 128 bits. SHA est un algorithme de hachage unidirectionnel qui produit une assimilation 160 bits. SHA1 est recommandé car il est plus sûr. Assurez-vous que les deux côtés du tunnel VPN utiliser la même méthode d'authentification.
- PFS. PFS (Perfect Forward Secrecy) vous assure que l'échange de clé et les propositions IKE sont sécurisées. Pour utiliser PFS, sélectionnez **Enable** (Activer). Pour désactiver le son, sélectionnez **Disable** (Désactiver).
- Pre-Shared Key (Clé pré-partagée). Saisissez une suite de chiffres ou de lettres dans le champ *Pre-Shared Key* (Clé pré-partagée). Une clé est générée sur la base de ce mot, qui DOIT être saisi des deux côtés du tunnel. Elle permet de crypter les données transmises par le tunnel et de les décrypter à l'autre bout du tunnel. Ce champ peut être renseigné à l'aide d'une combinaison de chiffres et de lettres de 24 caractères maximum. Les caractères spéciaux ou les espaces ne sont pas autorisés.
- Key Life Time (Durée de validité de la clé). Vous pouvez sélectionner une date d'expiration de la clé. Saisissez la durée de validité de la clé en secondes ou laissez ce champ vierge pour que la clé reste valide indéfiniment.

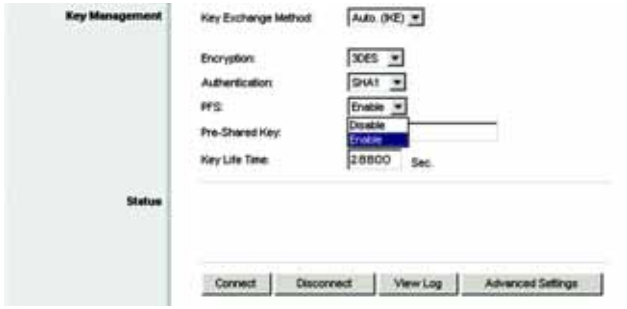


Figure 6-29 : Key Exchange Method - Auto (IKE) [Méthode d'échange de clés - Auto (IKE)]

Manual (Manuel)

Si vous sélectionnez Manual (Manuelle), vous générez vous-même la clé et aucune négociation de clé n'est nécessaire. La gestion de clé manuelle est utilisée dans les petits environnements statiques ou pour le dépannage.

- Encryption Algorithm (Algorithme de cryptage). Lorsque vous sélectionnez Manual (Manuelle), le cryptage 3DES (168 bits) est automatiquement sélectionné. Le même type de cryptage doit être utilisé par le périphérique VPN à l'autre bout du tunnel.
- Encryption Key (Clé de cryptage). Ce champ spécifie une clé utilisée pour crypter et décrypter le trafic IP. La clé de cryptage est de 48 bits. Vous devez donc saisir une clé de 24 caractères ASCII. Assurez-vous que les deux côtés du tunnel VPN utiliser la même clé de cryptage.
- Authentication Algorithm (Algorithme d'authentification). Sélectionnez une méthode d'authentification, **MD5** ou **SHA1**. Ceci détermine la manière dont les paquets ESP sont validés. MD5 est un algorithme de hachage unidirectionnel qui produit une assimilation 128 bits. SHA est un algorithme de hachage unidirectionnel qui produit une assimilation 160 bits. SHA1 est recommandé car il est plus sûr. Assurez-vous que les deux côtés du tunnel VPN utiliser la même méthode de d'authentification.
- Authentication Key (Clé d'authentification). Ce champ spécifie une clé utilisée pour authentifier le trafic IP. Saisissez une clé de valeurs hexadécimales. Si MD5 est sélectionné, la clé d'authentification est 32 bits. Vous devez donc saisir 16 caractères ASCII. Si SHA est sélectionné, la clé d'authentification est 40 bits. Vous devez donc saisir 20 caractères ASCII. Assurez-vous que les deux côtés du tunnel VPN utilisent la même clé d'authentification.
- Inbound et Outbound SPI (Security Parameter Index) [SPI en entrée et en sortie (Index de paramètre de sécurité)]. SPI transite dans l'en-tête ESP (Protocole Encapsulating Security Payload) et permet au destinataire et à l'expéditeur de sélectionner le SA, sous lequel un paquet doit être traité. Les valeurs hexadécimales sont acceptables et la plage de valeurs est 100~**ffffffff**. Chaque tunnel doit avoir un SPI en entrée et un SPI en sortie unique. Deux tunnels ne peuvent pas partager le même SPI. La valeur du champ Incoming SPI (SPI entrant) que vous définissez ici doit être identique à la valeur Outgoing SPI (SPI sortant) à l'autre bout du tunnel, et vice versa.

Figure 6-30 : Key Exchange Method -Manual (Méthode d'échange de clés - Manuelle)

Status (Etat)

Les informations d'état pour les tunnels VPN du modem routeur sont affichées ici.

Si vous sélectionnez Manual (Manuelle), vous aurez alors un bouton disponible. Cliquez sur le bouton **View Log** (Afficher fichier journal) pour voir les journaux d'activité.

Si vous sélectionnez Auto (IKE), vous aurez alors quatre boutons disponibles. Cliquez sur le bouton **Connect** (Connexion) pour démarrer la connexion VPN. Cliquez sur le bouton **Disconnect** (Déconnexion) pour terminer la connexion VPN. Cliquez sur le bouton **View Log** (Afficher fichier journal) pour voir les journaux d'activité. Cliquez sur le bouton **Advanced Settings** (Paramètres avancés) pour configurer les paramètres avancés du tunnel VPN.

Figure 6-31 : VPN Log (Fichier journal VPN)

Advanced VPN Tunnel Setup (Configuration avancée du tunnel VPN)

Cliquez sur le bouton **Advanced Settings** (Paramètres avancés) et l'écran *Advanced VPN Tunnel Setup* (Configuration avancée du tunnel VPN) s'affiche.

Ces paramètres IPSec avancés sont destinés aux utilisateurs expérimentés.

Phase 1

Cette phase permet de créer une association de sécurité (SA) souvent appelée IKE SA. Une fois la Phase 1 terminée, la Phase 2 permet de créer une ou plusieurs IPSec SA, qui sont ensuite utilisées dans les sessions de clés IPSec.

Operation Mode (Mode de fonctionnement). Il existe deux modes de fonctionnement : Main (Principal) et Aggressive (Agressif). Ils peuvent échanger les mêmes charges IKE en différentes séquences. Le mode Principal est le plus utilisé. Néanmoins, certains utilisateurs préfèrent le mode Agressif car il est plus rapide. Le mode Principal est destiné à utilisation normale et inclut plus de requêtes d'authentification que le mode Agressif. Le mode Principal est recommandé car il est plus sûr. Quel que soit le mode sélectionné, le modem routeur VPN acceptera les requêtes Principal et Agressif du périphérique VPN distant.

Local Identity (Identité locale). Sélectionnez le bouton radio **Local IP address** (Adresse IP locale) ou **Name** (Nom). Si vous sélectionnez Local IP address (Adresse IP locale), l'adresse IP Internet du modem routeur sera utilisée. Si vous sélectionnez Name (Nom), saisissez le FQDN (Fully Qualified Domain Name) du modem routeur dans le champ prévu à cet effet, ainsi son adresse IP actuelle pourra être localisée via DDNS.

Remote Identity (Identité distante). Sélectionnez le bouton radio **Remote IP address** (Adresse IP distante) ou **Name** (Nom). Si vous sélectionnez Remote IP address (Adresse IP distante), l'adresse IP Internet du périphérique VPN distant sera utilisé. Si vous sélectionnez Name (Nom), saisissez le FQDN (Fully Qualified Domain Name) du périphérique VPN distant dans le champ prévu à cet effet, ainsi son adresse IP actuelle pourra être localisée via DDNS.

Encryption (Cryptage). Pour le cryptage ou le décryptage des paquets ESP. Le cryptage 3DES (168 bits) est automatiquement sélectionné.

Authentication (Authentification). Sélectionnez la méthode utilisée pour authentifier les paquets ESP. Vous avez deux choix : MD5 et SHA1. SHA1 est recommandé car il est plus sûr.

Group (Groupe). Vous pouvez choisir entre trois groupes Diffie-Hellman : 768-bit (768 bits), 1024-bit (1024 bits) et 1536-bit (1536 bits). Diffie-Hellman se réfère à une technique de cryptographie utilisée par les clés publiques et privées pour le cryptage et le décryptage.

Key Life Time (Durée de validité de la clé). Dans le champ *Key Lifetime* (Durée de validité de la clé), vous pouvez sélectionner une date d'expiration de la clé (facultatif). Saisissez la durée de validité de la clé en secondes avant la prochaine renégociation de clé entre chaque point terminal.

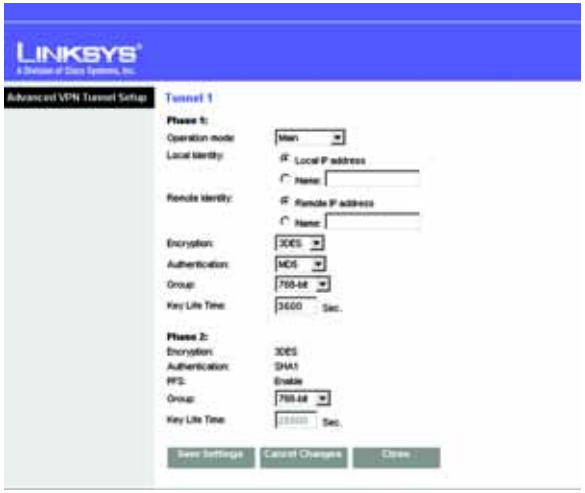


Figure 6-32 : Advanced VPN Tunnel Setup (Configuration avancée du tunnel VPN)

Phase 2

Encryption (Cryptage). La méthode de cryptage sélectionnée à la Phase 1 s'affiche à l'écran.

Authentication (Authentification). La méthode d'authentification sélectionnée à la Phase 1 s'affiche à l'écran.

PFS. L'état du PFS s'affiche à l'écran.

Group (Groupe). Vous pouvez choisir entre trois groupes Diffie-Hellman : 768-bit (768 bits), 1024-bit (1024 bits) et 1536-bit (1536 bits). Diffie-Hellman se réfère à une technique de cryptographie utilisée par les clés publiques et privées pour le cryptage et le décryptage.

Key Life Time (Durée de validité de la clé). Dans le champ *Key Lifetime* (Durée de validité de la clé), vous pouvez sélectionner une date d'expiration de la clé (facultatif). Saisissez la durée de validité de la clé en secondes avant la prochaine renégociation de clé entre chaque point terminal.

Lorsque vous avez terminé d'apporter des modifications dans cet écran, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer les modifications ou le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet Access Restrictions (Restrictions d'accès)

Onglet Internet Access Policy (Stratégie d'accès à Internet)

L'écran *Internet Access Policy* (Stratégie d'accès à Internet) vous permet de bloquer ou d'autoriser des modes spécifiques d'exploitation Internet. Vous pouvez définir vos stratégies d'accès à Internet pour des ordinateurs spécifiques et bloquer l'accès à certains sites Web avec leur URL ou leur mot de passe.

Internet Access Policy (Stratégie d'accès à Internet)

Internet Access Policy (Stratégie d'accès à Internet). Vous pouvez contrôler l'accès à l'aide d'une stratégie. Utilisez les paramètres de cet écran pour définir une stratégie d'accès [après avoir cliqué sur le bouton **Save Settings** (Enregistrer les paramètres)]. La sélection d'une stratégie dans le menu déroulant permet d'afficher les paramètres de la stratégie en question. Pour supprimer une stratégie, sélectionnez son numéro, puis cliquez sur le bouton **Delete** (Supprimer). Pour afficher l'ensemble des stratégies, cliquez sur le bouton **Summary** (Récapitulatif). Vous pouvez supprimer les stratégies à partir de l'écran *Summary* (Récapitulatif) en sélectionnant la ou les stratégies, puis en cliquant sur le bouton **Delete** (Supprimer). Pour revenir à l'écran Internet Access (Accès à Internet), cliquez sur le bouton **Close** (Fermer).

Status (Etat). Par défaut, les stratégies sont activées. Pour activer une stratégie, sélectionnez son numéro dans le menu déroulant, puis cliquez sur le bouton radio en regard de l'option *Enable* (Activer).

Pour créer une stratégie d'accès à Internet :

1. Sélectionnez un numéro dans le menu déroulant *Internet Access Policy* (Stratégie d'accès à Internet).
2. Pour activer cette stratégie, cliquez sur le bouton radio en regard de l'option *Enable* (Activer).
3. Saisissez le nom de la stratégie dans le champ Policy Name (Nom de la stratégie) prévu à cet effet.

Figure 6-33 : Internet Access Policy (Stratégie d'accès à Internet)

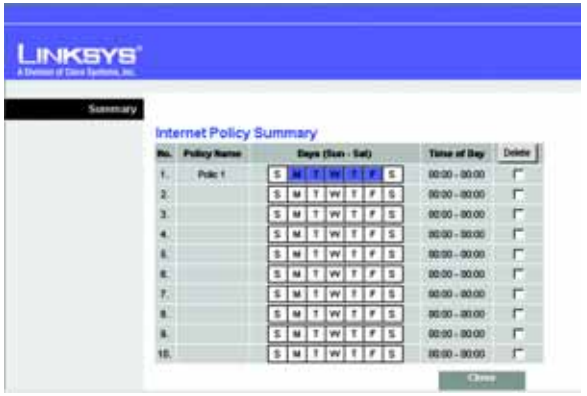


Figure 6-34 : Internet Policy Summary (Récapitulatif de la stratégie Internet)

4. Cliquez sur le bouton **Edit List of PCs** (Liste des ordinateurs) pour sélectionner les ordinateurs auxquels cette stratégie doit s'appliquer. L'écran *List of PCs* (Liste des ordinateurs) apparaît. Vous pouvez sélectionner un ordinateur selon son adresse MAC ou son adresse IP. Vous pouvez également saisir une plage d'adresses IP si vous souhaitez appliquer cette stratégie à un groupe d'ordinateurs. Une fois vos modifications effectuées, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour valider ces modifications ou sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Cliquez ensuite sur le bouton **Close** pour quitter cet écran.

5. Sélectionnez l'option **Deny** (Refuser) ou **Allow** (Autoriser) pour bloquer ou autoriser l'accès à Internet aux ordinateurs répertoriés dans l'écran *List of PCs* (Liste des ordinateurs).

6. Définissez les jours et les heures pendant lesquels vous souhaitez appliquer cette stratégie. Sélectionnez un à un les jours auxquels la stratégie doit s'appliquer, ou sélectionnez **Everyday** (Tous les jours). Saisissez une plage d'heures et de minutes pendant lesquelles la stratégie devra être appliquée, ou sélectionnez l'option **24 Hours** (24 heures).

7. Si vous souhaitez bloquer des sites Web dotés d'adresses URL spécifiques, saisissez chaque URL dans un champ distinct en regard de la section *Website Blocking by URL Address* (Blocage de site Web par adresse URL).

8. Si vous souhaitez bloquer des sites Web à l'aide de mots clés spécifiques, saisissez chaque mot clé dans un champ distinct en regard de la section *Website Blocking by Keyword* (Blocage de site Web par mot clé).

9. Vous pouvez filtrer l'accès à divers services accessibles par Internet, notamment FTP ou Telnet, en choisissant ces services dans les menus déroulants en regard de l'option *Blocked Services* (Services bloqués). Les numéros de port et le protocole pour le service sélectionné s'affichent automatiquement.

   Si le service souhaité n'est pas répertorié, sélectionnez **User-Defined** (Défini par l'utilisateur). Saisissez ses numéros de port dans les champs prévus à cet effet. Sélectionnez ensuite son protocole, **ICMP**, **TCP**, **UDP** ou **TCP & UDP** dans le menu déroulant.

10. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer les paramètres de la stratégie. Pour annuler ces mêmes paramètres, cliquez sur le bouton **Cancel Changes** (Annuler les modifications). Pour plus d'informations, cliquez sur **Help** (Aide).

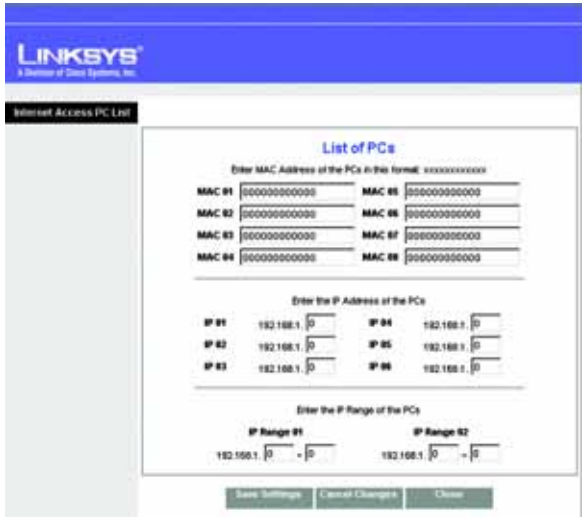


Figure 6-35 : List of PCs (Liste des ordinateurs)

Onglet Applications and Gaming (Applications et jeux)

Onglet Single Port Range Forwarding (Transfert de connexion unique)

L'écran *Single Port Range Forwarding* (Transfert de connexion unique) vous permet d'ouvrir un port spécifique de façon à ce que les utilisateurs puissent voir, sur Internet, les serveurs qui se trouvent derrière le modem routeur (tels que serveurs FTP ou de messagerie électronique). Lorsque des utilisateurs envoient ce type de requête vers votre réseau via Internet, le modem routeur transfère ces requêtes vers l'ordinateur approprié. Tout ordinateur dont le port est transféré doit avoir sa fonction de client DHCP désactivée et doit disposer d'une nouvelle adresse IP statique puisque son adresse IP risque de changer lors de l'utilisation de la fonction DHCP.

Single Port Forwarding (Transfert de connexion unique)

- Application. Saisissez le nom de l'application dans ce champ.
- External Port (Port externe) et Internal Port (Port interne). Saisissez ensuite les numéros de ports internes et externes.
- Protocol (Protocole). Sélectionnez le protocole que vous souhaitez utiliser pour chaque application : **TCP** ou **UDP**.
- IP Address (Adresse IP). Saisissez l'adresse IP de l'ordinateur concerné.
- Enabled (Activé). Cliquez sur **Enabled** (Activé) pour activer le transfert vers l'application choisie.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-36 : Single Port Forwarding (Transfert de connexion unique)

Onglet Port Range Forwarding (Transfert de connexion)

L'écran *Port Range Forwarding* (Transfert de connexion) définit les services publics de votre réseau, tels que serveurs Web, serveurs FTP, serveurs de messagerie électronique ou toute autre application Internet spécialisée. (Par applications spécialisées, on entend toutes les applications qui utilisent un accès à Internet pour effectuer des fonctions spécifiques, telles que la vidéoconférence ou les jeux en ligne. Certaines applications Internet peuvent n'exiger aucun transfert.)

Lorsque des utilisateurs envoient ce type de requête vers votre réseau via Internet, le modem routeur transfère ces requêtes vers l'ordinateur approprié. Tout ordinateur dont le port est transféré doit avoir sa fonction de client DHCP désactivée et doit disposer d'une nouvelle adresse IP statique puisque son adresse IP risque de changer lors de l'utilisation de la fonction DHCP.

Figure 6-37 : Port Range Forwarding (Transfert de connexion)

Port Range Forwarding (Transfert de connexion)

- Application. Saisissez le nom de l'application dans ce champ.
- Start (Début) et End (Fin). Saisissez les numéros de début et de fin du port que vous souhaitez transférer.
- Protocol (Protocole). Sélectionnez le protocole que vous souhaitez utiliser pour chaque application : **TCP**, **UDP** ou **Both** (Les deux).
- IP Address (Adresse IP). Saisissez l'adresse IP de l'ordinateur concerné.
- Enable (Activer). Activez la case à cocher **Enable** (Activer) pour activer le transfert vers l'application choisie.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet Port Triggering (Déclenchement de connexion)

Le déclenchement de connexion est utilisé pour des applications spécifiques qui peuvent nécessiter l'ouverture d'un port à la demande. Pour cette fonction, le modem routeur contrôle les données sortantes de certains numéros de ports spécifiques. le modem routeur enregistre l'adresse IP de l'ordinateur qui envoie une requête de données. Ainsi, lorsque les données transitent de nouveau par le modem routeur, elles sont dirigées vers l'ordinateur approprié au moyen de l'adresse IP et des règles de mappage de ports.

Port Range Triggering (Déclenchement de connexion)

- Application. Saisissez le nom que vous souhaitez donner à chaque application.
- Triggered Range (Connexion sortante déclenchée). Saisissez les numéros de port de départ et de fin de la connexion sortante transférée.
- Forwarded Range (Connexion entrante transférée). Saisissez les numéros de port de départ et de fin de la connexion entrante transférée.
- Enabled (Activé). Activez la case à cocher **Enabled** (Activé) pour activer le déclenchement de connexion pour l'application choisie.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-38 : Port Triggering (Déclenchement de connexion)

Onglet DMZ

L'écran *DMZ* permet à un utilisateur local d'accéder à Internet en vue d'utiliser un service à usage spécifique, tel que des jeux Internet ou un système de vidéoconférence via l'hébergement DMZ. L'hébergement DMZ transfère simultanément tous les ports d'un ordinateur, à la différence de l'option Port Range Forwarding (Transfert de connexion) qui ne permet de transférer que 10 connexions au maximum.

Figure 6-39 : DMZ

DMZ

- DMZ Hosting (Hébergement DMZ). Cette fonctionnalité permet à un utilisateur local d'accéder à Internet en vue d'utiliser un service à usage spécifique, tel que des jeux Internet ou un système de vidéoconférence. Pour activer cette fonctionnalité, sélectionnez **Enable** (Activer). Pour la désactiver, sélectionnez **Disable** (Désactiver).

- DMZ Host IP Address (Adresse IP de l'hôte DMZ). Pour exposer un ordinateur, saisissez l'adresse IP de cet ordinateur. Pour obtenir l'adresse IP d'un ordinateur, reportez-vous à l'« Annexe C : Recherche des adresses MAC et IP de votre carte Ethernet ».

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet QoS (QS)

QS (qualité de service)

La qualité de service (QS) assure un meilleur service aux types de priorité élevée du trafic réseau, pouvant impliquer des applications importantes en temps réel, comme les appels téléphoniques ou la vidéoconférence via Internet.

Figure 6-40 : QoS (QS)

Wireless (Sans fil)

- **ACK Mode** (Mode ACK). Ce paramètre affecte la priorité à QoS pour les utilisateurs qui ont activé ACK Mode (Mode ACK). Les utilisateurs avec Immediate ACK (ACK immédiat) (le paramètre par défaut) profiteront d'une connectivité fiable pour une utilisation normale du réseau. Burst ACK (ACK rafale) est plus rapide mais moins fiable et peut aussi affecter les performances sans fil longue distance. Le paramètre No ACK (Sans ACK) désactive la fonction ACK. Les clients qui utilisent ACK doivent veiller à ce que leur carte sans fil possède le même paramètre que le modem routeur. Ceci est normalement utilisé dans une multidiffusion comme de la vidéo. Ne l'utilisez pas, à moins que vous soyez un utilisateur expérimenté.
- **802.11e/QoS** (802.11e/QS). QS sera activé par défaut pour fournir une performance optimale de votre connexion sans fil. Sélectionnez **Disable** (Désactiver) pour améliorer les performances d'un réseau sans fil mixte.

Internet Access Priority (Priorité d'accès à Internet)

Dans cette section, vous pouvez définir la priorité basée sur l'application, le transfert de port ou l'adresse MAC. Vous pouvez définir quatre types de priorité : High (Haute), Medium (Moyenne), Normal (Normale) ou Low (Basse).

- Enable/Disable (Activer/Désactiver). Pour limiter la bande passante sortante des stratégies QS en cours d'utilisation, sélectionnez **Enabled** (Activé). Sinon, sélectionnez **Disabled** (Désactivé).
- Set Internet Bandwidth (Définir la bande passante Internet). Ce paramètre vous permet de limiter la bande passante sortante des stratégies QS en cours d'utilisation. Vous contrôlez ainsi la bande passante utilisée par une application donnée. Saisissez la bande passante dans ce champ.
- Application. Avec cette option, vous pouvez sélectionner **None** (Aucun), **Online Game** (Jeu en ligne), **MSN Messenger**, **YAHOO Messenger**, **Skype**, **Voice Device** (Périphérique vocal), **Add a New Application** (Ajout d'une nouvelle application) ou faites un choix dans la liste d'applications à définir. Pour créer une nouvelle entrée, sélectionnez **Add a New Application** (Ajout d'une nouvelle application) et reportez-vous à la section *Ajout d'une nouvelle application*.
- Priority (Priorité). Sélectionnez **High** (Haute), **Medium** (Moyenne), **Normal** (Normale) ou **Low** (Basse) pour la priorité de bande passante nécessaire pour l'application sélectionnée. Ne définissez pas toutes les applications sur High (Haute), sinon l'allocation de bande passante disponible échouera. Si vous souhaitez sélectionner la bande passante normale ci-dessous, sélectionnez **Low** (Basse). En fonction de l'application, quelques tentatives seront peut-être nécessaires pour définir la priorité de bande passante appropriée. Une fois le choix effectué, cliquez sur **Add** (Ajouter) pour l'ajouter à la liste Summary (Récapitulatif).

Online Game (Jeu en ligne)

La sélection de l'option Online Game (Jeu en ligne) affichera le menu déroulant *Select a Game* (Sélectionner un jeu), qui répertorie quelques jeux pré-configurés courants. Sélectionnez le jeu dans la liste, puis sélectionnez sa priorité.

MSN Messenger

Sélectionnez sa priorité dans le menu déroulant, puis cliquez sur **Add** (Ajouter).

YAHOO Messenger

Sélectionnez sa priorité dans le menu déroulant, puis cliquez sur **Add** (Ajouter).

Skype

Sélectionnez sa priorité dans le menu déroulant, puis cliquez sur **Add** (Ajouter).

Voice Device (Périphérique vocal)

Saisissez le nom du périphérique réseau dans le champ *Enter a Name* (Saisir un nom), saisissez son adresse MAC, puis sélectionnez sa priorité dans le menu déroulant, puis cliquez sur **Add** (Ajouter).

Add a New Application (Ajout d'une nouvelle application)

Enter a Name (Saisir un nom) — Saisissez un nom pour indiquer le nom de l'entrée.

Category (Catégorie) — Sélectionnez **Port Range** (Plage de ports) ou **MAC Address** (Adresse MAC) pour le modem routeur à utiliser pour définir la priorité de bande passante.

Port Range (Plage de ports) — Si vous sélectionnez Port Range (Plage de ports), cette catégorie sera disponible. Elle vous permet de saisir la(les) plage(s) de ports que l'application utilisera. Par exemple, si vous souhaitez allouer la bande passante pour FTP, vous pouvez saisir 21-21. Si vous avez besoin de services pour une application qui utilise entre 1000 et 1250 ports, saisissez 1000-1250 comme paramètre. Les nombres de ports peuvent varier de 1 à 65 535. Consultez la documentation relative à votre application pour plus de détails quant aux ports de service utilisés.

Vous pouvez définir jusqu'à trois plages pour cette allocation de bande passante. Pour chaque plage de port, désignez le(s) type(s) de protocole : **TCP**, **UDP** ou **Both** (Les deux).

Figure 6-41 : QoS - Online Game (QS - Jeu en ligne)

Figure 6-42 : QoS - MSN Messenger (QS - MSN Messenger)

Figure 6-43 : QoS - Voice Device (QS - Périphérique vocal)

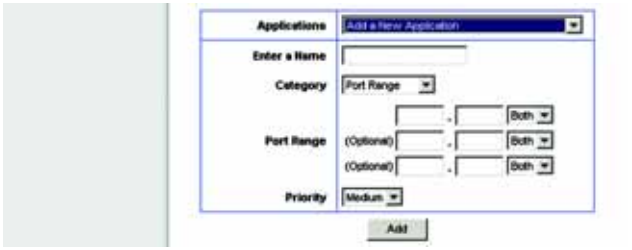


Figure 6-44 : QoS - Add a New Application (QS - Ajout d'une nouvelle application) - Port Range (Plage de ports)

MAC Address (Adresse MAC) Si vous sélectionnez MAC Address (Adresse Mac), cette catégorie sera disponible. Saisissez une adresse MAC à 12 chiffres hexadécimaux pour représenter le périphérique que vous souhaitez définir comme une priorité de bande passante. Il s'agit d'un identificateur unique pour votre périphérique réseau. Lorsque le modem routeur identifie le périphérique saisi, le modem routeur alloue la priorité définie pour cette entrée. Consultez la documentation relative à votre périphérique pour obtenir une adresse MAC.

Priority (Priorité) Sélectionnez la priorité de bande passante pour l'application sélectionnée. Sélectionnez **High** (Haute), **Medium** (Moyenne), **Normal** (Normale) ou **Low** (Basse) pour la bande passante, mais ne définissez pas toutes les applications sur High (Haute). Une fois le choix effectué, cliquez sur **Add** (Ajouter) pour l'ajouter à la liste Summary (Récapitulatif).

Summary (Récapitulatif)

Priority (Priorité) Ce champ affiche la priorité d'allocation de bande passante sur High (Haute), Medium (Moyenne), Normal (Normale) ou Low (Basse) que vous définissez pour l'application.

Name (Nom) Ce champ affiche le nom de l'application ou les entrées saisies à allouer.

Information (Informations) Ce champ affiche la plage de ports ou l'adresse MAC saisie lorsque vous avez ajouté une nouvelle application. Si une application pré-configurée a été sélectionnée, cette section ne contient pas aucune entrée valide.

Remove (Supprimer) Ce bouton vous permet de supprimer l'entrée d'application. Pour supprimer l'entrée, cliquez sur le bouton **Remove** (Supprimer). Pour enregistrer la configuration, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres). Sinon, pour annuler, cliquez sur le bouton **Cancel Changes** (Annuler les modifications).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-45 : QoS - Add a New Application (QS - Ajout d'une nouvelle application) - MAC Address (Adresse MAC)

Onglet Administration

Onglet Management (Gestion)

L'écran *Management* (Gestion) vous permet de modifier les paramètres d'accès au modem routeur et de configurer les fonctionnalités de gestion SNMP (Simple Network Management Protocol), UPnP (Universal Plug and Play) et WLAN.

Gateway Access (Accès au modem routeur)

Local Gateway Access (Accès local au modem routeur). Pour assurer la sécurité du modem routeur, vous devez entrer un mot de passe pour accéder à l'utilitaire Web du modem routeur. Le nom d'utilisateur et le mot de passe par défaut est **admin**.

- Gateway Userlist (Liste d'utilisateurs du modem routeur). Sélectionnez le numéro de l'utilisateur dans le menu déroulant.
- Gateway Username (Nom d'utilisateur du modem routeur). Saisissez le nom d'utilisateur par défaut, **admin**. Il est recommandé de remplacer ce nom d'utilisateur par défaut par un nom de votre choix.
- Gateway Password (Mot de passe du modem routeur). Il est recommandé de remplacer le mot de passe par défaut, **admin**, par un mot de passe de votre choix.
- Re-enter to confirm (Confirmation du mot de passe). Saisissez de nouveau le nouveau mot de passe du modem routeur pour le confirmer.

Remote Gateway Access (Accès distant au modem routeur). Cette fonction vous permet d'accéder au modem routeur à partir d'un emplacement distant, via Internet.

- Remote Management (Gestion distante). Cette fonction vous permet d'administrer le modem routeur à partir d'un emplacement distant, via Internet. Pour activer la gestion à distance, cliquez sur **Enable** (Activer).

IMPORTANT : L'activation de la gestion distante permet à chaque personne disposant de votre mot de passe de configurer à distance le modem routeur via Internet.

- Management Port (Port de gestion). Saisissez le numéro de port que vous souhaitez utiliser pour accéder à distance au modem routeur.

Figure 6-46 : Management (Gestion)

SNMP

SNMP est un protocole très répandu de contrôle et de gestion réseau.

- Device Name (Nom de périphérique). Saisissez le nom du modem routeur.
- SNMP. Pour activer la fonctionnalité SNMP, cliquez sur **Enable** (Activer). Pour désactiver la fonctionnalité SNMP, cliquez sur **Disable** (Désactiver).
- Get Community (Obtenir la communauté). Saisissez le mot de passe permettant l'accès en lecture seule aux informations SNMP du modem routeur.
- Set Community (Définir la communauté). Saisissez le mot de passe permettant l'accès en lecture/écriture aux informations SNMP du modem routeur.
- Trap Management (Gestion de déroutement) : Trap to (Dérouter vers). Saisissez l'adresse IP de l'ordinateur hôte distant auquel s'adressent les messages déroutés.

UPnP

La fonctionnalité UPnP permet à Windows Me et XP de configurer automatiquement le modem routeur pour diverses applications Internet, telles que des jeux Internet ou un système de vidéoconférence.

- UPnP. Pour activer la fonctionnalité UPnP, cliquez sur **Enable** (Activer). Sinon, cliquez sur **Disable** (Désactiver).

WLAN

- Management via WLAN (Gestion via WLAN). Cette fonction vous permet d'administrer le modem routeur sur un ordinateur sans fil du réseau local lorsqu'elle est connectée à l'utilitaire Web du modem routeur. Pour activer cette fonction, cliquez sur **Enable** (Activer). Sinon, cliquez sur **Disable** (Désactiver).

IGMP

- IGMP Proxy (Proxy IGMP). Si votre périphérique ou votre application multimédia ne fonctionnent pas correctement derrière le modem routeur, vous pouvez utiliser le proxy IGMP pour autoriser la multidiffusion via le modem routeur. Pour utiliser cette fonctionnalité, cliquez sur **Enable** (Activer). Sinon, cliquez sur **Disable** (Désactiver).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet Reporting (Rapports)

L'écran *Reporting* (Rapports) fournit un fichier journal de toutes les URL ou adresses IP entrantes et sortantes de votre connexion Internet. Il fournit également des fichiers journaux de tous les événements VPN et de pare-feu.

Figure 6-48 : Reporting (Rapports)

Reporting (Rapports)

- Log (Fichier journal). Pour activer la génération de fichiers journaux, cliquez sur **Enable** (Activer).

Email Alerts (Alertes de messagerie électronique)

- E-Mail Alerts (Alertes de messagerie électronique). Pour activer les alertes de messagerie électronique, cliquez sur **Enable** (Activer).
- Denial of Service Thresholds (Seuils de refus de service). Saisissez le nombre d'attaques DoS (Denial of Service) qui déclencheront une alerte par courrier électronique.
- SMTP Mail Server (Serveur de messagerie électronique SMTP). Saisissez l'adresse IP du serveur SMTP.
- E-Mail Address for Alert Logs (Adresse de messagerie électronique pour fichiers journaux d'alertes). Saisissez l'adresse électronique pour la réception des journaux d'alertes.
- Return E-Mail address (Adresse de messagerie électronique de retour). Saisissez l'adresse de retour des alertes de messagerie électronique.

Pour afficher les fichiers journaux, cliquez sur le bouton **View Logs** (Afficher les fichiers journaux). Un nouvel écran apparaît. Dans le menu déroulant, sélectionnez le journal que vous souhaitez visualiser : **ALL** (Tous), **Access Log** (Journal d'accès) ou **Firewall Log** (Journal du pare-feu). Cliquez sur le bouton **pageRefresh** (Actualiser la page) pour mettre à jour les informations. Cliquez sur le bouton **Clear** (Supprimer) pour supprimer les informations. Cliquez sur le bouton **Previous Page** (Page précédente) pour revenir à la page précédente. Cliquez sur le bouton **Next Page** (Page suivante) pour accéder à la page suivante.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-49 : System Log (Journal système)

Onglet Diagnostics

Cet écran vous permet d'effectuer des tests Ping et d'afficher les résultats.

Figure 6-50 : Diagnostics

Ping Test (Test Ping)

Ping Test Parameters (Paramètres de test Ping)

- Ping Target IP (IP de cible Ping). Saisissez l'adresse IP pour laquelle vous souhaitez effectuer le test Ping. Il peut s'agir d'une adresse IP locale (LAN) ou Internet (WAN).
- Ping Size (Taille de Ping). Saisissez la taille du paquet.
- Number of Pings (Nombre de Pings). Saisissez le nombre de fois que vous souhaitez effectuer le Ping.
- Ping Interval (Intervalle de Ping). Saisissez l'intervalle de Ping (fréquence du Ping de l'adresse IP cible) en millisecondes.
- Ping Timeout (Délai de Ping). Saisissez le délai de Ping (délai avant la fin du Ping) en millisecondes.

Cliquez sur le bouton **Start Test** (Démarrer le test) pour démarrer le test de Ping.

- Ping Result (Résultat de Ping). Les résultats du test Ping sont affichés ici.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet Backup&Restore (Sauvegarde&restauration)

Cet onglet permet de sauvegarder et de restaurer le fichier de configuration du modem routeur.

Figure 6-51 : Backup&Restore (Sauvegarde et restauration)

Backup Configuration (Sauvegarder la configuration)

Pour sauvegarder le fichier de configuration du modem routeur, cliquez sur le bouton **Backup** (Sauvegarder). Suivez les instructions affichées.

Restore Configuration (Restaurer la configuration)

Pour restaurer le fichier de configuration du modem routeur, cliquez sur le bouton **Browse** (Parcourir). Puis suivez les instructions affichées pour localiser le fichier. Après avoir sélectionné le fichier, cliquez sur le bouton **Restore** (Restaurer).

Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet Factory Defaults (Paramètres usine par défaut)

Cet écran vous permet de restaurer les paramètres d'usine (par défaut) du modem routeur.

Factory Defaults (Paramètres d'usine)

Restore Factory Defaults (Restaurer les paramètres d'usine) : Si vous souhaitez restaurer les paramètres d'usine du modem routeur (vous perdrez alors tous vos paramètres), cliquez sur **Restore Factory Defaults** (Restaurer les paramètres d'usine). Suivez les instructions affichées. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-52 : Factory Defaults (Paramètres d'usine)

Onglet Firmware Upgrade (Mise à niveau du micrologiciel)

Utilisez cet écran pour mettre à niveau le micrologiciel du modem routeur.

Firmware Upgrade (Mise à niveau du micrologiciel)

Pour mettre à niveau le micrologiciel du modem routeur :

1. Téléchargez le fichier de mise à niveau du micrologiciel du modem routeur depuis le site www.linksys.com/international.
2. Extrayez le fichier sur votre ordinateur.
3. Dans l'écran *Firmware Upgrade* (Mise à niveau du micrologiciel), cliquez sur le bouton **Browse** (Parcourir) pour trouver le fichier de mise à niveau du micrologiciel.
4. Cliquez deux fois sur le fichier du micrologiciel que vous venez de télécharger et de décompresser.
5. Cliquez sur le bouton **Start to Upgrade** (Lancer la mise à niveau) et suivez les instructions à l'écran.

Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-53 : Firmware Upgrade (Mise à niveau du micrologiciel)

Onglet Status (Etat)

Onglet Gateway (Passerelle)

Cet écran contient des informations sur votre modem routeur et sa connexion Internet.

Gateway Information (Informations sur le modem routeur)

Cette section contient les éléments suivants sur le modem routeur : Firmware Version (Version du micrologiciel), MAC Address (Adresse Mac) et Current Time (Heure actuelle).

Internet Connection (Connexion Internet)

Cette section contient les éléments suivants : Login Type (Type de connexion), Interface, IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau), Default Gateway (Passerelle par défaut) et adresses IP des serveurs DNS 1, 2 et 3.

Figure 6-54 : Gateway (Passerelle)

DHCP Renew (Renouvellement DHCP). S'il est disponible, cliquez sur le bouton **DHCP Renew** (Renouvellement DHCP) pour remplacer l'adresse IP actuelle du modem routeur par une nouvelle adresse IP.

DHCP Release (Version DHCP). S'il est disponible, cliquez sur le bouton **DHCP Release** (Version DHCP) pour supprimer l'adresse IP actuelle du modem routeur.

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Pour plus d'informations, cliquez sur **Help** (Aide).

Onglet Local Network (Réseau local)

Cet écran affiche des informations sur le réseau local du modem routeur.

Local Network (Réseau local)

Cette section contient les éléments suivants : local Mac Address (Adresse Mac locale), IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau), DHCP Server (Serveur DHCP), Start IP Address (Adresse IP de début) et End IP Address (Adresse IP de fin).

Pour afficher le DHCP Client Table (Tableau des clients DHCP), cliquez sur le bouton **DHCP Clients Table** (Tableau des clients DHCP). Pour afficher le ARP/RARP Table (Tableau ARP/RARP), cliquez sur le bouton **ARP/RARP Table** (Tableau ARP/RARP).

DHCP Clients Table (Tableau des clients DHCP). Le tableau des clients DHCP affiche les données actuelles des clients DHCP. Vous verrez les informations suivantes : nom de l'ordinateur, adresse IP, adresse MAC et délai d'expiration de l'adresse IP dynamique des clients sans fil utilisant le serveur DHCP. (Ces données sont stockées dans la mémoire temporaire et sont régulièrement modifiées.) Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Pour supprimer un client d'un serveur DHCP, sélectionnez le client, puis cliquez sur le bouton **Delete** (Supprimer). Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran *Local Network* (Réseau local).

ARP/RARP Table (Tableau ARP/RARP). Une requête ARP est une requête envoyée du modem routeur aux clients ayant une adresse IP pour leur demander leurs adresses MAC. le modem routeur peut ainsi établir une correspondance entre les adresses IP et les adresses MAC. RARP est le contraire de ARP. Le tableau ARP/RARP affiche les données actuelles des clients du réseau local du modem routeur. Vous verrez apparaître leurs adresses IP et MAC. (Ces données sont stockées dans la mémoire temporaire et sont régulièrement modifiées.) Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran *Local Network* (Réseau local).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-55 : Local Network (Réseau local)

Figure 6-56 : DHCP Active IP Table (Tableau IP active DHCP)

Figure 6-57 : ARP/RARP Table (Tableau ARP RARP)

Onglet Wireless (Sans fil)

Cet écran affiche des informations sur le réseau sans fil du modem routeur.

Wireless (Sans fil)

Cet écran affiche les éléments suivants : Wireless Firmware Version (Version du micrologiciel), MAC Address (Adresse MAC), Mode, SSID, Channel (Canal) et Encryption Function (Fonction de cryptage).

Cliquez sur le bouton **Wireless Clients Connected** (Clients sans fil connectés) pour afficher les clients sans fil connectés au modem routeur, ainsi que leurs noms d'ordinateurs, adresses IP et adresses Mac. Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran *Wireless* (Sans fil).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-58 : Wireless (Sans fil)

Figure 6-59 : Networked Computers (Ordinateurs réseau)

Onglet DSL Connection (Connexion DSL)

Cet écran contient des informations sur la connexion DSL.

DSL Status (Etat DSL)

Cette section présente les éléments suivants : Status (Etat), Downstream Rate (Débit de réception) et Upstream Rate (Débit d'émission).

PVC Connection (Connexion PVC)

Cette section présente les informations suivantes : Encapsulation, Multiplexing (Multiplexage), QoS (QS), Pcr Rate (Taux Pcr), Scr Rate (Taux Scr), Autodetect (Détection automatique), VPI, VCI, Enable status (Etat activation) et PVC Status (Etat PVC).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Pour plus d'informations, cliquez sur **Help** (Aide).

Figure 6-60 : DSL Connection (Connexion DSL)

Annexe A : Dépannage

Cette annexe est composée de deux sections, l'une abordant les problèmes courants et les solutions à y apporter, l'autre traitant des questions fréquemment posées. Des solutions envisageables pour les problèmes susceptibles de se produire lors de l'installation et de l'exploitation du modem routeur y sont décrites. Lisez les descriptions ci-dessous pour vous aider à résoudre vos problèmes. Si vous n'y trouvez aucune réponse, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

Problèmes courants et solutions

1. Je souhaite définir une adresse IP statique sur un ordinateur.

Vous pouvez attribuer une adresse IP statique à un ordinateur en procédant comme suit :

- Windows 98 et Windows Me :
  1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Double-cliquez sur **Réseau**.
  2. Dans la zone Les composants réseau suivants sont installés, sélectionnez le composant TCP/IP associé à votre adaptateur Ethernet. Si un adaptateur Ethernet unique est installé, une seule ligne TCP/IP apparaît sans association à un adaptateur Ethernet. Mettez-la en surbrillance, puis cliquez sur le bouton Propriétés.
  3. Dans la fenêtre Propriétés TCP/IP, sélectionnez l'onglet Adresse IP, puis l'option Spécifier une adresse IP. Saisissez une adresse IP unique n'étant utilisée par aucun autre ordinateur du réseau connecté au modem routeur. Assurez-vous que chaque adresse IP est unique pour chaque ordinateur ou périphérique du réseau.
  4. Cliquez sur l'onglet **Gateway** (Passerelle), puis saisissez 192.168.1.1 dans le champ New Gateway (Nouvelle passerelle), c'est-à-dire l'adresse IP par défaut du modem routeur. Cliquez sur le bouton Add (Ajouter) pour valider cette entrée.
  5. Cliquez sur l'onglet **DNS** et assurez-vous que l'option DNS Enabled (Désactiver DNS) est sélectionnée. Saisissez les noms de l'hôte et du domaine (par exemple, Jean pour l'hôte et « domicile » pour le domaine). Saisissez le système DNS fourni par votre fournisseur d'accès Internet (FAI). Si votre FAI ne vous a pas fourni l'adresse IP du système DNS, contactez-le pour obtenir ce renseignement ou recherchez l'adresse IP en question sur son site Web.
  6. Cliquez sur le bouton **OK** dans la fenêtre Propriétés TCP/IP, puis cliquez sur Fermer ou sur OK dans la fenêtre Réseau.
  7. Redémarrez l'ordinateur lorsque vous y êtes invité.
- Sous Windows 2000 :
  1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Double-cliquez sur **Connexions réseau et accès à distance**.
  2. Cliquez à l'aide du bouton droit de la souris sur la Connexion au réseau local associée à l'adaptateur Ethernet que vous utilisez, puis sélectionnez l'option Propriétés.
  3. Dans la zone Les composants sélectionnés sont utilisés par cette connexion, mettez l'option **Protocole Internet (TCP/IP)** en surbrillance, puis sélectionnez l'option Propriétés. Sélectionnez l'option **Utiliser l'adresse IP suivante**.

4. Saisissez une adresse IP unique n'étant utilisée par aucun autre ordinateur du réseau connecté au modem routeur.
5. Saisissez le masque de sous-réseau 255.255.255.0.
6. Saisissez l'adresse IP par défaut du modem routeur : 192.168.1.1.
7. Dans la partie inférieure de la fenêtre, sélectionnez l'option Utiliser l'adresse de serveur DNS suivante, puis saisissez le serveur DNS préféré et le serveur DNS auxiliaire (fournis par votre FAI). Contactez votre FAI ou consultez son site Web pour vous procurer cette information.
8. Cliquez sur **OK** dans la fenêtre Propriétés de Protocole Internet (TCP/IP), puis de nouveau sur **OK** dans la fenêtre Propriétés de Connexion au réseau local.
9. Redémarrez l'ordinateur si vous y êtes invité.

- Sous Windows XP :
  Les instructions ci-après supposent que vous utilisez l'interface par défaut de Windows XP. Si vous utilisez l'interface Classique (où les icônes et les menus se présentent comme dans les versions précédentes de Windows), suivez les instructions fournies pour Windows 2000.
  1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.
  2. Cliquez sur l'icône **Connexions réseau et Internet**, puis sur l'icône **Connexions réseau**.
  3. Cliquez à l'aide du bouton droit de la souris sur la **Connexion au réseau local** associée à l'adaptateur Ethernet que vous utilisez, puis sélectionnez l'option Propriétés.
  4. Dans la zone **Cette connexion utilise les éléments suivants**, mettez l'option **Protocole Internet (TCP/IP)** en surbrillance. Cliquez sur le bouton **Propriétés**.
  5. Saisissez une adresse IP unique n'étant utilisée par aucun autre ordinateur du réseau connecté au modem routeur.
  6. Saisissez le masque de sous-réseau 255.255.255.0.
  7. Saisissez l'adresse IP par défaut du modem routeur : 192.168.1.1.
  8. Dans la partie inférieure de la fenêtre, sélectionnez l'option Utiliser l'adresse de serveur DNS suivante, puis saisissez le serveur DNS préféré et le serveur DNS auxiliaire (fournis par votre FAI). Contactez votre FAI ou consultez son site Web pour vous procurer cette information.
  9. Cliquez sur le bouton **OK** dans la fenêtre Propriétés de Protocole Internet (TCP/IP). Cliquez sur le bouton **OK** dans la fenêtre Propriétés de Connexion au réseau local.

2. Je souhaite tester ma connexion Internet.

A. Vérifiez vos paramètres TCP/IP.

Windows 98, Me, 2000 et XP :

- Pour plus de détails, reportez-vous à l'aide de Windows. Assurez-vous que l'option Obtenir une adresse IP automatiquement est sélectionnée dans les paramètres.

Windows NT 4.0 :

- Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois sur l'icône **Réseau**.
- Cliquez sur l'onglet Protocole, puis double-cliquez sur le protocole TCP/IP.
- Dans la fenêtre qui s'affiche, assurez-vous que vous avez sélectionné l'adaptateur approprié et définissez-le à **Obtenir une adresse IP par un serveur DHCP**.
- Cliquez sur le bouton **OK** dans la fenêtre Propriétés TCP/IP, puis cliquez sur le bouton **Fermer** dans la fenêtre Réseau.
- Redémarrez l'ordinateur si vous y êtes invité.

B. Ouvrez une invite de commande.

Windows 98 et Windows Me :

- Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ Ouvrir, tapez command. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**.

Windows NT, 2000 et XP :

- Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ Ouvrir, tapez cmd. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**. Dans l'invite de commande, tapez ping 192.168.1.1, puis appuyez sur la touche Entrée.
- Si vous obtenez une réponse, cela signifie que l'ordinateur communique avec le modem routeur.
- Si vous n'obtenez PAS de réponse, vérifiez le câble et assurez-vous que l'option Obtenir une adresse IP automatiquement est sélectionnée dans les paramètres TCP/IP de votre adaptateur Ethernet.

C. Dans l'invite de commande, tapez la commande ping suivie de votre adresse IP Internet ou WAN, puis appuyez sur la touche **Entrée**. Vous pouvez vous procurer l'adresse IP Internet ou WAN dans l'écran Etat de l'utilitaire Web du modem routeur. Par exemple, si votre adresse IP Internet ou WAN est 1.2.3.4, vous devez saisir la commande ping 1.2.3.4, puis appuyer sur la touche Entrée.

- Si vous obtenez une réponse, cela signifie que l'ordinateur est connecté au modem routeur.
- Si vous n'obtenez PAS de réponse, essayez d'appliquer la commande ping à partir d'un autre ordinateur pour vérifier que l'ordinateur d'origine n'est pas la source du problème.

D. Dans l'invite de commande, tapez ping www.yahoo.com, puis appuyez sur la touche **Entrée**.

- Si vous obtenez une réponse, c'est le signe que l'ordinateur est connecté à Internet. Si vous ne parvenez pas à ouvrir une page Web, exécutez la commande ping à partir d'un autre ordinateur pour vérifier que l'ordinateur d'origine n'est pas la source du problème.
- Si vous n'obtenez PAS de réponse, le problème est peut-être lié à la connexion. Essayez d'appliquer la commande ping à partir d'un autre ordinateur pour vérifier que l'ordinateur d'origine n'est pas la source du problème.

3. Je n'obtiens aucune adresse IP sur Internet par le biais de ma connexion Internet.

- Reportez-vous au problème 3 (Je souhaite tester ma connexion Internet) pour vérifier votre connectivité.
  1. Assurez-vous que vous utilisez les paramètres de connexion Internet appropriés. Contactez votre FAI pour savoir si votre connexion Internet est de type RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, Bridged Mode Only (Bridged Mode uniquement) ou RFC 2364 PPPoA. Reportez-vous à la section Configuration du « Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200 » pour obtenir des informations détaillées sur les paramètres de connexion Internet.
  2. Assurez-vous que vous disposez du câble approprié. Vérifiez si le voyant ADSL du modem routeur est allumé.
  3. Assurez-vous que le câble reliant le port ADSL du modem routeur est connecté à la prise murale ADSL. Vérifiez que la page Status (Etat) de l'utilitaire Web du modem routeur indique une adresse IP valide fournie par votre FAI.
  4. Eteignez l'ordinateur et le modem routeur. Attendez 30 secondes puis allumez de nouveau le modem routeur et l'ordinateur. Vérifiez si disposez d'une adresse IP dans l'onglet Status (Etat) de l'utilitaire Web du modem routeur.

4. Je ne parviens pas à accéder à la page de configuration de l'utilitaire Web du modem routeur.

- Reportez-vous au « Problème 2 : Je souhaite tester ma connexion Internet » pour vérifier si votre ordinateur est correctement connecté au modem routeur.
  1. Reportez-vous à l'« Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet » pour vérifier que votre ordinateur possède bien une adresse IP, un masque de sous-réseau, une passerelle et une adresse DNS.
  2. Définissez une adresse IP statique sur votre système. Reportez-vous au « Problème 1 : Je dois définir une adresse IP statique sur un ordinateur ».
  3. Reportez-vous au « Problème 10 : Je dois supprimer les paramètres de proxy ou la fenêtre de connexion à distance (pour les utilisateurs PPPoE) ».

5. Mon VPN (Virtual Private Network) ne fonctionne pas via le modem routeur.

Accédez à l'interface Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur, puis sélectionnez l'onglet Security (Sécurité). Assurez-vous que l'intercommunication IPSec et/ou l'intercommunication PPTP sont activées.

- Les VPN qui utilisent l'authentification IPSec avec ESP (Encapsulation Security Payload, qui porte également le nom de Protocole 50) fonctionnent alors correctement. Au moins une session IPSec fonctionne via le modem routeur. Néanmoins, il est possible d'ouvrir plusieurs sessions IPSec simultanément, en fonction des spécifications de vos VPN.
- Les VPN qui utilisent IPSec et AH (Authentication Header, qui porte également le nom de Protocole 51) sont incompatibles avec le modem routeur. AH est soumis à des limitations en raison d'une incompatibilité occasionnelle avec la norme NAT.
- Remplacez l'adresse IP du modem routeur par un autre sous-réseau, afin d'éviter les conflits entre l'adresse IP du VPN et votre adresse IP locale. Par exemple, si votre serveur VPN attribue une adresse IP 192.168.1.X (X étant un numéro entre 1 et 254) et que votre adresse IP LAN locale est 192.168.1.X (X étant le même numéro utilisé dans l'adresse IP VPN), le modem routeur aura des difficultés à envoyer les informations vers l'emplacement correct. Si vous remplacez l'adresse IP du modem routeur par 192.168.2.1, le problème devrait être résolu. Changez l'adresse IP du modem routeur dans l'onglet Setup (Configuration) de l'interface Web.
- Si vous avez attribué une adresse IP statique à un ordinateur ou périphérique du réseau, vous devez remplacer son adresse IP par 192.168.2.Y (Y étant un nombre quelconque compris entre 1 et 254). Veuillez noter que chaque adresse IP doit être unique sur le réseau.
- Votre VPN peut exiger l'envoi de paquets port 500/UDP vers l'ordinateur connecté au serveur IPSec. Pour plus d'informations, reportez-vous au « Problème 7 : Je souhaite configurer un hébergement pour jeux en ligne ou utiliser d'autres applications Internet ».
- Pour plus d'informations, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

6. Je souhaite configurer un serveur derrière mon modem routeur et le rendre accessible au public.

Pour utiliser un serveur de type serveur de messagerie, serveur Web ou FTP, vous devez connaître les numéros de port utilisés. Par exemple, le port 80 (HTTP) est utilisé pour le Web, le port 21 (FTP) pour le FTP et les ports 25 (SMTP sortant) et 110 (POP3 entrant) pour le serveur de messagerie. Pour obtenir plus d'informations, reportez-vous à la documentation fournie avec le serveur que vous avez installé.

- Pour configurer le transfert de connexion via l'utilitaire Web du modem routeur, procédez comme suit : Nous allons configurer des serveurs Web, FTP et de messagerie.
  1. Accédez à l'utilitaire Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur. Cliquez sur Applications and Gaming (Applications et jeux), puis sur Port Range Forwarding (Transfert de connexion).
  2. Saisissez dans ce champ le nom que vous souhaitez donner à l'application personnalisée.
  3. Saisissez l'étendue de ports externes du service que vous utilisez. Par exemple, si vous utilisez un serveur Web, saisissez l'étendue 80 à 80.
  4. Vérifiez le protocole que vous allez utiliser : TCP et/ou UDP.
  5. Saisissez l'adresse IP de l'ordinateur ou du périphérique réseau auquel vous souhaitez que le serveur de port accède. Par exemple, si l'adresse IP de l'adaptateur Ethernet du serveur Web est 192.168.1.100, saisissez 100 dans le champ. Pour plus d'informations sur l'obtention d'une adresse IP, reportez-vous à l'« Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet ».
  6. Activez la case à cocher Enable (Activer) correspondant au service des ports à utiliser. Prenons l'exemple suivant :

Application personnalisée	Port externe	TCP	UDP	Adresse IP	Activer
Serveur Web	80 à 80	X		192.168.1.100	X
Serveur FTP	21 à 21	X		192.168.1.101	X
SMTP (sortant)	25 à 25	X		192.168.1.102	X
POP3 (entrant)	110 à 110	X		192.168.1.102	X

Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

7. Je dois configurer une solution d'hébergement de jeux en ligne ou utiliser d'autres applications Internet.

Le transfert de connexion ou l'hébergement DMZ ne sont pas nécessaires pour les jeux en ligne ou l'utilisation d'applications Internet. Il se peut que vous souhaitiez héberger un jeu en ligne ou une application Internet. Vous devez dans ce cas configurer le modem routeur pour qu'elle envoie les paquets entrants ou les données entrantes vers un ordinateur spécifique. Cela s'applique également aux applications Internet que vous utilisez. Pour savoir quels services des ports vous devez utiliser, la méthode la plus efficace consister à consulter le site Web des jeux en ligne ou des applications concernés. Pour configurer l'hébergement de jeux en ligne ou utiliser une application Internet spécifique, procédez comme suit :

1. Accédez à l'interface Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur. Cliquez sur Applications and Gaming (Applications et jeux), puis sur Port Range Forwarding (Transfert de connexion).
2. Saisissez dans ce champ le nom que vous souhaitez donner à l'application personnalisée.
3. Saisissez l'étendue de ports externes du service que vous utilisez. Par exemple, si vous souhaitez héberger Unreal Tournament (UT), saisissez l'étendue 7777 à 27900.
4. Vérifiez le protocole que vous allez utiliser : TCP et/ou UDP.

5. Saisissez l'adresse IP de l'ordinateur ou du périphérique réseau auquel vous souhaitez que le serveur de port accède. Par exemple, si l'adresse IP de l'adaptateur Ethernet du serveur Web est 192.168.1.100, saisissez 100 dans le champ. Pour plus d'informations sur l'obtention d'une adresse IP, reportez-vous à l'« Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet ».
6. Activez la case à cocher **Enable** (Activer) correspondant au service des ports à utiliser. Prenons l'exemple suivant :

Application personnalisée	Port externe	TCP	UDP	Adresse IP	Activer
UT	7777 à 27900	X	X	192.168.1.100	X
Halflife	27015 à 27015	X	X	192.168.1.105	X
PC Anywhere	5631 à 5631		X	192.168.1.102	X
VPN IPSEC	500 à 500		X	192.168.1.100	X

Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

8. Je ne parviens pas à faire fonctionner correctement un jeu Internet, un serveur ou une application.

Si vous rencontrez des difficultés à faire fonctionner correctement un jeu Internet, un serveur ou une application, identifiez un ordinateur sur Internet en passant par l'hébergement DMZ (DeMilitarized Zone). Cette option est disponible lorsqu'une application requiert un nombre de ports trop important ou lorsque vous ne savez pas quels services de ports utiliser. Assurez-vous que toutes les entrées de transfert sont désactivées si vous souhaitez utiliser l'hébergement DMZ. Le transfert a en effet priorité sur l'hébergement DMZ. En d'autres termes, les données qui accèdent au modem routeur seront d'abord contrôlées par les paramètres de transfert. Si le numéro de port auquel les données accèdent n'est pas soumis au transfert de connexion, le modem routeur transmet les données à l'ordinateur ou au périphérique réseau défini pour l'hébergement DMZ.

- Pour définir l'hébergement DMZ, procédez comme suit :
  1. Accédez à l'utilitaire Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur. Cliquez sur Applications and Gaming (Applications et jeux), puis sur DMZ. Cliquez sur Enabled (Activé) et saisissez l'adresse IP de l'ordinateur.
  2. Contrôlez les pages Port Forwarding (Transfert de connexion) et désactivez les entrées saisies pour le transfert. Conservez ces informations pour une éventuelle utilisation ultérieure.
- Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

9. J'ai oublié mon mot de passe ou l'invite de mot de passe apparaît toujours lorsque j'enregistre des paramètres du modem routeur.

- Réinitialisez le modem routeur avec les paramètres d'usine. Pour cela, appuyez sur le bouton Reset (Réinitialisation) pendant 10 secondes puis relâchez-le. Si le système vous demande toujours votre mot de passe lors de l'enregistrement des paramètres, procédez comme suit :
  1. Accédez à l'utilitaire Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur. Saisissez le nom d'utilisateur et le mot de passe par défaut **admin** (pour les deux), cliquez sur l'onglet **Administrations**, puis sur **Management** (Gestion).

2. Saisissez un nouveau mot de passe dans le champ Gateway Password (Mot de passe du modem routeur) et saisissez-le de nouveau dans le second champ pour confirmation.
3. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

10. Je dois supprimer les paramètres de proxy ou la fenêtre de connexion à distance - pour les utilisateurs PPPoE.

Si vous disposez de paramètres de proxy, vous devez les désactiver sur votre ordinateur. le modem routeur étant destinée à la connexion Internet, l'ordinateur n'a pas besoin des paramètres de proxy pour l'accès à Internet. Pour vérifier que les paramètres de proxy sont désactivés et que le navigateur que vous utilisez est défini pour une connexion directe au réseau local (LAN), procédez comme suit :

- Pour Microsoft Internet Explorer 5.0 ou version supérieure :
  1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Double-cliquez sur Options Internet.
  2. Cliquez sur l'onglet **Connexions**.
  3. Cliquez sur le bouton **Paramètres réseau** et désactivez toutes les cases à cocher.
  4. Cliquez sur le bouton **OK** pour revenir à l'écran précédent.
  5. Activez la case à cocher **Ne jamais établir de connexion**. Vous supprimez ainsi toutes les invites de connexion à distance pour les utilisateurs PPPoE.

- Pour Netscape 6 et versions supérieures :
  1. Démarrez **Netscape Navigator** et cliquez sur **Edition**, **Préférences**, **Avancé** et **Proxies**.
  2. Assurez-vous que la connexion directe à Internet est sélectionnée à l'écran.
  3. Fermez toutes les fenêtres pour terminer.

11. Pour recommencer, je dois redéfinir les réglages d'usine du modem routeur.

Maintenez pendant 10 secondes le bouton **Reset** (Réinitialiser) enfoncé, puis relâchez-le. Les réglages d'usine sont rétablis pour les paramètres Internet, le mot de passe, le transfert ainsi que tous les autres paramètres. En d'autres termes, le modem routeur revient à sa configuration initiale.

12. Je dois mettre le micrologiciel à niveau.

Pour mettre à niveau le micrologiciel avec les dernières fonctionnalités, vous devez accéder au site Web international de Linksys à l'adresse www.linksys.com/international et télécharger le dernier micrologiciel.

- Procédez comme suit :
  1. Accédez au site Web international de Linksys à l'adresse www.linksys.com/international et sélectionnez votre région ou pays.
  2. Cliquez sur l'onglet **Products** (Produits) et sélectionnez le modem routeur.
  3. Sur la page Web du modem routeur, cliquez sur **Firmware** (Micrologiciel) puis téléchargez la dernière version disponible pour le modem routeur.
  4. Pour mettre à niveau le micrologiciel, suivez les étapes décrites à la section Administration du « Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200 ».

13. La mise à niveau du micrologiciel a échoué et/ou le voyant Power (Alimentation) clignote.

La mise à niveau peut avoir échoué pour diverses raisons. Pour mettre à niveau le micrologiciel et/ou arrêter le clignotement du voyant d'alimentation, procédez comme suit :

- Si la mise à niveau du micrologiciel a échoué, utilisez le programme TFTP (téléchargé avec le micrologiciel). Ouvrez le fichier PDF téléchargé avec le micrologiciel et le programme TFTP et suivez les instructions contenues dans le fichier.
- Définissez une adresse IP statique sur l'ordinateur. Reportez-vous au « Problème 1 : Je souhaite définir une adresse IP statique sur un ordinateur ». Utilisez les paramètres d'adresse IP suivants pour votre ordinateur :
  Adresse IP : 192.168.1.50
  Masque de sous-réseau : 255.255.255.0
  Passerelle : 192.168.1.1
- Effectuez la mise à niveau à l'aide du programme TFTP ou l'utilitaire Web du modem routeur via l'onglet Administration.

14. Le protocole PPPoE de mon service DSL se déconnecte sans cesse.

En réalité, PPPoE n'est pas une connexion dédiée ou permanente. Il se peut que le FAI DSL déconnecte le service après une période d'inactivité, comme c'est le cas pour une connexion téléphonique à distance Internet.

- Une option de configuration permet de conserver une connexion « active ». Il se peut que cela ne fonctionne pas. Dans ce cas, vous devrez rétablir la connexion de manière périodique.
  1. Pour connecter le modem routeur, ouvrez le navigateur Web et saisissez http://192.168.1.1 ou l'adresse IP du modem routeur.
  2. Si le système vous y invite, saisissez le nom d'utilisateur et le mot de passe. (Par défaut, admin).
  3. Dans l'écran **Setup** (Configuration), sélectionnez l'option Keep Alive (Activée) et définissez le délai de rappel à 30 (secondes). Ainsi, la connexion au fournisseur d'accès Internet sera maintenue et votre communication ne sera pas interrompue.
  4. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres). Sélectionnez l'onglet **Status** (Etat), puis cliquez sur le bouton **Connect** (Connecter).
  5. Il se peut que l'état de la connexion soit défini à Connecting (Connexion en cours). Appuyez sur la touche F5 pour actualiser l'écran jusqu'à ce que l'état de la connexion soit défini à Connected (Connecté).
  6. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour continuer.
- Si vous perdez de nouveau la connexion, effectuez les étapes 1 à 6 pour la rétablir.

15. Je ne parviens pas à accéder à ma messagerie électronique, au Web ou au VPN, ou je reçois des données endommagées d'Internet.

Il se peut que le paramètre d'unité de transmission maximale (MTU) nécessite une modification. Par défaut, le paramètre MTU est défini automatiquement.

- Si vous rencontrez des difficultés, procédez comme suit :
  1. Pour connecter le modem routeur, ouvrez le navigateur Web et saisissez http://192.168.1.1 ou l'adresse IP du modem routeur.
  2. Si le système vous y invite, saisissez le nom d'utilisateur et le mot de passe. (Par défaut, admin).

3. Accédez à l'option MTU, puis sélectionnez **Manual** (Manuel). Dans le champ Size (Taille), saisissez 1492.
4. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour continuer.

- Si vous rencontrez toujours des difficultés, essayez différentes valeurs de taille. Essayez les valeurs de la liste suivante (une valeur à la fois et dans l'ordre indiqué) jusqu'à ce que le problème soit résolu :
  1462
  1400
  1362
  1300

16. Le voyant Power (Alimentation) clignote.

Le voyant Power (Alimentation) clignote lors de la mise sous tension de l'appareil. Pendant ce temps, le système démarre et vérifie les différents composants. Une fois cette opération terminée, le voyant reste allumé pour indiquer que le système fonctionne correctement. Si le voyant continue à clignoter, le système est défaillant. Essayez de démarrer le micrologiciel en attribuant une adresse IP statique à l'ordinateur, puis mettez le micrologiciel à niveau. Essayez les paramètres suivants : adresse IP à 192.168.1.50 et masque de sous-réseau à 255.255.255.0.

17. Lorsque je saisis une adresse URL ou IP, j'obtiens une erreur liée à l'expiration du délai et je suis invité à recommencer.

- Vérifiez si les autres ordinateurs fonctionnent. Si c'est le cas, assurez-vous que les paramètres IP de votre ordinateur sont corrects (IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau), Default Gateway (Passerelle par défaut) et DNS). Redémarrez l'ordinateur défaillant.
- Si l'ordinateur est configuré correctement, mais ne fonctionne toujours pas, vérifiez le modem routeur. Vérifiez si elle est connectée et sous tension. Connectez-vous au modem routeur et vérifiez ses paramètres. Si vous ne parvenez pas à établir la connexion, vérifiez le réseau local (LAN) et la connexion de l'alimentation.
- Si le modem routeur est configurée correctement, contrôlez votre connexion Internet (modem DSL/câble, etc.). Vous pouvez retirer le modem routeur pour vérifier la connexion directe.
- Configurez manuellement les paramètres TCP/IP à l'aide d'une adresse DNS fournie par votre FAI.
- Assurez-vous que le navigateur est configuré pour une connexion directe et que les connexions à distance sont désactivées. Dans Internet Explorer, cliquez sur **Outils**, **Options Internet**, puis sur l'onglet **Connexions**. Assurez-vous que la case à cocher **Ne jamais établir de connexion** est activée.
  Dans Netscape Navigator, cliquez sur **Edition**, **Préférences**, **Avancé** et **Proxies**. Assurez-vous que la case à cocher **Connexion directe à Internet** est activée.

18. J'essaie d'accéder à l'utilitaire Web du modem routeur mais je ne vois pas l'écran de connexion apparaître. A la place, le message « 404 Forbidden » (404 interdit) apparaît à l'écran.

Si vous utilisez Internet Explorer, effectuez les étapes ci-après jusqu'à ce que l'écran de connexion de l'utilitaire Web du routeur s'affiche (la même procédure est à suivre si vous utilisez Netscape) :

1. Cliquez sur **Fichier**. Assurez-vous que l'option *Travailler hors connexion* n'est PAS activée.
2. Appuyez sur les touches **CTRL + F5**. Ce type d'actualisation forcée contraint Internet Explorer à charger les nouvelles pages Web et non les pages mises en cache.

- Cliquez sur **Outils**. Cliquez sur **Options Internet**. Cliquez sur l'onglet **Sécurité**. Cliquez sur le bouton **Niveau par défaut**. Assurez-vous que le niveau de sécurité choisi est Moyen ou inférieur. Cliquez sur le bouton **OK**.

Questions fréquemment posées

Quel est le nombre maximal d'adresses IP que le modem routeur peut prendre en charge ?
le modem routeur peut prendre en charge jusqu'à 253 adresses IP.

L'intercommunication IPSec est-elle prise en charge par le modem routeur ?
Oui, il s'agit d'une fonction intégrée qui est activée par défaut.

Où le modem routeur est-elle installée sur le réseau ?
Dans un environnement standard, le modem routeur est installée entre la prise murale ADSL et le réseau local (LAN).

le modem routeur prend-elle en charge IPX ou AppleTalk ?
Non. TCP/IP est le seul protocole standard pour Internet et est devenu la norme internationale appliquée dans le cadre des communications. Les protocoles IPX (protocole de communication NetWare utilisé uniquement pour acheminer des messages d'un nœud à un autre) et AppleTalk (protocole de communication utilisé sur les réseaux Apple et Macintosh) peuvent être adoptés pour des connexions de LAN à LAN, mais ne peuvent être utilisés pour relier Internet à un LAN.

La connexion LAN du modem routeur prend-elle en charge Ethernet 100 Mbit/s ?
le modem routeur prend en charge 100 Mbit/s par l'intermédiaire d'un commutateur 10/100 Fast Ethernet à détection automatique sur le côté LAN du modem routeur.

Qu'est-ce que la technologie NAT (Network Address Translation) et quelle est sa fonction ?
La technologie NAT (Network Address Translation) permet de convertir plusieurs adresses IP d'un réseau local privé en une adresse IP publique diffusée sur Internet. Ceci ajoute un niveau de sécurité car l'adresse de l'ordinateur connecté au LAN privé ne transite jamais via Internet. En outre, la technologie NAT permet l'utilisation du modem routeur sur des comptes Internet bon marché alors que l'adresse TCP/IP est fournie par le FAI. L'utilisateur peut posséder plusieurs adresses privées derrière cette adresse unique fournie par le FAI.

le modem routeur prend-elle en charge d'autres systèmes d'exploitation que Windows 98 Deuxième Edition, Windows Millennium, Windows 2000 ou Windows XP ?
Oui, mais Linksys ne propose à l'heure actuelle aucun service de support technique réservé à l'installation, à la configuration et au dépannage de ces systèmes d'exploitation.

le modem routeur prend-elle en charge le fichier d'envoi ICQ ?

Oui, à l'aide du correctif suivant : cliquez sur le menu ICQ, sélectionnez successivement l'option Préférences, l'onglet Connexions, puis activez la case à cocher indiquant que votre système se trouve derrière un pare-feu ou un serveur proxy. Dans les paramètres du pare-feu, définissez ensuite le délai à 80 secondes. L'utilisateur Internet peut alors envoyer un fichier à un autre utilisateur derrière le modem routeur.

Je souhaite définir un serveur Unreal Tournament (UT), mais les autres utilisateurs du réseau local (LAN) ne peuvent pas y accéder. Que dois-je faire ?

Si vous avez configuré un serveur Unreal Tournament, vous devez créer une adresse IP statique pour chaque ordinateur du réseau local et transférer les ports 7777, 7778, 7779, 7780, 7781 et 27900 vers l'adresse IP du serveur. Vous pouvez également utiliser une étendue de transfert de connexion comprise entre 7777 et 27900. Si vous souhaitez utiliser la fonctionnalité d'administration de serveur Unreal Tournament (UT Server Admin), transférez un autre port. (Le port 8080 fonctionne généralement bien, mais il est utilisé pour l'administration à distance. Il se peut que vous deviez le désactiver.) Ensuite, dans la section [UWeb.WebServer] du fichier server.ini, définissez ListenPort à 8080 (pour qu'il corresponde au port mappé ci-dessus) et ServerName à l'adresse IP attribuée au modem routeur par votre FAI.

Plusieurs joueurs sur le réseau local (LAN) peuvent-ils accéder à un seul serveur de jeux et jouer simultanément à l'aide d'une seule adresse IP publique ?

Cela dépend du jeu réseau et du type de serveur de jeux que vous utilisez. Par exemple, Unreal Tournament prend en charge les connexions multiples avec une seule adresse IP publique.

Comment puis-je faire fonctionner Half-Life: Team Fortress avec le modem routeur ?

Le port client par défaut pour Half-Life est 27005. « +clientport 2700x » doit être ajouté à la ligne de commande de raccourci HL sur les ordinateurs de votre LAN, x correspondant à 6, 7, 8 et ainsi de suite. Plusieurs ordinateurs peuvent ainsi être connectés au même serveur. Problème : la version 1.0.1.6 ne permet pas à plusieurs ordinateurs dotés d'une même clé CD de se connecter simultanément, même s'il s'agit du même LAN (ce qui n'est pas le cas avec la version 1.0.1.3). En matière d'hébergement de jeux, il n'est pas nécessaire que le serveur HL soit dans la zone démilitarisée (DMZ). Transférez simplement le port 27015 vers l'adresse IP locale du serveur.

La page Web se bloque, les fichiers téléchargés sont corrompus et des caractères illisibles apparaissent à l'écran. Que dois-je faire ?

Forcez votre adaptateur Ethernet à 10 Mbits/s ou en mode semi-duplex, puis désactivez temporairement la fonction d'évaluation automatique de la configuration de votre adaptateur Ethernet. (Accédez au Panneau de configuration du réseau dans l'onglet Propriétés avancées de l'adaptateur Ethernet). Assurez-vous que votre paramètre de proxy est désactivé dans le navigateur. Pour plus d'informations, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

Si tout le reste échoue au cours de l'installation, que puis-je faire ?

Réinitialisez le modem routeur en appuyant sur le bouton Reset (Réinitialisation) jusqu'à ce que le voyant Power (Alimentation) s'éteigne puis s'allume. Réinitialisez votre modem DSL en le mettant hors tension puis sous tension. Téléchargez et installez la dernière version du micrologiciel à partir du site Web international de Linksys, à l'adresse suivante www.linksys.com/international.

Comment serai-je averti de la disponibilité des nouvelles mises à niveau du micrologiciel du modem routeur ?
Toutes les mises à niveau du micrologiciel Linksys sont disponibles sur le site Web international de Linksys à l'adresse www.linksys.com/international. Vous pouvez les télécharger gratuitement. Pour mettre à niveau le micrologiciel du modem routeur, utilisez l'onglet Administration de l'utilitaire Web du modem routeur. Si la connexion Internet du modem routeur fonctionne correctement, il est inutile de télécharger une version plus récente du micrologiciel, à moins que cette version ne contienne des nouvelles fonctionnalités que vous souhaitez utiliser.

le modem routeur fonctionne-t-elle dans un environnement Macintosh ?
Oui, mais les pages de configuration du modem routeur ne sont accessibles que par l'intermédiaire de Internet Explorer 4.0 ou Netscape Navigator 4.0 (ou version ultérieure) pour Macintosh.

Je ne parviens pas à afficher l'écran de configuration Web du modem routeur. Que puis-je faire ?
Il se peut que vous deviez supprimer les paramètres de proxy sur votre navigateur Internet (par exemple, Netscape Navigator ou Internet Explorer). Consultez la documentation de votre navigateur. Dans Internet Explorer, cliquez sur Outils, Options Internet, puis sur l'onglet Connexions. Assurez-vous que la case à cocher Ne jamais établir de connexion est activée. Dans Netscape Navigator, cliquez sur Edition, Préférences, Avancé et Proxies. Assurez-vous que la case à cocher Connexion directe à Internet est activée.

Qu'est-ce que l'hébergement DMZ ?
Une zone démilitarisée (DeMilitarized Zone) permet à une adresse IP (ordinateur) d'être visible sur Internet. Certaines applications nécessitent l'ouverture de plusieurs ports TCP/IP. Il est recommandé de configurer votre ordinateur avec une adresse IP statique si vous souhaitez utiliser l'hébergement DMZ. Pour obtenir l'adresse IP du réseau local (LAN), reportez-vous à l'« Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet ».

Si l'hébergement DMZ est utilisé, l'utilisateur exposé partage-t-il l'adresse IP publique avec le modem routeur ?
Non.

Est-ce que le modem routeur transmet les paquets PPTP ou route activement les sessions PPTP ?
le modem routeur permet la transmission des paquets PPTP.

le modem routeur est-elle compatible avec différentes plates-formes ?

Toutes les plates-formes qui prennent en charge Ethernet et TCP/IP sont compatibles avec le modem routeur.

Combien de ports est-il possible de transférer simultanément ?
Théoriquement, le modem routeur peut établir 520 sessions simultanément, mais vous ne pouvez transférer que 10 étendues du port.

Quelles sont les fonctionnalités avancées du modem routeur ?
Les fonctionnalités avancées du modem routeur sont les paramètres sans fil avancés, les filtres, le transfert de connexion, le routage et DDNS.

Comment puis-je savoir si je dispose d'une adresse IP statique ou DHCP ?
Contactez votre FAI pour obtenir cette information.

Comment puis-je faire fonctionner mIRC avec le modem routeur ?
Dans l'onglet Port Forwarding (Transfert de connexion), définissez le transfert de connexion à 113 pour l'ordinateur sur lequel vous utilisez mIRC.

le modem routeur peut-elle être utilisée en tant que serveur DHCP ?
Oui. Le logiciel serveur DHCP est intégré au modem routeur.

Puis-je exécuter une application à partir d'un ordinateur distant via le réseau sans fil ?
Cela dépend si votre application est conçue ou non pour une utilisation en réseau. Consultez la documentation de l'application pour déterminer si elle prend en charge le fonctionnement en réseau.

Qu'est-ce que la norme IEEE 802.11g ?
Il s'agit de l'une des normes IEEE appliquées aux réseaux sans fil. La norme 802.11g permet aux appareils réseau sans fil issus de différents fabricants, mais conformes à cette norme, de communiquer entre eux. La norme 802.11g établit un taux de transfert de données maximal de 54 Mbit/s et une fréquence de fonctionnement de 2,4 GHz.

Qu'est ce que la norme IEEE 802.11b ?
Il s'agit de l'une des normes IEEE appliquées aux réseaux sans fil. La norme 802.11b permet à des périphériques réseau sans fil de différentes marques de communiquer entre eux, à condition qu'ils soient conformes à cette norme. La norme 802.11b établit un taux de transfert de données maximal de 11 Mbit/s et une fréquence de fonctionnement de 2,4 GHz.

Quelles sont les fonctionnalités IEEE 802.11b et IEEE 802.11g prises en charge ?
Le produit prend en charge les fonctions IEEE 802.11b et IEEE 802.11g suivantes :

- CSMA/CA CA (Carrier Sense Multiple Access/Collision Avoidance) avec accusé de réception
- Itinérance multicanal

- Sélection de débit automatique
- Fonctionnalité RTS/CTS
- Fragmentation
- Gestion de l'alimentation

Il prend également en charge la technologie OFDM pour une mise en réseau 802.11g.

Qu'est-ce que le mode Ad hoc ?

Lorsqu'un réseau sans fil est défini en mode Ad hoc (point à point), les ordinateurs équipés sans fil sont configurés pour communiquer directement entre eux, point à point, sans l'intervention d'un point d'accès.

Qu'est-ce que le mode Infrastructure ?

Lorsqu'un réseau sans fil est défini en mode Infrastructure, le réseau sans fil est configuré pour communiquer avec un réseau via un point d'accès sans fil.

Qu'est-ce que l'itinérance ?

L'itinérance est la capacité d'un utilisateur d'ordinateur portable à communiquer en continu tout en se déplaçant dans une zone plus étendue que la zone couverte par un point d'accès unique. Avant d'utiliser la fonction d'itinérance, l'ordinateur doit s'assurer que le numéro de canal est identique au point d'accès de la zone de couverture dédiée.

Pour garantir une connectivité parfaite et harmonieuse, le réseau local (LAN) sans fil doit incorporer différentes fonctions. Ainsi, chaque nœud et point d'accès doit systématiquement accuser réception de chacun des messages. Chaque nœud doit maintenir le contact avec le réseau sans fil, même en l'absence de transmission de données. L'application simultanée de ces fonctions requiert une technologie de mise en réseau RF dynamique qui relie les points d'accès et les nœuds. Dans ce système, le nœud de l'utilisateur final recherche le meilleur accès possible au système. Il évalue tout d'abord les facteurs tels que l'intensité du signal, la charge de messages supportée par chaque point d'accès et la distance entre chaque point d'accès et le réseau fédérateur câblé. Sur la base de ces informations, le nœud sélectionne ensuite le point d'accès correct et enregistre son adresse. Les communications entre le nœud final et l'ordinateur hôte peuvent alors être acheminées de/vers le réseau fédérateur.

Lorsque l'utilisateur se déplace, l'émetteur RF du nœud final vérifie régulièrement le système afin de déterminer s'il est en contact avec le point d'accès d'origine ou s'il doit en rechercher un autre. Lorsqu'un nœud ne reçoit plus de confirmation de son point d'accès d'origine, il entreprend une nouvelle recherche. Une fois le nouveau point d'accès trouvé, il l'enregistre et le processus de communication se poursuit.

Qu'est ce que la bande ISM ?

La FCC et ses homologues internationaux ont défini une bande passante destinée à une utilisation hors licence : la bande ISM (Industrial, Scientific and Medical). Le spectre situé aux alentours de 2,4 GHz est disponible dans le

monde entier. Il offre la possibilité sans précédent de mettre à la disposition des utilisateurs du monde entier un système haut débit sans fil.

Qu'est-ce que la technologie d'étalement du spectre ?

La technologie d'étalement du spectre est une technique hautes fréquences à large bande développée par l'armée pour disposer d'un système fiable de transmission des communications jugées sensibles. Elle est conçue pour optimiser l'efficacité de la bande passante pour plus de fiabilité, d'intégrité et de sécurité. En d'autres termes, ce système utilise plus de bande passante que la transmission à bande étroite. Cependant, l'optimisation produit un signal qui, dans les faits, est plus important et donc plus facile à détecter, pourvu que le récepteur connaisse les paramètres du signal d'étalement du spectre transmis. Si un récepteur n'est pas réglé sur la bonne fréquence, le signal d'étalement du spectre est perçu comme un bruit d'arrière-plan. Les deux principales alternatives sont : les systèmes DSSS (Direct Sequence Spread Spectrum) et FHSS (Frequency Hopping Spread Spectrum).

Qu'est-ce que le système DSSS ? Qu'est-ce que le système FHSS ? Et quelles sont leurs différences ?

Le système FHSS (Frequency-Hopping Spread-Spectrum) utilise une porteuse à bande étroite qui modifie la fréquence en un modèle connu à la fois de l'émetteur et du récepteur. S'il est synchronisé correctement, l'effet immédiat est le maintien d'un canal logique unique. Pour un récepteur non concerné, le signal FHSS ressemble à un bruit à impulsions courtes. Le système DSSS (Direct-Sequence Spread-Spectrum) génère un modèle de bit redondant pour chaque bit transmis. Pour ce modèle de bit, on parlera alors de hachage. Plus la partie hachée est longue, plus la probabilité de récupérer les données d'origine est grande. Même si une ou plusieurs parties hachées sont endommagées au cours de la transmission, les techniques statistiques intégrées à la radio peuvent récupérer les données d'origine sans avoir à les retransmettre. Pour un récepteur non concerné, le signal DSSS apparaît comme un faible bruit de transmission à large bande et est rejeté (ignoré) par la plupart des récepteurs à bande étroite.

Les informations peuvent-elles interceptées lors de leur transmission « par les airs » ?

Un réseau local sans fil offre deux types de protections. Au niveau matériel, il offre une sécurité inhérente de cryptage via la technologie DSSS (Direct Sequence Spread Spectrum). Au niveau logiciel, il offre une fonction de cryptage (WEP) qui améliore la sécurité et le contrôle des accès.

Qu'est-ce que le système WEP ?

WEP (Wired Equivalent Privacy) est un système de protection des données fondé sur un algorithme de clé partagée 64 bits ou 128 bits, conforme à la norme IEEE 802.11.

Qu'est-ce qu'une adresse MAC ?

L'adresse MAC (Media Access Control) est un numéro unique attribué par le fabricant à un périphérique réseau Ethernet, tel qu'un adaptateur réseau, qui permet au réseau de l'identifier au niveau matériel. Pour des raisons de simplicité d'utilisation, ce numéro est généralement permanent. A la différence des adresses IP qui peuvent

changer dès qu'un ordinateur se connecte au réseau, l'adresse MAC d'un périphérique reste identique, ce qui en fait un identifiant réseau particulièrement fiable.

Comment puis-je réinitialiser le modem routeur ?
Appuyez pendant environ 10 secondes sur le bouton Reset (Réinitialisation) situé sur le panneau arrière du modem routeur. Cette opération réinitialise les paramètres d'usine du modem routeur.

Comment puis-je résoudre les problèmes liés à une perte de signal ?
Il n'est pas possible de connaître l'étendue exacte de votre réseau sans fil sans le tester. Chaque obstacle placé entre le modem routeur et un ordinateur sans fil crée une perte de signal. Le verre au plomb, le métal, les sols en béton, l'eau et les murs réduisent le signal et sa portée. Placez d'abord le modem routeur et l'ordinateur sans fil dans la même pièce et déplacez-le progressivement afin de déterminer l'étendue maximale de votre environnement.

Vous pouvez également essayer d'utiliser différents canaux et éliminer ainsi les interférences liées à un canal unique.

Mon signal est excellent, mais je ne parviens pas à « voir » mon réseau.
La sécurité sans fil est probablement activée sur le modem routeur, mais désactivée sur votre adaptateur sans fil (ou inversement). Vérifiez si les paramètres de sécurité sans fil utilisés sur tous les nœuds de votre réseau sans fil sont identiques.

Combien de canaux/fréquences sont disponibles avec le modem routeur ?
Onze canaux sont disponibles, classés de 1 à 11 (en Amérique du Nord, Amérique centrale et Amérique du Sud). Treize canaux sont disponibles, classés de 1 à 13 (dans la plupart des pays de l'Union Européenne). Des canaux supplémentaires peuvent être disponibles dans d'autres régions et soumis aux réglementations de votre région et/ou pays.

Si certaines de vos questions ne sont pas abordées dans cette annexe, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

Annexe B : Sécurité sans fil

Linksys souhaite rendre la mise en réseau sans fil aussi fiable et facile que possible. La génération actuelle de produits Linksys intègre plusieurs fonctions de sécurité réseau, que vous devez cependant mettre en œuvre vous-même. Tenez compte des points suivants lors de la configuration ou de l'utilisation de votre réseau sans fil.

Mesures de sécurité

Cette rubrique présente une liste exhaustive des mesures de sécurité à envisager (suivez au moins les étapes 1 à 5) :

1. Modifiez le SSID par défaut.
2. Désactivez la fonctionnalité de diffusion du SSID.
3. Modifiez le mot de passe par défaut du compte de l'administrateur.
4. Activez le filtrage des adresses MAC.
5. Modifiez régulièrement le SSID.
6. Utilisez l'algorithme de cryptage le plus élevé possible. Utilisez la technologie WPA si elle est disponible. Notez que son utilisation peut réduire les performances de votre réseau.
7. Modifiez les clés de cryptage WEP régulièrement.

Pour plus d'informations sur la mise en place de ces fonctions de sécurité, consultez le « Chapitre 6 : Configuration du modem routeur ADSL sans fil - G avec SRX200 ».

REMARQUE : Certaines de ces fonctions de sécurité sont disponibles uniquement via le modem routeur réseau, le routeur ou le point d'accès réseau. Pour plus d'informations, consultez la documentation du modem routeur, du routeur ou du point d'accès.

Menaces liées aux réseaux sans fil

Les réseaux sans fil sont faciles à localiser. Les pirates informatiques savent que pour se connecter à un réseau sans fil, les produits réseau sans fil doivent d'abord écouter et détecter les « messages de balises ». Ces messages sont faciles à décrypter et renferment la plupart des informations relatives au réseau, notamment son SSID (Service Set Identifier). Voici la procédure de protection que vous pouvez mettre en place :

Modifiez régulièrement le mot de passe de l'administrateur. Il faut savoir que les paramètres de réseau (SSID, clé WEP, etc.) des périphériques sans fil que vous utilisez sont stockés dans le micrologiciel. L'administrateur réseau est la seule personne qui puisse modifier les paramètres réseau. Si un pirate informatique vient à connaître le mot de passe de l'administrateur, il a également la possibilité de modifier ces paramètres à sa guise. Compliquez-lui alors la tâche et rendez cette information plus difficile à obtenir. Modifiez régulièrement le mot de passe de l'administrateur.

SSID. Vous devez garder à l'esprit plusieurs informations concernant le nom SSID :

1. Désactivez l'option de diffusion.
2. Définissez un SSID unique.
3. Modifiez-le régulièrement.

La plupart des périphériques sans fil vous donnent la possibilité de diffuser le SSID. Bien que cette option puisse s'avérer pratique, elle permet à n'importe qui de se connecter à votre réseau sans fil, y compris aux pirates informatiques. Par conséquent, ne diffusez pas le SSID.

Les périphériques réseau sans fil possèdent un SSID par défaut, configuré en usine (celui de Linksys est « linksys »). Les pirates informatiques connaissent ces noms par défaut et peuvent vérifier s'ils sont utilisés sur votre réseau. Modifiez votre SSID, afin qu'il soit unique, tout en évitant d'en choisir un en relation avec votre société ou les périphériques réseau que vous utilisez.

Modifiez régulièrement votre nom SSID pour obliger les pirates ayant accès à votre réseau sans fil à recommencer à zéro lors de toute tentative d'infiltration.

Adresses MAC. Activez le filtrage des adresses MAC. La fonctionnalité de filtrage des adresses MAC vous permet de réserver l'accès aux nœuds sans fil dotés de certaines adresses MAC. Les pirates informatiques rencontrent ainsi plus de difficultés pour accéder à votre réseau au moyen d'une adresse MAC choisie au hasard.

WEP Encryption (Cryptage WEP). Le cryptage WEP (Wired Equivalent Privacy) est souvent considéré comme la panacée en matière de protection sans fil, ce qui n'est pas toujours vrai. Cette protection fournit seulement un niveau de sécurité suffisant pour compliquer la tâche du pirate informatique.

Plusieurs moyens permettent d'optimiser l'efficacité du cryptage WEP :

1. Utilisez le niveau de cryptage le plus élevé.
2. Optez pour une authentification par clé partagée.
3. Modifiez vos clés WEP régulièrement.

WPA. Le système WPA (Wi-Fi Protected Access) offre la plus récente et la meilleure norme de sécurité Wi-Fi existante. **WPA2** est la dernière version de Wi-Fi Protected Access et est dotée d'un cryptage renforcé. WPA vous propose deux méthodes de cryptage : la méthode TKIP (Temporal Key Integrity Protocol) qui fait appel à une méthode de cryptage renforcé et intègre un code MIC (Message Integrity Code) de protection contre les pirates et enfin la méthode AES (Advanced Encryption System) qui procède au cryptage symétrique des données par blocs de 128 bits. WPA/WPA2 Entreprise utilisent un serveur RADIUS (Remote Authentication Dial-In User Service) pour l'authentification.

IMPORTANT : Gardez toujours à l'esprit que chaque périphérique de votre réseau sans fil DOIT utiliser la même méthode et la même clé de cryptage, sans quoi votre réseau sans fil ne fonctionnera pas correctement.

WPA Personal. Sélectionnez le type d'algorithme (TKIP ou AES), saisissez un mot de passe de 8 à 63 caractères dans le champ Passphrase (Phrase de passe), puis précisez un délai de renouvellement des clés dans l'option Group Key Renewal (Renouvellement des clés du groupe) compris entre 0 et 99 999 secondes qui indique au modem routeur ou un autre périphérique la fréquence de changement des clés de cryptage.

WPA2 Personal. WPA2 vous propose une méthode de cryptage, AES, avec des clés de cryptage dynamiques. Saisissez une phrase de passe composée de 8 à 63 caractères. Saisissez une valeur dans le champ Group Key Renewal (Renouvellement des clés du groupe) pour indiquer au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage.

WPA2 Mixed Mode. WPA2 Mixed Mode vous propose le cryptage TKIP+AES. Saisissez une phrase de passe composée de 8 à 63 caractères. Saisissez une valeur dans le champ Group Key Renewal (Renouvellement des clés du groupe) pour indiquer au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage.

WPA entreprise. Cette méthode associe le système WPA à l'utilisation conjointe d'un serveur RADIUS. Saisissez l'adresse IP et le numéro de port du serveur RADIUS, puis saisissez la clé partagée par le modem routeur et le serveur RADIUS. Saisissez ensuite un délai de renouvellement des clés dans la zone Key Renewal Timeout (Délai de renouvellement des clés) pour préciser au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage.

WPA2 entreprise. Cette méthode associe le système WPA2 à l'utilisation conjointe d'un serveur RADIUS. Saisissez l'adresse IP et le numéro de port du serveur RADIUS, puis saisissez la clé partagée par le modem routeur et le serveur RADIUS. Saisissez ensuite un délai de renouvellement des clés dans la zone Key Renewal Timeout (Délai de renouvellement des clés) pour préciser au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage.

La mise en place d'une méthode de cryptage peut avoir un impact négatif sur les performances de votre réseau, mais reste conseillée si des données que vous jugez confidentielles transitent par votre réseau.

Ces conseils de sécurité vous permettent de conserver votre tranquillité d'esprit tout en profitant de la technologie la plus adaptée et la plus souple que Linksys vous propose.

Annexe C : Recherche des adresses MAC et IP de votre carte Ethernet

Cette section explique comment rechercher l'adresse MAC de la carte Ethernet de votre ordinateur pour être en mesure d'utiliser la fonctionnalité de filtrage MAC du modem routeur. Vous pouvez également rechercher l'adresse IP de la carte Ethernet de votre ordinateur. Cette adresse IP est utilisée pour les fonctionnalités de filtrage, de transfert de connexion et/ou DMZ du modem routeur. Suivez la procédure décrite dans cette annexe pour rechercher l'adresse MAC ou IP de la carte sous Windows 98, Windows Me, Windows 2000 ou Windows XP.

Instructions pour Windows 98 ou Me

1. Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ *Ouvrir*, saisissez **winipcfg**. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**.

2. Lorsque l'écran *Configuration IP* apparaît, sélectionnez la carte Ethernet que vous avez connectée au modem routeur à l'aide d'un câble réseau Ethernet CAT 5. Voir la figure C-1.

3. Notez l'adresse de la carte qui s'inscrit à l'écran (voir Figure C-2). Il s'agit de l'adresse MAC de votre carte Ethernet. Elle apparaît sous une forme hexadécimale (série de nombres et de lettres).

   L'adresse MAC/adresse de la carte vous servira pour le filtrage MAC. La figure D-2 présente un exemple d'adresse MAC 00-00-00-00-00-00 des cartes Ethernet. Cette adresse sera différente sur votre ordinateur.

   La figure D-2 présente un exemple d'adresse IP 192.168.1.100 pour la carte Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

REMARQUE : L'adresse MAC est également appelée Adresse de la carte.

Figure C-1 : Ecran Configuration IP

Figure C-2 : Adresse MAC/Adresse de la carte

Instructions pour Windows 2000 ou Windows XP

1. Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ *Ouvrir*, saisissez **cmd**. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**.

REMARQUE : L'adresse MAC est également appelée Adresse physique.

2. A l'invite de commande, saisissez **ipconfig /all**. Appuyez ensuite sur la touche **Entrée**.

3. Notez l'adresse physique indiquée à l'écran (Figure C-3). Il s'agit de l'adresse MAC de votre carte Ethernet. Elle apparaît sous la forme d'une série de chiffres et de lettres.

   L'adresse MAC/adresse physique vous servira pour le filtrage MAC. La figure C-3 présente un exemple d'adresse MAC 00-00-00-00-00-00 pour la carte Ethernet. Cette adresse sera différente sur votre ordinateur.

   La figure C-3 présente un exemple d'adresse IP 192.168.1.100 pour la carte Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

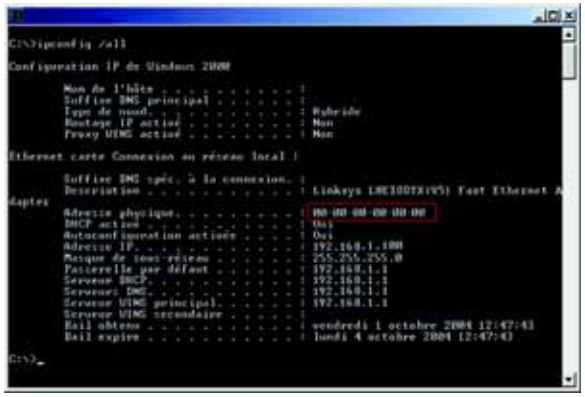


Figure C-3 : Adresse MAC/Adresse physique

Annexe D : Mise à niveau du micrologiciel

Pour mettre à niveau le micrologiciel du modem routeur :

1. Téléchargez le fichier de mise à niveau du micrologiciel du modem routeur depuis le site *www.linksys.com/international*.
2. Extrayez le fichier sur votre ordinateur.
3. Ouvrez l'utilitaire Web du modem routeur et cliquez sur l'onglet **Administration**.
4. Cliquez sur l'onglet **Firmware Upgrade** (Mise à niveau du micrologiciel).
5. Cliquez sur le bouton **Browse** (Parcourir) pour rechercher le fichier extrait, puis double-cliquez sur le fichier.
6. Cliquez sur le bouton **Upgrade** (Mettre à niveau) et suivez les instructions affichées.

Figure D-1 : Firmware Upgrade (Mise à niveau du micrologiciel)

Annexe E : Glossaire

802.11b : norme de mise en réseau sans fil qui spécifie un débit de transfert de données maximum de 11 Mbits/s et une fréquence de 2,4 GHz.

802.11g : norme de mise en réseau sans fil qui spécifie un débit de transfert de données maximum de 54 Mbits/s, une fréquence de 2,4 GHz et une rétro-compatibilité avec les périphériques 802.11b.

Ad hoc : groupe de périphériques sans fil communiquant directement entre eux (point à point) sans l'intervention d'un point d'accès.

Adresse IP : adresse utilisée pour l'identification d'un ordinateur ou d'un périphérique sur un réseau.

Adresse IP dynamique : adresse IP attribuée provisoirement par un serveur DHCP.

Adresse IP statique : adresse fixe attribuée à un ordinateur ou périphérique connecté à un réseau.

Adresse MAC (**M**edia **A**ccess **C**ontrol) **:** adresse unique qu'un fabricant attribue à chaque périphérique réseau.

AES (**A**dvanced **E**ncryption **S**tandard) **:** méthode de sécurité utilisant un cryptage symétrique des données par blocs de 128 bits.

Bande ISM : bande radio utilisée lors de transmissions sans fil.

Bande passante : capacité de transmission d'un périphérique ou d'un réseau donné.

Base de données : ensemble de données organisées pour faciliter l'accès, la gestion et la mise à jour de leur contenu.

Bit : chiffre binaire.

Carte : périphérique ajoutant de nouvelles fonctionnalités réseau à votre ordinateur.

Commande Finger : programme indiquant le nom associé à une adresse de messagerie.

Commutateur : 1. Commutateur de données qui relie les périphériques informatiques aux ordinateurs hôtes, permettant ainsi à de nombreux périphériques de partager un nombre limité de ports. 2. Périphérique permettant de produire, interrompre ou modifier les connexions au sein d'un circuit électrique.

Cryptage : codage des données transmises sur un réseau.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) **:** méthode de transfert des données adoptée pour éviter les collisions de données sur un réseau.

CTS (**C**lear **T**o **S**end) **:** signal émis par un périphérique sans fil pour indiquer qu'il est prêt à recevoir des données.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) **:** autorise l'hébergement d'un site Web, d'un serveur FTP ou d'un serveur de messagerie avec un nom de domaine fixe (par exemple, www.xyz.com) et une adresse IP dynamique.

Débit : quantité de données déplacées avec succès d'un nœud à un autre dans un délai donné.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **:** protocole réseau permettant aux administrateurs d'attribuer des adresses IP temporaires aux ordinateurs du réseau en louant une adresse IP à un utilisateur pour une période limitée, au lieu d'attribuer des adresses IP permanentes.

DMZ (**D**emilitarized **Z**one) **:** fonction qui supprime la protection pare-feu du routeur sur un ordinateur et le rend visible sur Internet.

DNS (**D**omain **N**ame **S**erver) **:** adresse IP du serveur de votre fournisseur d'accès Internet (FAI). Le système DNS permet de convertir des noms de sites Web en adresses IP.

Domaine : nom spécifique d'un réseau d'ordinateurs.

DSL (**D**igital **S**ubscriber **L**ine) **:** connexion haut débit permanente par le biais des lignes téléphoniques standard.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) **:** transmission de fréquence qui introduit un modèle de bit redondant pour diminuer les risques de perte de données lors d'une transmission.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) **:** message intégré aux paquets de données et permettant d'accroître l'efficacité des structures sans fil.

EAP (**E**xtensible **A**uthentication **P**rotocol) **:** protocole d'authentification général utilisé pour contrôler l'accès au réseau. De nombreuses méthodes d'authentification spécifiques fonctionnent ainsi.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) **:** méthode d'authentification mutuelle utilisant une combinaison de certificats numériques et un autre système, comme des mots de passe.

EAP-TLS (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) **:** méthode d'authentification mutuelle utilisant des certificats numériques.

Etalement de spectre : technique de fréquence radio à large bande utilisée pour une transmission plus fiable et sécurisée des données.

Ethernet : protocole de mise en réseau qui spécifie le mode de placement et d'extraction des données via un support de transmission courant.

FAI (**F**ournisseur d'**A**ccès à **I**nternet) **:** société proposant un service d'accès à Internet.

Fragmentation : acte de scinder un paquet en unités lors d'une transmission sur un support réseau inapte à prendre en charge la taille d'origine du paquet.

FTP (**F**ile **T**ransfer **P**rotocol) **:** protocole utilisé pour la transmission de fichiers sur un réseau TCP/IP.

Full Duplex : aptitude d'un périphérique réseau à recevoir et transmettre simultanément des données.

Guirlande : méthode utilisée pour connecter des périphériques en série, l'un après l'autre.

Haut débit : connexion Internet rapide et permanente.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) **:** protocole de communication utilisé pour la connexion à des serveurs sur Internet.

Infrastructure : réseau sans fil relié à un réseau câblé via un point d'accès.

Initialiser : démarrer un périphérique et lui faire exécuter des instructions.

Intervalle de transmission de balise : données transmises sur un réseau sans fil en vue de le synchroniser.

IP (**I**nternet **P**rotocol) **:** protocole utilisé pour transmettre des données sur un réseau.

IPCONFIG : utilitaire des systèmes Windows 2000 et XP qui affiche l'adresse IP d'un périphérique réseau spécifique.

IPSec (**I**nternet **P**rotocol **S**ecurity) **:** protocole VPN employé pour la mise en place d'un échange sécurisé des paquets au niveau de la couche IP.

Itinérance : acte de faire passer un périphérique sans fil d'un point d'accès à un autre sans perdre la connexion.

LAN : ordinateurs ou périphériques mis en réseau qui constituent votre réseau local.

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) **:** méthode d'authentification mutuelle utilisant un système avec nom d'utilisateur et mot de passe.

Logiciel : instructions destinées à l'ordinateur. Série d'instructions destinée à l'exécution d'une tâche donnée appelée « programme ».

Masque de sous-réseau : code d'adresse qui détermine la taille du réseau.

Matériel : présentation physique des ordinateurs, des systèmes de télécommunication et autres périphériques informatiques.

Mbit/s (**M**éga**bit**s par **s**econde) **:** un million de bits par seconde ; unité de mesure de transmission de données.

Micrologiciel : code de programmation qui exécute un périphérique réseau.

mIRC : programme de messagerie instantanée exécuté sous Windows.

Mise à niveau : acte de remplacer un logiciel ou micrologiciel existant par une version plus récente.

Modem câble : périphérique qui établit une connexion Internet par le biais d'un réseau de télévision câblé.

Multidiffusion : envoi simultané de données à un groupe de destinataires.

NAT (**N**etwork **A**ddress **T**ranslation) **:** technologie permettant de convertir les adresses IP d'un réseau local en adresses IP distinctes sur Internet.

Navigateur : application permettant d'afficher et de modifier des informations sur Internet.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) **:** protocole utilisé pour connecter des groupes Usenet sur Internet.

Nœud : liaison ou point de connexion réseau (généralement, un ordinateur ou une station de travail).

Octet : unité de données généralement équivalente à huit bits.

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) **:** transmission de fréquence qui permet de séparer le flux de données en un certain nombre de flux de données à moindre débit, transmis ensuite en parallèle pour diminuer les risques de perte de données lors d'une transmission.

Paquet : unité de données transmise sur un réseau.

Pare-feu : ensemble de programmes associés situés sur un serveur de réseau protégeant les ressources d'un réseau contre les utilisateurs d'autres réseaux.

Pare-feu SPI (**S**tateful **P**acket **I**nspection) **:** technologie inspectant les paquets d'informations entrants avant de les autoriser à pénétrer le réseau.

Passerelle : périphérique permettant de relier entre eux des réseaux dotés de protocoles de communication incompatibles.

Passerelle par défaut : périphérique utilisé pour transférer le trafic Internet depuis votre réseau local.

PEAP (**P**rotected **E**xtensible **A**uthentication **P**rotocol) **:** méthode d'authentification mutuelle utilisant une combinaison de certificats numériques et un autre système, comme des mots de passe.

Phrase de passe : équivalent d'un mot de passe, une phrase de passe simplifie le processus de cryptage WEP en générant automatiquement les clés de cryptage WEP des produits Linksys.

Ping (**P**acket **IN**ternet **G**roper) **:** utilitaire Internet utilisé pour déterminer si une adresse IP particulière est en ligne.

Point d'accès : périphérique permettant aux ordinateurs et aux autres périphériques sans fil de communiquer avec un réseau câblé. Il sert également à étendre la portée d'un réseau sans fil.

Pont : périphérique reliant différents réseaux.

POP3 (**P**ost **O**ffice **P**rotocol **3**) **:** serveur de messagerie standard couramment utilisé sur Internet.

Port : point de connexion sur un ordinateur ou un périphérique réseau utilisé pour le branchement à un câble ou une carte.

Power over Ethernet (**PoE**) **:** technologie permettant à un câble réseau Ethernet d'acheminer des données et l'alimentation.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **:** type de connexion haut débit qui permet l'authentification (nom d'utilisateur et mot de passe) et l'acheminement des données.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) **:** protocole VPN qui permet au protocole PPP (Point to Point Protocol) de traverser un réseau IP. Il est également utilisé comme type de connexion haut débit en Europe.

Préambule : partie du signal sans fil chargée de synchroniser le trafic réseau.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) **:** protocole utilisant un serveur d'authentification pour contrôler l'accès au réseau.

Réseau : série d'ordinateurs ou de périphériques reliés entre eux dans le but de partager et de stocker des données et/ou de permettre la transmission de données entre des utilisateurs.

Réseau fédérateur : partie d'un réseau qui permet de relier la plupart des systèmes et des réseaux entre eux et de gérer la majorité des données.

RJ-45 (**R**egistered **J**ack-**45**) **:** connecteur Ethernet pouvant accueillir jusqu'à huit broches.

Routage statique : transfert de données sur un réseau par une voie fixe.

Routeur : périphérique réseau qui relie entre eux plusieurs ordinateurs.

RTS (**R**equest **T**o **S**end) **:** méthode de transfert des paquets volumineux par le biais du paramètre RTS Threshold (Seuil RTS).

Semi-duplex : transmission de données à double sens sur une ligne unique, mais dans un seul sens à la fois.

Serveur : tout ordinateur dont le rôle sur un réseau est de fournir aux utilisateurs un accès à des fichiers, des imprimantes, des outils de communication et d'autres services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) **:** protocole de messagerie standard utilisé sur Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) **:** protocole très répandu de contrôle et d'administration de réseau.

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) **:** segment de marché des professionnels qui travaillent à domicile ou dans des petits bureaux.

SSID (**S**ervice **S**et **ID**entifier) **:** nom de votre réseau sans fil.

Tampon : zone de mémoire partagée ou affectée utilisée pour prendre en charge et coordonner plusieurs activités informatiques et réseau de façon à ce qu'une activité ne soit pas interrompue par une autre.

TCP (**T**ransmission **C**ontrol **P**rotocol) **:** protocole réseau de transmission de données exigeant la validation de la personne à qui elles sont destinées.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) **:** désigne un ensemble d'instructions (ou protocole) que tous les ordinateurs suivent pour communiquer sur un réseau.

Téléchargement (envoi) **:** transmission d'un fichier sur un réseau.

Téléchargement : réception d'un fichier transmis sur un réseau.

Telnet : commande utilisateur et protocole TCP/IP utilisés pour l'accès à des ordinateurs distants.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) **:** version du protocole FTP TCP/IP n'offrant aucune fonction de répertoire ou de mot de passe.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) **:** protocole de cryptage sans fil qui fournit des clés de cryptage dynamiques pour chaque paquet transmis.

Topologie : configuration physique d'un réseau.

UDP (**U**ser **D**atagram **P**rotocol) **:** protocole réseau de transmission de données n'exigeant aucune validation de la personne à qui elles sont destinées.

URL (**U**niform **R**esource **L**ocator) **:** adresse d'un fichier situé sur Internet.

Vitesse de transmission : taux de transmission.

VPN (**V**irtual **P**rivate **N**etwork) **:** mesure de sécurité visant à protéger des données lorsqu'elles quittent un réseau et s'acheminent vers un autre via Internet.

WAN (**W**ide **A**rea **N**etwork) **:** Internet.

WEP (**W**ired **E**quivalent **P**rivacy) **:** méthode permettant de crypter des données transmises sur un réseau sans fil pour une sécurité accrue.

WINIPCFG : utilitaire Windows 98 et Windows Me qui affiche l'adresse IP d'un périphérique réseau spécifique.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) **:** groupe d'ordinateurs et de périphériques réunis au sein d'un réseau sans fil.

WPA (**W**i-Fi **P**rotected **A**ccess) **:** protocole de sécurité sans fil faisant appel au cryptage TKIP (Temporal Key Integrity Protocol) et pouvant être utilisé en association avec un serveur RADIUS.

Annexe F : Spécifications

Modèle	WAG54GX2
Normes	IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, IEEE 802.3, G.992.1 (G.dmt), g.992.2 (g.lite), g.992.3, g.992.5, T1.413i2
Ports	Power (Alimentation), ADSL, Ethernet (1-4)
Bouton	Reset (Réinitialisation), Power (Alimentation)
Type de câblage	UTP CAT 5
Voyants	Power (Alimentation), Wireless (Sans fil), Ethernet (1-4), DSL, Internet
Nombre d'antennes	2
Connecteur d'antenne Type	Fixe (non amovible)
Puissance RF (EIRP) en dBm	802.11b : 18, 802.11g : 16, 802.11g MIMO : 17
Gain de l'antenne	3,3 dBi
Prise en charge UPnP (possible/certifiée)	Possible

Fonctions de sécurité	Configuration protégée par mot de passe pour l'accès Web Authentifications PAP et CHAP Prévention des attaques DoS (Denial of Service) Filtrage des URL et blocage des mots-clés, de Java, d'ActiveX, de Proxy et des cookies Filtre ToD (accès aux blocs selon le moment) Intercommunications VPN pour IPSec, protocoles PPTP et L2TP WEP 128 bits, 64 bits avec génération de clé WEP/ phrase mot de passe SSID Broadcast Disable (Désactivation de la diffusion SSID) Restriction d'accès par les adresses MAC et IP Supporte jusqu'à 5 tunnelsVPN IPsec, (création, Act / Déact.) Prise en charge WPA et WPA2
Configuration binaire de la clé WEP	64/128 bits
Dimensions	140 x 140 x 27 mm
Poids	270 g (9,60 oz.)
Alimentation	12 Vcc 1 A
Certifications	CE
Température de fonctionnement	0º~40ºC
Température de stockage	-20º~70ºC
Humidité en fonctionnement	10 à 85 %, sans condensation
Humidité de stockage	5 à 95 %, sans condensation

Annexe G : Informations de garantie

Linksys garantit que vos produits Linksys sont, pour l'essentiel, exempts de vices matériels et de fabrication, sous réserve d'une utilisation normale, pendant une période de trois années consécutives (« Période de garantie »). Votre unique recours et l'entière responsabilité de Linksys sont limités, au choix de Linksys, soit à la réparation ou au remplacement du produit, soit au remboursement du prix à l'achat moins les remises obtenues. Cette garantie limitée concerne uniquement l'acheteur d'origine.

Si ce produit devait s'avérer défectueux pendant cette période de garantie, contactez le support technique de Linksys pour obtenir, si besoin est, un numéro d'autorisation de retour. N'OUBLIEZ PAS DE CONSERVER VOTRE PREUVE D'ACHAT A PORTEE DE MAIN LORS DE TOUT CONTACT TELEPHONIQUE. Si Linksys vous demande de retourner le produit, indiquez lisiblement le numéro d'autorisation de retour à l'extérieur de l'emballage et joignez-y une copie de l'original de votre preuve d'achat. AUCUNE DEMANDE DE RETOUR NE PEUT ETRE TRAITEE EN L'ABSENCE D'UNE PREUVE D'ACHAT. Les frais d'expédition des produits défectueux à Linksys sont à votre charge. Linksys prend uniquement en charge les envois via UPS Ground de Linksys chez vous. Les frais d'envoi restent à la charge des clients implantés en dehors des Etats-Unis et du Canada.

TOUTES LES GARANTIES IMPLICITES ET CONDITIONS DE VALEUR MARCHANDE OU D'ADEQUATION A UN USAGE PARTICULIER SONT LIMITEES A LA DUREE DE LA PERIODE DE GARANTIE. TOUTES LES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES IMPLICITES OU EXPLICITES, Y COMPRIS TOUTE GARANTIE IMPLICITE DE NON-CONTREFACON, SONT EXCLUES. Certaines juridictions n'autorisent pas les restrictions relatives à la durée d'une garantie implicite. Par conséquent, la restriction susmentionnée peut ne pas vous être applicable. Cette garantie vous accorde des droits spécifiques. Vous pouvez avoir d'autres droits qui varient en fonction des juridictions.

Cette garantie ne s'applique pas si le produit (a) a été modifié, sauf si cette modification est le fait de Linksys, (b) n'a pas été installé, exploité, réparé ou entretenu conformément aux instructions fournies pas Linksys ou (c) a été altéré suite à une charge physique ou électrique anormale, un usage inadapté du produit, une négligence ou un accident. De plus, en raison du développement permanent de nouvelles techniques visant à infiltrer et attaquer les réseaux, Linksys ne garantit pas que le présent produit est protégé contre toute intrusion ou attaque dont vous feriez l'objet.

CONFORMEMENT A LA LOI ET INDEPENDAMMENT DU FONDEMENT DE LA RESPONSABILITE (Y COMPRIS LES ACTES DE NEGLIGENCE), LINKSYS NE PEUT EN AUCUN CAS ETRE TENU RESPONSABLE DES PERTES DE DONNEES, DE REVENUS OU DE PROFITS OU DES DOMMAGES SPECIAUX, INDIRECTS, CONSECUTIFS, ACCIDENTELS OU ACCESSOIRES LIES OU NON LIES A L'UTILISATION OU A L'INCAPACITE A UTILISER LE PRODUIT (Y COMPRIS TOUS LES LOGICIELS), MEME SI LINKSYS A ETE AVERTI DE LA POSSIBILITE DE TELS DOMMAGES. LA RESPONSABILITE DE LINKSYS NE DEPASSE EN AUCUN CAS LE MONTANT REGLE PAR VOS SOINS POUR LE PRODUIT. Les restrictions susmentionnées s'appliquent même si toutes les garanties ou les recours stipulés dans le présent contrat ne remplissent pas leur fonction principale. Certaines juridictions n'autorisent pas l'exclusion ou la limitation des dommages accessoires ou fortuits, de telle sorte que la limitation ou l'exclusion susmentionnée peut ne pas vous être applicable.

Cette garantie est valide et peut ne s'appliquer que dans le pays d'acquisition du produit.

Veuillez envoyer toutes vos demandes de renseignement à l'adresse suivante : Linksys, P.O. Box 18558, Irvine, CA 92623, Etats-Unis.

Annexe H : Réglementation

Déclaration FCC

Cet équipement a été testé et déclaré conforme aux normes des équipements numériques de catégorie B, conformément à la section 15 des règlements FCC. L'objectif de ces normes est de fournir une protection raisonnable contre toute interférence nuisible dans une installation résidentielle. Cet équipement génère, utilise et peut émettre de l'énergie à hautes fréquences nuisibles et, s'il n'est pas installé et utilisé selon le manuel d'instruction, peut provoquer des interférences gênantes pour les communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences gênantes. Si cet équipement provoque des interférences gênantes pour la réception des ondes de radio ou de télévision, détectables en mettant l'équipement hors tension et sous tension, l'utilisateur peut tenter de remédier à ces interférences des façons suivantes :

- Réorientation ou déplacement de l'antenne de réception
- Augmentation de la distance entre l'équipement ou les périphériques
- Branchement de l'équipement sur une prise différente de celle du récepteur
- Demande d'aide à un revendeur ou technicien radio/télévision expérimenté

Déclaration FCC sur l'exposition aux radiations

Cet équipement est conforme aux normes FCC d'exposition en matière de radiations définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé en respectant une distance minimale de 20 cm entre l'émetteur de radiations et vous-même.

INDUSTRY CANADA

This device complies with Canadian ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industrie Canada.

Informations de conformité pour les produits sans fil 2,4 GHz concernant l'Union européenne et les autres pays suivant la directive européenne 1999/5/EC (R&TTE).

Déclaration de conformité concernant la directive européenne 1999/5/EC (R&TTE)

Česky [Czech]:	Toto zařízeni je v souladu se základnimi požadavky a ostatnimi odpovidajicimi ustanovenimi Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

REMARQUE : La déclaration de conformité est mise à votre disposition sous différentes formes :

- Un fichier PDF figure sur le CD du produit.
- Une copie imprimée est fournie avec le produit.
- Un fichier PDF est disponible sur la page Web du produit. Visitez le site www.linksys.com/international et sélectionnez votre pays ou région. Sélectionnez ensuite votre produit.

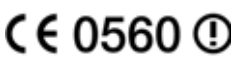
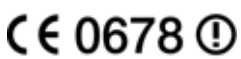
Si vous avez besoin de documentation technique complémentaire, consultez la rubrique « Technical Documents » (Documentation technique) sur le site www.linksys.com/international, mentionnée plus loin dans l'annexe.

Les normes suivantes ont été appliquées lors de l'appréciation du produit conformément aux spécifications de la Directive 1999/5/EC :

- Radio : EN 300 328
- Compatibilité électromagnétique : EN 301 489-1, EN 301 489-17
- Sécurité : EN 60950

Marquage CE

Pour les produits Linksys sans fil B et G, le marquage CE, le numéro de l'organisme notifié (le cas échéant) et l'identifiant de classe 2 suivants sont ajoutés à l'équipement.

 ou  ou 

Vérifiez l'étiquette CE sur le produit pour déterminer le numéro d'organisme notifié chargé de l'évaluation.

Restrictions nationales

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'Union européenne (et dans tous les pays ayant transposé la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous :

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

Belgique

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

France

In case the product is used outdoors, the output power is restricted in some parts of the band. See Table 1 or check http://www.art-telecom.fr/ for more details.

Dans le cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous au tableau 1 ou visitez le site Web http://www.art-telecom.fr/ pour de plus amples détails.

Tableau 1 : Niveaux de puissance en vigueur en France

Emplacement	Bande de fréquences (MHz)	Puissance (PIRE)
Utilisation en intérieur (pas de restrictions)	2400-2483.5	100 mW (20 dBm)
Utilisation en extérieur	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

Italie

Ce produit est conforme à National Radio Interface et aux recommandations définies dans la National Frequency Allocation Table de l'Italie. Au-delà des limites de la propriété du propriétaire, l'utilisation de ce produit réseau sans fil 2,4 GHz exige une « autorisation générale ». Consultez le site http://www.comunicazioni.it/it/ pour de plus amples détails.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2,4 GHz richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Restrictions d'utilisation du produit

Ce produit est conçu pour une utilisation en intérieur uniquement. L'utilisation en extérieur n'est pas recommandée.

Ce produit est conçu pour une utilisation avec une ou plusieurs antennes standard, intégrées ou dédiées (externes) livrées avec l'équipement. Toutefois, certaines applications peuvent exiger que la ou les antennes soient physiquement séparées du produit, si elles sont amovibles, et installées à distance de l'équipement à l'aide de câbles d'extension. Pour ces applications, Linksys propose deux câbles d'extension R-SMA (AC9SMA) et R-TNC (AC9TNC). Ces câbles mesurent tous les deux 9 mètres de long et présentent une atténuation de 5 dB. Pour la compenser, Linksys propose également des antennes à gain plus élevé, la HGA7S (avec le connecteur R-SMA) et la HGA7T (avec le connecteur R-TNC). Ces antennes présentent un gain de 7 dBi et ne peuvent être utilisées qu'avec le câble R-SMA ou R-TNC.

L'utilisation conjointe de câbles d'extension et d'antennes générant un niveau de puissance émise supérieur à 100 mW de la puissance isotrope rayonnée équivalente (PIRE) est considérée comme non conforme.

Puissance de sortie de votre périphérique

Afin de respecter les réglementations de votre pays, vous devrez peut-être modifier la sortie de votre périphérique sans fil. Reportez-vous à la section consacrée à votre périphérique.

REMARQUE : Le réglage de la puissance de sortie n'est peut-être pas disponible sur tous les produits sans fil. Pour plus d'informations, reportez-vous à la documentation fournie sur le CD du produit ou consultez le site http://www.linksys.com/international.

Cartes sans fil

La sortie des cartes sans fil est définie sur 100 % par défaut. La sortie maximale de chaque carte ne dépasse pas 20 dBm (100 mW). Elle est généralement de 18 dBm (64 mW) ou inférieure. Si vous avez besoin de modifier la sortie de votre carte sans fil, suivez les instructions correspondant au système d'exploitation de votre ordinateur :

Windows XP
1. Double-cliquez sur l'icône **Sans fil** dans la barre d'état système de votre bureau.
2. Ouvrez la fenêtre *Connexion réseau sans fil*.
3. Cliquez sur le bouton **Propriétés**.
4. Sélectionnez l'onglet **Général** et cliquez sur le bouton **Configurer**.
5. Dans la fenêtre *Propriétés*, cliquez sur l'onglet **Avancé**.
6. Sélectionnez **Sortie**.
7. A partir du menu déroulant à droite, sélectionnez le pourcentage de puissance de sortie de la carte sans fil.

Windows 2000
1. Ouvrez le **Panneau de configuration**.
2. Double-cliquez sur **Connexions réseau et accès à distance**.
3. Sélectionnez votre connexion sans fil actuelle et sélectionnez **Propriétés**.
4. Dans l'écran *Propriétés*, cliquez sur le bouton **Configurer**.
5. Cliquez sur l'onglet **Avancé** et sélectionnez **Sortie**.
6. A partir du menu déroulant à droite, sélectionnez le paramètre de puissance de la carte sans fil.

Si vous utilisez Windows Millennium ou 98, reportez-vous à l'aide de Windows pour obtenir des instructions sur le mode d'accès aux paramètres avancés d'une carte réseau.

Points d'accès, routeurs ou autres produits sans fil

Si vous utilisez un point d'accès, un routeur ou un autre produit sans fil, utilisez son utilitaire Web pour configurer son paramètre de sortie (reportez-vous à la documentation du produit pour plus d'informations).

Documents techniques disponibles sur le site www.linksys.com/international

Pour accéder aux documents techniques, procédez comme suit :

1. Ouvrez la page http://www.linksys.com/international.
2. Cliquez sur votre région de résidence.
3. Cliquez sur le nom de votre pays de résidence.
4. Cliquez sur **Products** (Produits).
5. Cliquez sur la catégorie de produits appropriée.
6. Sélectionnez un produit.
7. Cliquez sur le type de documentation que vous souhaitez. Le document va s'ouvrir automatiquement au format PDF.

REMARQUE : Si vous avez des questions au sujet de la conformité de ces produits ou si vous ne trouvez pas les informations que vous recherchez, contactez votre bureau de vente local ou consultez le site http://www.linksys.com/international.

Annexe I : Contacts

Besoin de contacter Linksys ?
Consultez notre site Web pour obtenir des informations sur les derniers produits et les mises à jour disponibles pour vos produits existants à l'adresse suivante : http://www.linksys.com/international

Si vous rencontrez des problèmes avec un produit Linksys, adressez un e-mail au service de support technique du pays où vous résidez :

Europe	Adresse e-mail
Allemagne	support.de@linksys.com
Autriche	support.at@linksys.com
Belgique	support.be@linksys.com
Danemark	support.dk@linksys.com
Espagne	support.es@linksys.com
France	support.fr@linksys.com
Italie	support.it@linksys.com
Norvège	support.no@linksys.com
Pays-Bas	support.nl@linksys.com
Portugal	support.pt@linksys.com
Royaume-Uni et Irlande	support.uk@linksys.com
Suède	support.se@linksys.com
Suisse	support.ch@linksys.com

Hors Europe	Adresse e-mail
Amérique Latine	support.portuguese@linksys.com ou support.spanish@linksys.com
Asie Pacifique	asiasupport@linksys.com (anglais uniquement)
Etats-Unis et Canada	support@linksys.com
Moyen-Orient et Afrique	support.mea@linksys.com (anglais uniquement)